5-2017

On Rings of Invariants for Cyclic p-Groups

Daniel Juda
University of Arkansas, Fayetteville

On Rings of Invariants for Cyclic p-Groups

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy in Mathematics

by

Daniel P. Juda
Pacific Lutheran University
Bachelor of Science in Mathematics, 2013
University of Arkansas
Master of Science in Mathematics, 2015

May 2017
University of Arkansas

This dissertation is approved for recommendation to the Graduate Council.

Dr. Lance E. Miller
Dissertation Director

Dr. Mark Johnson
Committee Member

Dr. Paolo Mantero
Committee Member

Abstract

This thesis studies the ring of invariants R^G of a cyclic p-group G acting on $k[x_1, \ldots, x_n]$ where k is a field of characteristic $p > 0$. We consider when R^G is Cohen-Macaulay and give an explicit computation of the depth of R^G. Using representation theory and a result of Nakajima, we demonstrate that R^G is a unique factorization domain and consequently quasi-Gorenstein. We answer the question of when R^G is F-rational and when R^G is F-regular.

We also study the a-invariant for a graded ring S, that is, the maximal graded degree of the top local cohomology module of S. We give an upper bound for the a-invariant of R^G and we show for any subgroup $H \leq G$, we can bound the a-invariant of R^G by the a-invariant of R^H. We extend this result to more general modular rings of invariants where $R^{G'}$ is quasi-Gorenstein and G' has a normal, cyclic, p-Sylow subgroup.

Given a subgroup $H \leq G$ we consider the natural action of H on R and the associated ring of invariants R^H. When G acts in a particular way, we determine the representation underlying the action of H on R. Building on work of Watanabe and Yoshida, we estimate the Hilbert-Kunz multiplicity of R^G in a way that does not depend on finding explicit generators for R^G. We extend this result to modular rings of invariants for groups G' which have a normal, cyclic, p-Sylow subgroup.

Finally, we also consider computations of the norm of x_4 for a cyclic modular action on $k[x_1, \ldots, x_n]$. This builds on and extends work of Sezer and Shank.

Acknowledgements

I would first and foremost like to thank my mother and father, Susan and Paul, for always being a source of inspiration and encouragement. I would also like to thank my uncles, Richard Raymond and Michael Juda, without whom my interest in mathematics might never have occurred. Without such caring and wonderful family members, my completion of this degree would not have been possible.

I would also like to thank my friends at the University of Arkansas, and in particular William Taylor, Jesse Keyton, and Kevser Erdem, who have made the graduate experience exceptional and have helped me through all the moments of difficulty and frustration.

I want to recognize the professors at Pacific Lutheran University, and in particular Thomas Edgar, for giving me a solid grounding in mathematics that set me on the path to success. I would like to recognize the math department staff at the University of Arkansas for their exceptional work helping me with this process.

My committee has played no small role in my success as a mathematician and in my research and I would like to thank Mark and Paolo for their diligence, patience, and help.

Working with Lance has been a true blessing. His patience and teaching has shaped my thinking and approach to mathematics. His guidance has led me down many interesting paths and taught me how to ask the right questions and turn over every stone in the research process. He has not only been an optimistic and dedicate mentor, but a good friend.

Finally, I would be remiss if I did not offer thanks to my wife, Mary Juda, who is my rock in life. She has stood with me through this entire process. Without her, I would not be the mathematician I am today.

Table of Contents

1 Introduction

Let k be a field and V a k-vector space of dimension $n < \infty$. Let G be a finite group and consider a representation of G in $\mathrm{GL}(V) \cong \mathrm{GL}_n(k)$. The action of the representation of G on V defines an action of G on $R := \mathrm{Sym}(V) \cong k[x_1, \ldots, x_n]$. The ring

$$R^G := \{x \in R \mid g \cdot x = x \text{ for all } g \in G\}$$

is called the ring of invariants. Invariant theory is a classic field of study dating back to Gordon, Hilbert, and Noether's studies regarding finite generation of R^G. Indeed, it was the study of invariant theory that led to Noether's famous normalization lemma and the definition of noetherian rings.

Set $m = \mathrm{char}\, k$. We say that the action of G on R is non-modular when $\#G \in R^\times$ and modular otherwise. Noether gave a positive answer to the question of finite generation when G is a finite group, however her proof was non-constructive. In the non-modular case there is a great deal known regarding not only a minimal generating set for R^G but also regarding important properties such as the Cohen-Macaulay property. For example, Eagon and Hochster showed that if G is a finite a group and the action of G on R is non-modular, then R^G is always Cohen-Macaulay [14]. On the other hand, much less is known regarding the modular case. Indeed, if the action of G on R is modular, in many cases there is no known explicit generating set. Although algorithms exist for determining generating sets in the modular case, writing closed forms of these generators is still quite difficult. In this thesis, we consider questions regarding rings of invariants when the action is modular.

Given a group G and a subgroup $H \leq G$, there is a natural inclusion of rings $R^G \subseteq R^H$. In particular, if H is normal in G, then $R^G \cong (R^H)^{G/H}$. Applying this idea gives a natural way to deal with the complexity of modular rings of invariants. If G has a normal, p-Sylow subgroup, $P \leq G$, and we can describe R^P, then the action of G/P on R^P is non-modular. Under these conditions, Chan showed that the inclusion $R^G \subseteq R^P$ is a split inclusion and therefore many desirable properties are preserved from R^P to R^G [8]. In order for this approach to work we need to have a good understanding of R^P. To this end, we restrict our attention in this thesis primarily to $G = \mathbb{Z}/p^e\mathbb{Z}$ and assume $\operatorname{char} k = p > 0$. This gives us that R^G is a graded normal sub-algebra of R. Moreover, for any action of G on $R = k[x_1, \ldots, x_n]$, the action is defined by a degree-preserving k-algebra homomorphism so we will assume throughout that our actions satisfy this.

Our choice of G, while restrictive, allows us to take advantage of the simplicity of the representation theory with respect to G. An action of G on R is said to be indecomposable when the representation, V, of G cannot be written as a direct sum of distinct, non-trivial subrepresentations, i.e. if $V = V_1 \oplus V_2$ with V_1, V_2 subrepresentations of V then $V_1 = \{0\}$ and $V_2 = V$ or vice versa. We show for our choice of G and fixed $n > 0$, there is a unique indecomposable representation for G. We write $V = V_1 \oplus \cdots \oplus V_\ell$ when the representation of G is decomposable, i.e. each V_i is a subrepresentation of V with $V_i \neq \{0\}$ and $V_i \neq V$ for $1 \leq i \leq \ell$. We use this representation theory in our study of R^G to show that R^G is rarely Cohen-Macaulay but has trivial canonical module.

Theorem 1.1 (Corollary 3.6, Theorem 3.14). *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ with representation $V_1 \oplus \cdots \oplus V_\ell$. Set $n_i = \dim V_i$.*

1. *If $n > \ell + 2$, then R^G is not Cohen-Macualay.*

2. *If $n \leq \ell + 2$, then R^G is Cohen-Macualay when one of the following conditions holds.*

   (a) *If $p = 2$, then either $e = 1$ and $n_i = 2$ for one V_i, $e = 1$ and $n_i = 2$ for two V_i, or $e = 2$ and $n_i = 3$ for one V_i; in each case all other V_j has $n_j = 1$.*

   (b) *If $p \geq 3$, then $e = 1$ and either $n_i = 2$ for one V_i, $n_i = 2$ for two V_i, or $n_i = 3$ for one V_i; in each case all other V_j have $n_j = 1$.*

3. *The ring of invariants R^G is quasi-Gorenstein, that is, $R^G \cong \omega_{R^G}$.*

Although already known, we give simple proofs demonstrating these results, including showing explicitly that R^G is a unique factorization domain by considering pseudo-reflections. Note, this also gives a number of examples of rings which are non Cohen-Macaulay unique factorization domains. This combination of properties was thought to be rare for a long time.

The fact that R^G is often not Cohen-Macualay is useful in the study of the F-singularities of Hochster and Huneke. Using the representation theory of G again, we give a classification of what conditions cause R^G to satisfy the strong F-regularity property which is a generalization of a result of Jeffries when $e = 1$ [18].

Theorem 1.2 (Corollary 3.18)**.** *Let $G = \mathbb{Z}/p^e\mathbb{Z}$. act on $R = k[x_1, \ldots, x_n]$. The ring of invariants R^G is F-rational if and only if R^G is F-regular if and only if $n = 2$ or G acts by representation $V_1 \oplus \cdots \oplus V_\ell$ with $n_1 = 2$ and $n_i = 1$ for $2 \leq i \leq \ell$.*

In order to get a more detailed understanding of the properties of R^G we consider the Jordan-Hölder filtration of G. If $g \in G$ is a generator, then

$$0 \leq \langle g^{p^e} \rangle \leq \langle g^{p^{e-1}} \rangle \leq \cdots \leq \langle g^2 \rangle \leq \langle g \rangle = G$$

is a composition series for G with cyclic composition factors, which are isomorphic to $\mathbb{Z}/p\mathbb{Z}$. In a manner similar to Theorem 1.1 we show for any subgroup $H \leq G$, R^H is quasi-Gorenstein. Along with the obvious composition series for G, we use this to prove the following regarding the a-invariant defined in terms of the top local cohomology module of $R^{G'}$ for groups G' with $\mathbb{Z}/p^e\mathbb{Z}$ a normal p-Sylow subgroup.

Theorem 1.3 (Corollary 4.9)**.** *Let G be a group with $\mathbb{Z}/p^e\mathbb{Z} = H \leq G$ a unique p-Sylow subgroup and R^G quasi-Gorenstein. Suppose G acts on a ring R with $\operatorname{char} R = p > 0$. If $0 = N_e \leq N_{e-1} \leq \cdots \leq N_1 \leq N_0 = H$ is a composition series of subgroups acting naturally on R, then*

$$a(R^G) \leq a(R^H) \leq a(R^{N_1}) \leq \cdots \leq a(R^{N_{e-1}}) \leq a(R).$$

This motivates us to give a more explicit representation of R^{N_i} with N_i as defined above. To do so, we consider the structure of the representation of any subgroup $H \leq G$. Recall for our choice of G and fixed $n > 0$, there is a unique indecomposable representation for G. Using this we show that we may view the representation of $H \leq G = \mathbb{Z}/p^e\mathbb{Z}$ in a canonical way.

Theorem 1.4 (Corollary 4.14)**.** *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ by the indecomposable action. Let $g \in G$ be a generator. For $p^{e-1} + m_i p^i < n \leq p^e + (m_i + 1)p^i$ with $0 \leq m_i \leq p^{e-i} - p^{e-i-1} - 1$ and $i = 1, \ldots, e-1$, set*

$$a_t = n - p^{e-1} - m_t p^t, \quad b_t = p^{e-1} + (m_t + 1)p^t - n, \quad c_t = p^{e-t-1} + m_t.$$

We have

$$k[V_n]^G \hookrightarrow k[V_{c_1+1}^{a_1} \oplus V_{c_1}^{b_1}]^{\left\langle g^{p^1} \right\rangle} \hookrightarrow \cdots \hookrightarrow k[V_{c_{e-1}+1}^{a_{e-1}} \oplus V_{c_{e-1}}^{b_{e-1}}]^{\left\langle g^{p^{e-1}} \right\rangle} \hookrightarrow k[V_n]$$

where $\dim_k V_i = i$*.*

This gives a very explicit structure to the natural inclusion of rings $R^G \subseteq R^H$. As mentioned previously, computations involving modular rings of invariants can be quite difficult. Indeed, not knowing a generating set for R^G or even knowing one that is simply too cumbersome to work with makes saying anything regarding properties of R^G a challenge. Our hope is that this structure theorem will be useful for reducing the difficulty in showing various properties of R^G to determining these properties for a subgroup whose ring of invariants is simple enough to compute explicitly.

We next consider the Hilbert-Kunz multiplicity, a positive-characteristic analogue of the well-known Hilbert-Samuel multiplicity, of R^G for modular actions. To do so, we use a special class of ideals in R with respect to G. If $I \subseteq R$ is an ideal, we say that I is G-stable provided $ga \in I$ for all $g \in G$ and $a \in I$. We prove an analogue of Noether's bound on the top degree of a homogeneous generating set for a special case of modular rings of invariants. Along with a theorem of Watanabe and Yoshida, this allows us to give the following bound on the Hilbert-Kunz multiplicity of $R^{G'}$ when G' has a unique p-Sylow subgroup where $p = \operatorname{char} R$.

Theorem 1.5 (Theorem 5.10)**.** *Let R be a graded domain with $\operatorname{char} R = p > 0$, $R_0 = k$ a field and $d = \dim R$. Let G act on R by a degree preserving k-algebra homomorphism, $P \leq G$ be a p-Sylow subgroup, and $s = [G : P]$. If P is normal, $\mathfrak{n}$ is the homogeneous maximal ideal for R^P, and $I \subseteq R^P$ is a G-stable $\mathfrak{n}$-primary ideal, then*

$$e_{HK}(R^G) \leq \frac{\binom{s+d-1}{d} e(I, R^P)}{s}.$$

We use some more classical invariant theory including the algebra of coinvariants and the Hilbert ideal, to give bounds on the Hilbert-Kunz multiplicity when $G = \mathbb{Z}/p^e\mathbb{Z}$. We define the top degree of the algebra of coinvariants for a group G by $\operatorname{td}(R_G)$ and get the following extension of Theorem 1.5 when the p-Sylow subgroup, P, is cyclic.

Theorem 1.6 (Corollary 5.13)**.** *Let R be a graded domain with $\operatorname{char} R = p > 0$, $R_0 = k$ a field and $d = \dim R$. Let G act on R by a degree preserving k-algebra homomorphism with $p \mid \#G$. Let $P \leq G$ be a p-Sylow subgroup acting naturally on R with $s = [G : P]$. If P is normal, then*

$$e_{HK}(R^G) \leq (d!) \frac{\binom{s+d-1}{d} \binom{\operatorname{td}(R_P)+d}{d}}{\#G}.$$

We demonstrate that this bound is sharp, however explicit computations show that in some cases this bound can be quite large. As general bounds are completely unknown and our formula relies only on the representation theory of the chosen group G, which determines the representation theory of P as a subgroup of G, and the generators of the subgroup P, i.e. not on the generators for R^G, this bound is of interest.

The techniques used for all these results mostly avoid using elements of R^G. This is due to the fact that determining nice representations of the generators of R^G is difficult.

Motivated by work of Sezer and Shank, we consider the problem of giving a closed form of a particularly useful invariant called the norm. Let P be a chosen set of equivalence classes for $\mathbb{Z}/p\mathbb{Z}$. We define the sets $S_i := \{A \subseteq P \mid |A| = i\}$, $S_{i,j} := \{A \subseteq P \mid |A| = i, j \notin A\}$, and for $\alpha \subseteq P$, $S_{i,\alpha} := \{A \subseteq P - \alpha \mid |A| = i\}$. For $\alpha \subseteq P$ let $\sigma_j(\alpha)$ denote the jth elementary symmetric polynomial in the elements of α and we will use $\pi(\alpha)$ to denote $\sigma_i(\alpha)$ for $\alpha \in S_i$. We define

$$\hat{d}_{q_1,q_2,j_1,j_2,j_3} := \sum_{\substack{\alpha \in S_{q_1} \\ \beta \in S_{q_2,\alpha}}} \pi(\alpha)\pi(\beta)\sigma_{j_1}(\alpha)\sigma_{j_2}(\alpha)\sigma_{j_3}(\beta).$$

Using $\hat{d}$, we prove several combinatorial results useful for computing coefficients of these invariants and give the following description of the norm of a particular element.

Theorem 1.7 (Theorem 6.5)**.** *Let $G = \mathbb{Z}/p\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ with $\operatorname{char} k = p$ and $n \geq 4$. Write $N(x_4) = \beta_0 + \beta_1 x_1 + \cdots + \beta_{p-(n+1)} x_1^{p-3}$, with $\beta_i \in k[x_2, x_3, x_4]$ and for all i*

$$\beta_i = \gamma_{i,0} + \gamma_{i,1} x_2 + \cdots + \gamma_{i,p-(n+2)-i} x_2^{p-2-i}$$

with $\gamma_{i,j} \in k[x_3, x_4]$. We have

$$\gamma_{i,j} = \begin{cases} \sum_{\ell=1}^{j+1} \xi_{i,j,\ell} x_4^{\ell} x_3^{p-i-j-\ell} & \text{for } 1 \leq j \leq \frac{p-1}{2} \\ \sum_{\ell=1}^{p-j} \xi_{i,j,k} x_4^{\ell} x_3^{p-i-j-\ell} & \text{for } \frac{p+1}{2} \leq j \end{cases}$$

where

$$\xi_{i,j,\ell} = \sum_{s=0}^{i} \sum_{t=0}^{i} \sum_{u=0}^{j} \frac{(-1)^{j-(s+t+u)}}{3^i 2^{j+s}} \binom{p-i-\ell-u}{p-i-j-\ell} \hat{d}_{i,p-i-\ell,s,t,u}.$$

Our hope is that the computations here will provide insight into how to give explicit representations of these invariants in general. In particular, we believe this is a step along the path to giving an explicit generating set as these invariants are known to be a part of any minimal generating set for R^G.

We now outline the rest of the thesis. In Chapter 2 we introduce basic notions and definitions of invariant theory. We also provide some example calculations of algorithms useful for finding generating sets. We give explicit generating sets for two examples of modular rings of invariants of cyclic p-groups, one of which will be used later in the thesis for a theorem regarding singularities. In Chapter 3 we restrict our attention to modular rings of invariants when the group is $G = \mathbb{Z}/p^e\mathbb{Z}$. We prove Theorem 1.1 and Theorem 1.2. We also give an explicit computation regarding the depth of R^G and find examples of regular sequences to exhibit this. In Chapter 4 we prove Theorems 1.3 and 1.4 and give explicit examples of the computations described in their proofs. In Chapter 5 we prove the applications to Hilbert-Kunz multiplicities and again provide several example computations at each step. In Chapter 6 we prove Theorem 1.7 along with several closed forms for $\hat{d}$ and give an example computation using this theorem. In Chapter 7 we extend some of our results on cyclic p-groups to abelian p-groups.

2 Preliminaries

We begin by reviewing some basic notions of invariant theory. Throughout let k be a field with $\operatorname{char} k = p > 0$.

Definition 2.1. Let G be a group and k a field. A *representation* of G is a k-vector space V and a homomorphism $\pi\colon G \to \mathrm{GL}(V)$. We say that a subspace $W \subseteq V$ is a *subrepresentation* provided $\pi\mid_W\colon W \to W$ is a representation of G on W. A representation V is called *indecomposable* provided when $V = W_1 \oplus W_2$ with W_1, W_2 subrepresentations, either $W_1 = \{0\}$ and $W_2 = V$ or vice versa.

Given a representation V of G, each $\varphi \in \mathrm{GL}(V)$ defines an action on $\mathrm{Sym}(V)$, the symmetric algebra of V. Suppose V has finite dimension and set $\dim_k V = n$. Up to a choice of basis, $GL(V) \cong GL_n(k)$. We can identify $\mathrm{Sym}(V) \cong k[x_1, \dots, x_n]$ by fixing a basis $\{e_1, \dots, e_n\}$ for V and mapping $e_i \mapsto x_i$. Identifying V with $\mathrm{span}_k\{x_1, \dots, x_n\}$, each $\varphi \in GL(V)$ gives a k-algebra automorphism of $k[x_1, \dots, x_n]$ defined by $x_i \mapsto \varphi(x_i)$. Set $R = k[x_1, \dots, x_n]$. Throughout, we say that G acts on R rather than use φ and denote the action of $g \in G$ on $f \in R$ by $g(f)$ or $g \cdot f$. The ring of invariants for G acting on R is denoted

$$R^G := \{f \in R \mid g(f) = f \text{ for all } g \in G\}.$$

Alternatively, we use $k[V]$ and $k[V]^G$ in place of R and R^G where convenient.

Rings of invariants have several nice properties. For example, if G is a finite group then R^G is a finitely-generated $\mathbb{N}$-graded k-algebra. Denote by $\mathfrak{m}$ the homogeneous maximal ideal. Throughout the thesis, when a result requires R^G to be a local ring we will consider R^G localized at $\mathfrak{m}$. A representation of a group G acting on R is faithful provided for each $g \in G$ with $g \neq \mathrm{id}_G$, there exists $f \in R$ such that $g \cdot f \neq f$. If G is a finite group with faithful representation, then R^G is normal. We will denote the fraction fields of $k[V]$ and $k[V]^G$ by $k(V)$ and $k(V)^G$ respectively.

Theorem 2.1. *[2, Proposition 1.1.1] If V is a finite dimensional faithful representation of* *a finite group G over a field k, then $k(V)$ is a Galois extension of $k(V)^G$ with Galois group G. The field $k(V)^G$ is the field of fractions of $k[V]^G$, and $k[V]^G$ is integrally closed in $k(V)^G$.*

As many properties are preserved under split inclusions, it is natural to ask when the inclusion, $R^G \subseteq R$, is split. When $\#G \in R^\times$ we say the action of G on R is non-modular. In this case, the inclusion $R^G \subseteq R$ is always split with a splitting given by the following map.

Definition 2.2. Let G be a group acting on a ring R. Suppose $\#G$ is a unit in R. The *Reynolds operator* is a ring homomorphism $\varphi\colon\ R \to R^G$ defined by

$$\varphi(r) = \frac{1}{\#G} \sum_{g \in G} g(r).$$

It is easy to see that $\varphi(R) \subseteq R^G$ and that the Reynolds operator provides a splitting of the inclusion $R^G \subseteq R$. Thus, when the action of G is non-modular, we have a canonically defined splitting. To emphasize its importance, we note that the Reynolds operator is instrumental in the proof of the following celebrated theorem of Eagon and Hochster.

Theorem 2.2. *[14, Eagon, Hochster] If G is a finite subgroup of $\mathrm{GL}(V)$ and $\#G \in k[V]^\times$, then $k[V]^G$ is Cohen-Macaulay.*

When the action of G is modular, that is, $\#G \notin R^\times$, the Reynolds operator is not defined. Indeed a splitting may not exist at all. As a consequence, when the action of G on R is modular, the answer to whether or not R^G is Cohen Macaulay is less clear and will be addressed later. We begin our investigation of modular rings of invariants by considering $G = \mathbb{Z}/p^e\mathbb{Z}$.

2.1 Rings of Invariants for Cyclic p-Groups

Our focus in this section is modular actions of $G = \mathbb{Z}/p^e\mathbb{Z}$. We first explore the eigenspace of a generator of G as a linear map on V.

Theorem 2.3. *Let $g \in G = \mathbb{Z}/p^e\mathbb{Z}$ be a generator. If V is an n-dimensional representation of G over k, then V is indecomposable if and only if $p^{e-1} < n \leq p^e$. In an eigenbasis for V, g acts on a basis via the Jordan block*

$$\begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

More generally, let $V_1 \oplus V_2 \oplus \cdots \oplus V_\ell$ be an n-dimensional representation of G. Set $n_i = \dim V_i$. There is an appropriate basis for $V_1 \oplus V_2 \oplus \cdots \oplus V_\ell$, so that g acts on a basis of V_i via the Jordan block J_i, and so g has the Jordan block decomposition

$$\begin{bmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_\ell \end{bmatrix},$$

where at least one of the V_i has $p^{e-1} < n_i \leq p^e$ and each V_i is indecomposable.

Proof. This follows immediately from the Jordan Normal Form theorem. Let $g \in \mathbb{Z}/p^e\mathbb{Z}$ be a generator. Recall, a representation of G is a k-vector space V together with a homomorphism $\pi\colon G \to \mathrm{GL}(V) \cong \mathrm{GL}_n(k)$. We have $g^{p^e} = 1$, that is, $g^{p^e} - 1 = (g-1)^{p^e} = 0$. The characteristic polynomial for $\pi(g)$ is a factor of $T^{p^e} - 1 = (T-1)^{p^e} \in k[T]$ but not $(T-1)^{p^{e-1}}$ otherwise the order of $\pi(g)$ would be p^{e-1}. This forces $p^{e-1} < n \leq p^e$, i.e., p and e bound the dimension of the representation V. The linear map, $\pi(g)$, has a unique eigenvalue of 1. Since the only eigenvalue for $\pi(g)$ is 1, each distinct eigenvector gives rise to a distinct fixed subspace of V, i.e., a subrepresentation.

Moreover, each Jordan block in $\pi(g)$ gives rise to a subrepresentation. As the Jordan canonical form of a matrix is unique up to permutation of the Jordan blocks, it follows that V is indecomposable if and only if $\pi(g)$ consists of precisely one Jordan block and in particular is represented by J as above.

For the more general case, we once again apply the Jordan Normal Form theorem and the fact that if g is a generator, $g^{p^e} = 1$. We first note that if $\pi(g)$ is an indecomposable representation, then

$$\pi(g)^m = \begin{bmatrix} 1 & \binom{m}{1} & \binom{m}{2} & \binom{m}{3} & \cdots & \binom{m}{n-1} \\ 0 & 1 & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{n-2} \\ 0 & 0 & 1 & \binom{m}{1} & \cdots & \binom{m}{n-3} \\ \vdots & \vdots & \vdots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \binom{m}{1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

It suffices to show that we must have $p^{e-1} < n_i \leq p^e$ for some i and $n_i \leq p^e$ for all i. If $n_i > p^e$ for some i, then the Jordan block J_i has $J_i^{p^e} \neq \mathrm{id}$ whence $\pi(g)^{p^e} \neq \mathrm{id}$ which is a contradiction. If $n_i \leq p^{e-1}$ for all i, then $\pi(g)^{p^{e-1}} = \mathrm{id}$ which is a contradiction. $\square$

Definition 2.3. If G has representation V with V indecomposable, then we say that G acts by the *indecomposable action*. Otherwise we say that G acts by a *decomposable action*. In the decomposable case we need at least one of the Jordan blocks, J_i, to have $p^{e-1} < n_i \leq p^e$. Up to change of basis, i.e. an automorphism of R, we may assume that J_1 satisfies this condition, that is, $p^{e-1} < n_1 \leq p^e$.

Despite the simplicity of the representation theory for $G = \mathbb{Z}/p^e\mathbb{Z}$ there are many open questions regarding the associated ring of invariants. Indeed an explicit generating set, while known to be finite due to Noether, is not known in general. When the action of G is indecomposable with representation given by V with $\dim V \leq 5$, explicit generating sets are known [32]. In the case where $\dim V = 2, 3$ there are known explicit minimal generating sets. When $\dim V > 5$, the question of finding an explicit generating set remains open. While helpful, our study of the rings of invariants does not depend on knowing such explicit sets. In particular, in Chapter 4 we develop a technique for studying R^G to this effect. However, as explicit generators help make these rings concrete, we explore algorithms for finding them in small examples. This will be helpful for Example 3.5 and Corollary 3.18.

Remark 1. It is not difficult to see what happens to coefficients of a polynomial under an indecomposable action. For example, take $G = \mathbb{Z}/2\mathbb{Z}$, $R = k[x, y]$ with $\operatorname{char} k = 2$, and $f \in R$ to be homogeneous of degree n. Writing $f = \sum_{i+j=n} a_{i,j} x^i y^j$, we have the following relationship between the coefficient of $x^2 y^{n-2}$ in f and $g \cdot f$

$$a_{2,n-2} = a_{2,n-2} + \binom{(n-2)+1}{1} a_{1,n-1} + \binom{(n-2)+2}{2} a_{0,n}$$

where the $\binom{(n-2)+i}{i}$ comes from the fact that $y^{(n-2)+i} \mapsto (y+x)^{(n-2)+i}$ and we must choose i binomials in the product $(y+x)^{(n-2)+i}$ to give x when expanding. A similar pattern holds if we increase the number of variables.

Lemma 2.4. *Consider $G = \mathbb{Z}/p^e\mathbb{Z}$ acting by the indecomposable action on $R = k[x_1, \ldots, x_n]$ with $p^{e-1} \leq n \leq p^e$. If $g \in G$ is a generator, then for $0 \leq \ell \leq e-1$*

$$g^{p^\ell}(x_i) = \begin{cases} x_i & i \leq p^\ell \\ x_i + x_{i-p^\ell} & p^\ell + 1 \leq i \leq n \end{cases}. \tag{1}$$

Proof. We use induction on ℓ. If $\ell = 0$ this is by defintion of the indecomposable action. Fix $0 \leq m \leq e-2$ and suppose (1) holds for $0 \leq \ell \leq m$. By direct calculation, for each x_i we have

$$g^{p^{m+1}}(x_i) = g^{pp^m}(x_i) = (g^{p^m})^p(x_i).$$

We now consider three cases $i \leq p^m$, $p^m < i \leq p^{m+1}$, or $p^{m+1} < i$.

Case 1: If $i \leq p^m$, then by the induction hypothesis $g^{p^m}(x_i) = x_i$ and therefore

$(g^{p^m})^p(x_i) = x_i$.

Case 2: Suppose $p^m < i \leq p^{m+1}$. We make the following two observations.

For the jth iteration of g^{p^m}, i.e., $(g^{p^m})^j(x_i)$, we have that the coefficient of x_{i-sp^m} is given by adding the coefficients of $x_{i-(s-1)p^m}$ and x_{i-sp^m} in the $j-1$ iteration by defintion of the indecomposable action. In particular, denoting the coefficient of x_q in $(g^{p^m})^j(x_i)$ by $a_{q,j}$, we have $a_{q,j} = a_{q-1,j-1} + a_{q,j-1}$. Hence by induction we get the binomial coefficients as seen in Pascal's Triangle.

When $i - (p-1)p^m \leq p^{m+1} - (p-1)p^m = p^m$, we have that $g^{p^m}(x_{i-(p-1)p^m}) = x_{i-(p-1)p^m}$ by the induction hypothesis.

If $p^m < i \leq p^{m+1}$, then by the induction hypothesis

$$\begin{aligned}
(g^{p^m})^p(x_i) &= (g^{p^m})^{p-1}(x_i + x_{i-p^m}) \\
&= (g^{p^m})^{p-2}(x_i + 2x_{i-p^m} + x_{i-2p^m}) \\
&= (g^{p^m})^{p-3}(x_i + 3x_{i-p^m} + 3x_{i-2p^m} + x_{i-3p^m}).
\end{aligned}$$

After j steps,

$$(g^{p^m})^p(x_i) = (g^{p^m})^{p-j}\left(\binom{j}{0}x_i + \binom{j}{1}x_{i-p^m} + \cdots + \binom{j}{j}x_{i-jp^m}\right)$$

and for $j = p$,

$$(g^{p^m})^p(x_i) = \binom{p}{0}x_i + \binom{p}{1}x_{i-p^m} + \cdots + \binom{p}{p-1}x_{i-(p-1)p^m} = x_i.$$

Case 3. If $p^{m+1} < i$, then since $i - (p-1)p^m > p^{m+1} - (p-1)p^m = p^m$, the induction hypothesis and the computation in Case 2 gives

$$\begin{aligned}(g^{p^m})^p(x_i) &= \binom{p}{0}x_i + \binom{p}{1}x_{i-p^m} + \cdots + \binom{p}{p-1}x_{i-(p-1)p^m} + \binom{p}{p}x_{i-pp^m} \\ &= x_i + x_{i-p^{m+1}}.\end{aligned}$$

Thus

$$g^{p^{m+1}}(x_i) = \begin{cases} x_i, & i \leq p^{m+1} \\ x_i + x_{i-p^{m+1}}, & p^{m+1}+1 \leq i \leq n \end{cases}.$$

□

With these facts in mind, we compute the generators in two examples. Our first example is when G acts on R by the indecomposable action and $\dim V = 2$ where V is the representation of G. This example is well-known, but we include the details here.

Example 2.1. Let $G = \mathbb{Z}/2\mathbb{Z}$ act on $R = k[x, y]$ by the indecomposable action where $\operatorname{char} k = 2$. By Theorem 2.3, since $n = 2$ and we must have $p^{e-1} < n \leq p^e$, it follows that $e = 1$ for all $p > 0$. Thus we have a group $G = \mathbb{Z}/2\mathbb{Z}$ acting on $R = k[x, y]$ by $x \mapsto x, y \mapsto x + y$. It is well-known that $R^G = k[x, xy + y^2]$. To see this, suppose $f \in R$ and write

$$f = \sum_{i,j} a_{i,j}x^iy^j \tag{2}$$

Therefore

$$\begin{aligned}f \mapsto \sum_{i,j} a_{i,j}x^i(y+x)^j = a_{0,0} &+ x(a_{0,1} + a_{1,0}) + ya_{1,0} + x^2(a_{2,0} + a_{1,1} + a_{0,2}) + xy(a_{1,1}) \\ &+y^2(a_{0,2}) + x^3(a_{3,0} + a_{2,1} + a_{1,2} + a_{0,3}) + x^2y(a_{2,1} + a_{0,3}) \\ &+xy^2(a_{1,2} + 3a_{0,3}) + y^3(a_{0,3}) + \cdots\end{aligned} \tag{3}$$

Now relate the coefficients in (2) and (3) in order to determine information about each $a_{i,j}$. For example, $a_{0,1} = 0$, $a_{1,1} = a_{0,2}$, $3a_{0,3} = 0$, which means $a_{0,3} = 0$ since 3 and $\operatorname{char} k$ are relatively prime, and $a_{2,1} = a_{1,2}$. This information corresponds to saying the following polynomials and any k-linear combination of them are in R^G,

$$x, xy + y^2, x^2y + y^3 = x(xy + y^2)$$

i.e., $k[x, xy + y^2] \subseteq R^G$. It suffices to demonstrate that if $f \in R^G$ has degree greater than or equal to 3, then it can be written using the generating set $1, x, xy + y^2$. Since the indecomposable action is homogeneous, we may assume f is homogeneous and we will use induction on the degree of $f \in R^G$ to prove the claim.

For our base case: if f is homogeneous of degree three, then as shown above

$$f = c(x^2y + xy^2) = cx(xy + y^2)$$

where $c \in k$. Suppose that f can be written using the generators $1, x, xy + y^2$ whenever $f \in R^G$ is homogeneous of degree t. If $f \in R^G$ is homogeneous of degree $t + 1$, then either t is even or odd.

If t is even, then the relation

$$a_{1,t} = a_{1,t} + (t + 1)a_{0,t+1},$$

gives $a_{0,t+1} = 0$. Thus if t is even, then since f is homogeneous we can write $f = xh$ and apply the induction hypothesis.

If t is odd, then $2 \mid t + 1$, ie, $t + 1 = 2n$ for some $n \in \mathbb{N}$. Moreover, we have

$$t + 1 = 2^{\alpha_1} + 2^{\alpha_2} + \cdots + 2^{\alpha_\ell},$$

where $\alpha_i \in \mathbb{Z}_{\geq 1}$ for $1 \leq i \leq \ell$. Write

$$f = y^{2n} + g = y^{2^{\alpha_1}+2^{\alpha_2}+\cdots+2^{\alpha_\ell}} + g$$

with g a polynomial such that each term has at least one x, ie, $g = xg'$ and $\deg g' = t$.

By direct calculation

$$\begin{aligned}
f &= y^{2^{\alpha_1}\cdots 2^{\alpha_\ell}} + xg' \\
&= y^{2^{\alpha_1}+\cdots+2^{\alpha_\ell}} + xg' + 2(xy)^{2^{\alpha_\ell - 1}} y^{2^{\alpha_1}+\cdots+2^{\alpha_{\ell-1}}} \\
&= (y^{2^{\alpha_1}+\cdots+2^{\alpha_\ell}} + (xy)^{2^{\alpha_\ell - 1}} y^{2^{\alpha_1}+\cdots+2^{\alpha_{\ell-1}}}) + xg' + (xy)^{2^{\alpha_\ell - 1}} y^{2^{\alpha_1}+\cdots+2^{\alpha_{\ell-1}}} \\
&= y^{2^{\alpha_1}+\cdots+2^{\alpha_{\ell-1}}}(y^{2^{\alpha_\ell}} + (xy)^{2^{\alpha_\ell - 1}}) + xh \\
&= y^{2^{\alpha_1}+\cdots+2^{\alpha_{\ell-1}}}(y^2 + xy)^{2^{\alpha_\ell - 1}} + xh \\
&= y^{2^{\alpha_1}+\cdots+2^{\alpha_{\ell-1}}}(y^2 + xy)^{2^{\alpha_\ell - 1}} + xh + 2(xy)^{2^{\alpha_1 - 1}+\cdots+2^{\alpha_{\ell-1} - 1}}(y^2 + xy)^{2^{\alpha_\ell - 1}} \\
&= (y^2 + xy)^{2^{\alpha_1 - 1}+\cdots+2^{\alpha_\ell - 1}} + xh + (xy)^{2^{\alpha_1 - 1}+\cdots+2^{\alpha_{\ell-1} - 1}}(y^2 + xy)^{2^{\alpha_\ell - 1}}
\end{aligned}$$

where in the forth equality,

$$xh = xg' + (xy)^{2^{\alpha_\ell - 1}} y^{2^{\alpha_1}+\cdots+2^{\alpha_{\ell-1}}}$$

and as such $\deg h = t$. We have $(y^2 + xy)^{2^{\alpha_1 - 1}+\cdots+2^{\alpha_\ell - 1}} \in R^G$ and therefore

$$xh + (xy)^{2^{\alpha_1 - 1}+\cdots+2^{\alpha_{\ell-1} - 1}}(y^2 + xy)^{2^{\alpha_\ell - 1}} \in R^G. \tag{4}$$

Moreover, the degree of the expression in (4) is at most t so we may apply the induction hypothesis to write it using the desired generators. Thus, we may write f using the generators $1, x, xy + y^2$.

We found the ring of invariants in this example by explicitly relating polynomial coefficients before and after applying the group action. As the number of variables increases, the complexity of this process becomes significantly more difficult. Alternatively, we can use an algorithm developed by Kemper. For more details and a proof of what follows see Algorithms 7 and 8 in [20]. For any graded k-algebra R with $\dim R = n$ and $R_0 = k$, by Noether's normalization, there exists homogeneous elements $f_1, \ldots, f_n \in R$ such that R is finitely generated as a module over $S = k[f_1, \ldots, f_n]$. In the case of rings of invariants, $f_1, \ldots, f_n$ are called primary invariants and generators for R^G as a module over S are called secondary invariants. The following proposition is helpful in computing primary invariants.

Proposition 2.5. *[20, Proposition 1] A set $\{f_1, \ldots, f_i\} \in R^G$ of homogeneous invariants can be extended to a system of primary invariants if and only if the height of $(f_1, \ldots, f_i)$ is i. In particular, homogeneous $f_1, \ldots, f_t \in R^G$ form a system of primary invariants if and only if $t = n$ and $V_{\overline{k}}(f_1, \ldots, f_t) = \{0\}$ where $V_{\overline{k}}$ denotes the set of zeroes over the algebraic closure of k.*

Remark 2. If $G = \mathbb{Z}/p^e\mathbb{Z}$ acts on $k[x_1, \ldots, x_n]$ by the indecomposable action, a set of primary invariants is given by

$$S = \left\{ \prod_{d=1}^{\ell_i} g^d \cdot x_i \mid 1 \leq i \leq n, \ell_i = \min\{p^e \mid i \leq p^e\} \right\}.$$

More generally, if G has representation $V_1 \oplus V_2 \oplus \cdots \oplus V_\ell$, then a set of primary invariants for R^G is given by $S = \{S_1, \ldots, S_\ell\}$ where each S_i is the set of primary invariants for V_i as above since each V_i is indecomposable.

Algorithm 2.6. Let $g \in G$ be a generator and $S = \{f_1, \ldots, f_n\}$ be a set of primary invariants. Set $A = k[S]$. We choose a subgroup $H \leq G$ and find a homogeneous generating set, $h_1, \ldots, h_n$, for R^H. We may choose $H = 0$ so that $R^H = R$. Compute the module $M \leq R^r$ of all $(p_1, \ldots, p_r) \in R^r$ with

$$\sum_{i=0}^{r} (g(h_i) - h_i) p_i = 0.$$

We next take $M \cap A^r$ to get a set of generators $c_1, \ldots, c_m \in A^r$ of $M \cap A^r$ as a module over A. To do so, we take additional indeterminates $t_1, \ldots, t_n$ and set $Q = k[x_1, \ldots x_n, t_1, \ldots, t_n]$. Let $\widetilde{M} \leq Q^r$ be the submodule generated by a generating set $b_1, \ldots, b_s$ for M and by

$(t_j - f_j)e_i$ for $j = 1, \ldots, n$ and $i = 1, \ldots, r$. Let B be a Gröbner basis of $\widetilde{M}$ with respect to a term order such that each x_i is greater than any monomial t_j. Take $\{c_1, \ldots, c_m\}$ to be the set resulting from taking $B \cap (k[t_1, \ldots, t_n])^r$ and substituting t_j for f_j.

We now have $M \cap A^r = \sum_{i=1}^m Ac_i$. Set $g_i := \sum_{j=1}^r c_{i,j}h_j$ for $i = 1, \ldots, m$, $(c_{i,1}, \ldots, c_{i,r}) \in A^r$. The g_i are the secondary invariants and $R^G = \sum_{i=1}^m Ag_i$.

We demonstrate Algorithm 2.6 by rederiving R^G in Example 2.1. By Proposition 2.5, $f_1 := x$ and $f_2 := xy + y^2$ form a system of primary invariants for R^G. Using these we compute the secondary invariants. Set $A = k[f_1, f_2]$, $g \in G$ a generator, and consider the subgroup $\{0\} = H \leq G$. Note that $R^H = R$ and is generated by $1, y$ as an A-module. We need to compute the module $M \leq R^2$ of all points $(p_1, p_2) \in R^2$ such that

$$(g(1) - 1)p_1 + (g(y) - y)p_2 = 0.$$

This forces $xp_2 = 0$, that is, $p_2 = 0$. Thus $M = \langle (1, 0) \rangle$. We now want to compute $M \cap A^2$. To do so, set $S = k[x, y, t_1, t_2]$ and consider the submodule $\widetilde{M} \leq S^2$ generated by $\langle (1, 0), (t_1 - f_1, 0), (0, t_1 - f_1), (t_2 - f_2, 0), (0, t_2 - f_2) \rangle$. By direct computation, a Gröbner basis for $\widetilde{M}$ is given by $B = \{(1, 0), (0, x + t_1), (0, y^2 + yt_1 + t_2)\}$. Thus $M \cap A^r$ is given by taking $B \cap k[t_1, t_2]^2 = \langle (1, 0) \rangle$ and substituing f_i for t_i, that is, $M \cap A^2 = \langle (1, 0) \rangle$. We are now ready to compute the secondary invariants of which there is only one, given by $g = 1(1) + 0(y) = 1$. Thus $R^G = A \cdot 1 = A$.

Example 2.2. If $G = \mathbb{Z}/p\mathbb{Z}$ acts on $k[x, y]$ by the indecomposable action, then the ring of invariants is given by $R^G = k[x, x^{p-1}y - y^p]$. This follows in a similar manner to Example 2.1 with the following differences.

1. Our initial system of primary invariants is given by $f_1 := x$ and $f_2 := x^{p-1}y - y^p$.

2. A Gröbner basis for $\widetilde{M}$ is given by

$$B = \{(1, 0), (0, t_1 - x), (0, t_2 + y^p + x^{p-2}yt_1)\}.$$

We claim $R^G \cong k[a,b]$. Consider the surjective k-algebra homomorphism $\phi\colon\ k[a,b] \twoheadrightarrow R^G$ defined by

$$1 \mapsto 1, a \mapsto x, b \mapsto x^{p-1}y - y^p.$$

Observe that $\ker \phi = 0$ since there are no non-trivial polynomial relations between x and $x^{p-1}y - y^p$, i.e. if $f_1 x + f_2(x^{p-1}y - y^p) = 0$, then either $f_1 = f_2 = 0$ or $f_1 = f'(x^{p-1}y - y^p)$ and $f_2 = f'x$ for some $f' \in k[x,y]$. Thus ϕ is an isomorphism, the claim holds, and R^G is isomorphic to a polynomial ring.

This gives a complete characterization of the indecomposable action on $k[x,y]$ for all p prime. For a more computationally intensive example, we consider $G = \mathbb{Z}/4\mathbb{Z}$ acting on $R = k[x,y,z]$ with $\operatorname{char} k = 2$.

Example 2.3. Let $G = \mathbb{Z}/4\mathbb{Z}$ act on $k[x,y,z]$ by the indecomposable action with $\operatorname{char} k = 2$. Note that by Theorem 2.3, since we must have $2^{e-1} < n = 3 \leq 2^e$, it follows that $e = 2$, that is, to define a faithful action of a group $G = \mathbb{Z}/2^e\mathbb{Z}$ on $k[x,y,z]$ we must have $e = 2$. Fix $g \in G$ a generator. We claim that

$$\begin{aligned} R^G &= k[x, xy + y^2, z^4 + z^2x^2 + zyx^2 + z^2xy + z^2y^2 + zy^2x, xy^2 + y^3 + x^2z + xz^2] \\ &= k\left[g \cdot x, \prod_{1\leq \ell \leq 2} g^\ell \cdot y, \prod_{1 \leq \ell \leq 4} g^\ell \cdot z, xy^2 + y^3 + x^2z + xz^2\right]. \end{aligned} \tag{5}$$

Let $S = \left\{g \cdot x, \prod_{1\leq \ell \leq 2} g^\ell \cdot y, \prod_{1 \leq \ell \leq 4} g^\ell \cdot z \cdot\right\}$. Using Algorithm 2.6, we first need to compute primary invariants. By Remark 2, the elements of S form a system of primary invariants for R^G. We denote the elements of S by f_1, f_2, and f_3 respectively. We now can use S and a generator $g \in G$ to find the secondary invariants and consequently R^G. Set $A = k[S]$ and consider $\langle g^2 \rangle = H \leq G$, which is the subgroup whose elements are representated by the identity matrix and

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

By a computation similar to Example 2.1, $R^H = k[x, y, z^2 + xz]$. A homogeneous system of generators for R^H as a module over A is given by $\{1, y, z^2 + xz, y(z^2 + xz)\}$. To calculate $M \leq k[x, y, z]^4$ we need to find $(p_0, p_1, p_2, p_3) \in k[x, y, z]^4$ satisfying

$$\begin{aligned} 0 &= (g(1) - 1)p_0 + (g(y) - y)p_1 + (g(z^2 + xz) - z^2 + xz)p_2 + (g(y(z^2 + xz)) - y(z^2 + xz))p_3 \\ &= xp_1 + (y^2 + xy)p_2 + (y^3 + xz^2 + x^2z + x^2y)p_3. \end{aligned}$$

By direct calculation, a generating set for M is given by

$$\begin{aligned} \{&(1,0,0,0), (0, y^2 + xy, x, 0), (0, y^3 + xz^2 + x^2z + x^2y, 0, x), \\ &\qquad (0, 0, y^3 + xz^2 + x^2z + x^2y, y^2 + xy), (0, z^2 + xz + xy + y^2, y, 1)\}, \end{aligned}$$

call these $b_1, \ldots, b_4$ respectively. We want to compute $M \cap A^4$ which will yield the secondary invariants and consequently the ring of invariants. Set $T = k[x, y, z, t_1, t_2, t_3]$ and $\widetilde{M} \subseteq T^4$ the submodule generated by

$$\{b_j, (t_1 - f_1)e_i, (t_2 - f_2)e_i, (t_3 - f_3)e_i \mid 1 \leq j \leq 4, 1 \leq i \leq 4\}.$$

After computing a Gröbner basis B for $\widetilde{M}$, we have

$$B \cap k[t_1, t_2, t_3]^4 = \langle (1, 0, 0, 0), (0, t_2, t_1, 0) \rangle.$$

Substituting x for t_1 and $y^2 + xy$ for t_2 yields

$$M \cap A^4 = \langle (1,0,0,0,0), (0, y^2 + xy, x, 0) \rangle.$$

We are now ready to compute the secondary invariants which are given by
$g_1 = 1(1) + 0(y) + 0(z^2 + xz) + 0(y(z^2 + xz)) = 1$ and

$$g_2 = 0(1) + (y^2 + xy)(y) + x(z^2 + xz) + 0(y(z^2 + xz)) = y^3 + xy^2 + xz^2 + x^2 z.$$

Thus $R^G = A \cdot 1 + A \cdot (y^3 + xy^2 + xz^2 + x^2 z)$ which proves the claim.

3 Cohen-Macaulay and Quasi-Gorenstein Rings of Invariants

3.1 Depth and Cohen-Macaulay Rings of Invariants

One question of interest in invariant theory is when a ring of invariants is Cohen-Macaulay. Recall given a noetherian local ring $(S, \mathfrak{n})$ and a finitely generated S-module $M \neq 0$, the depth of M is the infimum over n such that $\operatorname{Ext}_S^n(S/\mathfrak{n}, M) \neq 0$. The S-module M is Cohen-Macaulay if $\operatorname{depth} M = \dim M$ and the ring S is Cohen-Macaulay if it is Cohen-Macaulay as a module over itself. Recall, we localize R^G at the homogeneous maximal ideal $\mathfrak{m}$ when we require R^G to be local. In the case where the action of G on R is non-modular, we have the following celebrated theorem of Eagon and Hochster.

Theorem 3.1. *[14, Eagon, Hochster] If G is a finite subgroup of $\mathrm{GL}(V)$ and $\#G$ is not divisible by the characteristic of k, then $k[V]^G$ is Cohen-Macaulay.*

However, when the action of G on R is modular the answer to whether or not R^G is Cohen Macaulay is less clear. In the modular case the p-Sylow subgroups help determine when R^G is Cohen-Macaulay as follows.

Lemma 3.2. *[18, Jeffries] Let G be a finite subgroup of $\mathrm{GL}(V)$ with $\operatorname{char} k \mid \#G$. Let $P \leq G$ be a p-Sylow subgroup. If $k[V]^P$ is Cohen-Macaulay, then $k[V]^G$ is Cohen-Macaulay.*

This reduces the question of whether R^G is Cohen-Macaulay when the action of G on R is modular to the case of considering p-Sylow subgroups. In this section, we collect known facts and summarize when R^G is Cohen-Macaulay or quasi-Gorenstein for $G = \mathbb{Z}/p^e\mathbb{Z}$. This builds on the work of Kemper in [21] which uses bireflections.

Definition 3.1. Let G be a subgroup of $\mathrm{GL}(V)$. We say that $g \in G$ is a *pseudo-reflection* if $\operatorname{rank}(g - id) = 1$. We say that $g \in G$ is a *bireflection* if $\operatorname{rank}(g - \mathrm{id}) \leq 2$.

Theorem 3.3. *[21, Kemper] Let G be a group of order p^e and $R = k[x_1, \ldots, x_n]$. If R^G is Cohen-Macaulay, then G is generated by bireflections.*

Thus to determine if R^G is Cohen-Macualay, we study the bireflections. In particular, Theorem 3.3 tells us that when G is not generated by bireflections, R^G is not Cohen-Macaulay.

Corollary 3.4. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ by the indecomposable action. If $n > 3$, then R^G is not Cohen Macaulay.*

Proof. If $g \in G$ is a generator, then since $n > 3$ we have $\operatorname{rank}(g - \mathrm{id}) > 2$ by definition of the indecomposable action. By Theorem 3.3, R^G is not Cohen-Macaulay. □

As many of the rings of invariants we are considering are not Cohen-Macuaulay, we know the depth and dimension of R^G are not the same. We would like to know how far apart these two invariants are. Since we know that R is integral over R^G, it follows that $\dim(R^G) = \dim(R) = n$. There are known results to compute the depth for any action of $G = \mathbb{Z}/p^e\mathbb{Z}$ on R. Indeed, the formula we present here is well-known and is proved in [29] using spectral sequences but we will avoid such methods in our treatment. For cyclic p-groups acting on rings of characterstic p, well known results of Ellingsrud and Skjelbred [9, 20] give that $\operatorname{depth}(R^G) = \min\{n, n - m + 2\}$ where m is the dimension of the k-vector space generated by

$$\{g^d(x_i) - x_i \mid 1 \le i \le n, 1 \le d \le p^e\}. \tag{6}$$

We use this to give an elementary proof of the depth when $G = \mathbb{Z}/p^e\mathbb{Z}$.

Theorem 3.5. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ and $R = k[x_1, \ldots, x_n]$.*

1. *If G acts on R by the indecomposable action with $n = 1, 2$, then* $\operatorname{depth}(R^G) = n$.

2. *If G acts on R by the indecomposable action with $n \ge 3$, then* $\operatorname{depth}(R^G) = 3$.

3. *Let G act on R with representation $V_1 \oplus \cdots \oplus V_\ell$. We have*

$$\operatorname{depth}(R^G) = \min\{n, \ell + 2\}.$$

Proof. Let $g \in G$ be a generator. Let V denote the vector space generated by the set defined in (6).

1. It is well known that when $n = 1, 2$, R^G is a polynomial ring (see Example 2.2).

2. We claim $m = \dim V = n - 1$. For $i = 1$, $g^d(x_i) - x_i = 0$ for all $d = 1, \ldots, p^e - 1$. For $i > 1$, we have $g(x_i) - x_i = x_{i-1}$. By definion of the indecomposable action, $g(x_j) - x_j = x_{j-1}$ cannot have a monomial term x_n for all $1 \leq j \leq n$ since $g(x_n) - x_n = x_{n-1}$ does not have a monomial term x_n. If we consider $g^d(x_i) - x_i$ for any $i = 1, \ldots, n$ and $d = 1, \ldots, p^e - 1$, then by definition of the indecomposable action it will be a linear combination of the x_j. Since it is clear the x_i are linearly independent, it follows that $x_1, \ldots, x_{n-1}$ forms a $\mathbb{F}_p$-vector space basis for V. Thus

$$\operatorname{depth}(R^G) = \min\{n, n - m + 2\} = \min\{n, 3\} = 3.$$

3. We need to compute the dimension of V. Note that any element $g^d \in G$ acts independently on each V_i. Since the elements of G act independently on each V_i, a basis for V is given by a union of bases for the V_i of the desired form. By the proof in part (2), V_i will contribute $i - 1$ elements to a basis for the vector space V. Thus, in this case, the dimension of V is $\sum_{i=1}^{\ell}(i-1)$. Moreover, this gives

$$n - m + 2 = \left(\sum_{i=1}^{\ell} i\right) - \left(\sum_{i=1}^{\ell}(i-1)\right) + 2 = \ell + 2$$

   and the result follows.

□

We can now observe, using this characterization of depth, that when G acts by the indecomposable action with $n = 1, 2, 3$, R^G is Cohen Macaulay. Of more interest is when G acts by a decomposable action. In particular, we see that if there are enough 1×1 Jordan blocks in the decomposition of the representation of G, R^G may be Cohen-Macaulay since this will increase the depth of R^G but will not increase the dimension.

Example 3.1. Consider G acting on R with the following Jordan block decomposition of its representation.

$$\left[\begin{array}{cc|c|c} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right]$$

According to Theorem 3.5, $\operatorname{depth}(R^G) = \min\{4, 3+2\} = 4$ and therefore R^G is Cohen-Macaulay since $\operatorname{depth}(R^G) = \dim(R^G)$. On the other hand, suppose the action of G on R has the following Jordan block decomposition.

$$\left[\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

Again by Theorem 3.5, $\operatorname{depth}(R^G) = \min\{5, 2+2\} = 4$ and therefore R^G is not Cohen-Macaulay.

This allows us to give a characterization of when any action of $G = \mathbb{Z}/p^e\mathbb{Z}$ on R is Cohen-Macaulay.

Corollary 3.6. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ with representation $V_1 \oplus \cdots \oplus V_\ell$. Set $n_i = \dim V_i$.*

1. *If $n > \ell + 2$, then R^G is not Cohen-Macualay.*

2. *If $n \leq \ell + 2$, then R^G is Cohen-Macualay when one of the following conditions hold.*

(a) *If $p = 2$, then either $e = 1$ and $n_i = 2$ for one V_i, $e = 1$ and $n_i = 2$ for two V_i, or $e = 2$ and $n_i = 3$ for one V_i; in each case all other V_j has $n_j = 1$.*

(b) *If $p \geq 3$, then $e = 1$ and either $n_i = 2$ for one V_i, $n_i = 2$ for two V_i, or $n_i = 3$ for one V_i; in each case all other V_j have $n_j = 1$.*

Proof. For part (1), apply Theorem 3.5 to see that when $n > \ell + 2$, $\dim(R^G) > \operatorname{depth}(R^G)$. For part (2), Theorem 3.5 implies we must have $n_i \leq 3$ for all i. If there exists V_i with $n_i = 3$, then it is unique and all other V_j are trivial. This guarantees that $n = \ell + 2$. We can have $n_i = 2$ for up to two values of i and all other V_j trivial; in these cases, we have $n = \ell + 1$ or $n = \ell + 2$ respectively. The bounds on e follow from Theorem 2.3. $\square$

We have established a formula for the depth of R^G. According to Theorem 3.5 when $n \geq 3$ any regular sequence has length at most 3. Our next goal is to find explicit regular sequences in the ring of invariants.

Theorem 3.7. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$.*

1. *If G acts by the indecomposable action, then $x_1, x_1^{p-1}x_2 - x_2^p$ is a regular sequence in R^G.*

2. *If $n \geq 3$, G acts by the indecomposable action, and $g \in G$ is a generator, then*

$$x_1, x_1^{p-1}x_2 - x_2^p, \prod_{d=1}^{p} g^d(x_3)$$

   is a regular sequence in R^G.

3. *If G acts by a decomposable action and $\operatorname{depth}(R^G) = \ell + 2 > n$ with $J_1, \cdots, J_\ell$ the Jordan blocks in the Jordan block decomposition of the representation of G and $n_i \geq 3$ for some $1 \leq i \leq \ell$, then*

$$x_1, x_1^{p-1}x_2 - x_2^p, \prod_{d=1}^{p} g^d(x_3), x_{n_1+1}, x_{n_1+n_2+1}, \cdots, x_{n_1+\cdots+n_{\ell-1}+1}$$

is a regular sequence.

4. *Let G act by a decomposable action with representation $V_1 \oplus \cdots \oplus V_\ell$ and suppose R^G is Cohen-Macaulay. Set $S = \{S_1, \cdots, S_\ell\}$ where S_i is a set of primary invariants for V_i. The set S is a regular sequence.*

Proof. Let $g \in G$ be a generator. Denote $f_1 = x_1$, $f_2 = x_1^{p-1}x_2 - x_2^p$, and $f_3 = \prod_{d=1}^{p} g^d(x_3)$.

1. Since R^G is a domain, it is clear that f_1 is a regular element in R^G. Moreover, it is clear that f_2 is not a zero-divisor in R^G/x_1R^G hence is a regular element of R^G/x_1R^G.

2. Note that $R^G/(x_1, f_2)R^G$ is a subring of $R/(x_1, x_2^p)R$. If f_3 is a zero-divisor in $R^G/(x_1, f_2)R^G$ then it is a zero-divisor in $R/(x_1, x_2^p)R$. Thus it suffices to prove that f_3 is a regular element of $R/(x_1, x_2^p)R$. In $R/(x_1, x_2^p)R$

$$f_3 = a_1x_3x_2^{p-1} + a_2x_3^2x_2^{p-2} + \cdots + a_{p-1}x_3^{p-1}x_2 + x_3^p$$

   where each $a_i \in k$ and it is clear f_3 is a regular element of $R/(x_1, x_2^p)R$.

3. This follows from (2), the conventions in Definition 2.3, and the fact that it is clear $x_{n_1+\cdots+n_i+1}$ is a regular element of

$$R^G/\left(x_1, x_1^{p-1}x_2 - x_2^p, \prod_{d=1}^{p} g^d(x_3), x_{n_1+1}, x_{n_1+n_2+1}, \cdots, x_{n_1+\cdots+n_{i-1}+1}\right) R^G$$

   for all $2 \leq i \leq \ell - 1$.

4. We give the set S in each of the three cases described in Corollary 3.6 using Remark 2. If $n_1 = 2$ and $n_i = 1$ for $i \neq 1$, then

$$S = \{x_1, x_2^p - x_1^{p-1}x_2, x_3, \ldots, x_\ell\}.$$

If $n_1 = n_2 = 2$ and $n_i = 1$ for $i \neq 1, 2$, then

$$S = \{x_1, x_2^p - x_1^{p-1}x_2, x_3, x_4^p - x_3^{p-1}x_4, x_5, \ldots, x_\ell\}.$$

If $n_1 = 3$ and $n_i = 1$ for $i \neq 1$, then

$$S = \{x_1, x_2^p - x_1^{p-1}x_2, \prod_{d=1}^{p} g^d(x_3), x_4, \ldots, x_\ell\}.$$

It is not difficult to see that these form regular sequences. For the first two cases apply part (1) and the argument in part (3). For the third case apply part (2) and the argument in part (3).

□

Remark 3. Theorem 3.5 tells us that under the conditions for part (2) of Theorem 3.7, $\operatorname{depth} R^G = 3$. However, the proof of part (2) does not demonstrate why the technique used cannot be extended to show that, for example,

$$x_1, x_1^{p-1}x_2 - x_2^p, \prod_{d=1}^{p} g^d(x_3), \prod_{d=1}^{p} g^d(x_4)$$

is a regular sequence. Set $I = \left(x_1, x_1^{p-1}x_2 - x_2^p, \prod_{d=1}^{p} g^d(x_3)\right) \subseteq R^G$. The proof technique fails in this case due to the fact that R^G/IR^G no longer injects into R/IR. As a specific example, consider $G = \mathbb{Z}/3\mathbb{Z}$ acting on $k[x_1, x_2, x_3]$ by the indecomposable action with $\operatorname{char} k = 3$. It is well known that

$$R^G = k\left[x_1, x_2^3 - x_1^2x_2, \prod_{d=1}^{3} g^d(x_3), x_2^2 - 2x_1x_3 - x_1x_2\right]$$

and $(x_2^2 - 2x_1x_3 - x_1x_2)^3 \equiv 0 \bmod IR^G$ while $(x_2^2 - 2x_1x_3 - x_1x_2)^3 \not\equiv 0 \bmod IR$.

3.2 Quasi-Gorenstein Rings of Invariants

We have established that many of the rings of invariants of interest to us are not Cohen-Macaulay. Failing to satisfy this property, we can ask how bad the structure of R^G can get. Recall when a ring T is of finite type over a field k, i.e. $T = k[x_1, \ldots, x_n]/I = S/I$ and T is equidimensional with $\dim T = d$, then we define the *canonical module of* T to be the T-module

$$\omega_T := \mathrm{Ext}_S^{n-d}(T, S).$$

If T is Cohen-Macaulay and $T \cong \omega_T$, we say that T is *Gorenstein.* If T is not Cohen-Macaulay but $T \cong \omega_T$ we say that T is *quasi-Gorenstein.* The quasi-Gorenstein property is nice for a variety of reasons. For example, when a local ring $(T, \mathfrak{m})$ admits a canonical module, we may apply local duality to investigate the local cohomology modules, $H^i_{\mathfrak{m}}(T)$, of T, i.e., we may translate questions regarding local cohomology to questions regarding ω_T. When T is quasi-Gorenstein, this technique becomes especially useful since if T is not Cohen-Macaulay, then it may have several non-zero local cohomology modules which are in general difficult to compute.

Recall, Noether demonstrated that R^G is of finite type over a field, whence R^G has a canonical module. Moreover, as R^G is normal, ω_{R^G} is unique up to isomorphism and is isomorphic to an unmixed ideal of height one in R^G, that is, ω_{R^G} can be identified with a divisor on $\mathrm{Spec}(R^G)$. We would like to determine what form the canonical module takes. As presentations of the canonical module are in general hard to construct we will take an abstract approach using representation theory to describe the structure of ω_{R^G} rather than give an explicit representation. In particular, we consider which of our groups have pseudo-reflections and make use of the following theorem.

Theorem 3.8. *[2, Nakajima, Corollary 3.9.3, page 38] If G is a finite group acting on a ring $R = k[x_1, \ldots, x_n]$ with k a field, then R^G is a unique factorization domain if and only if there are no non-trivial homomorphism $G \to k^\times$ taking the value 1 on every* *pseudo-reflection.*

Recall for a unique factorization domain T, the divisor class group of T is trivial. Given that ω_{R^G} can be identified with a divisor on $\mathrm{Spec}(R^G)$ showing that R^G is a unique factorization domain implies that R^G is quasi-Gorenstein. Our goal is therefore to apply Theorem 3.8 to the rings of invariants we are interested in. To this end, we first give some examples of what kind of pseudo-reflections can occur for $G = \mathbb{Z}/p^e\mathbb{Z}$. Recall that we use $\pi(g)$ to denote the representation of a generator $g \in G$.

Example 3.2. If $G = \mathbb{Z}/4\mathbb{Z}$ acts on $R = k[x, y, z]$ by the indecomposable action with $\operatorname{char} k = 2$, then we have

$$\pi(g)^2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and therefore $\operatorname{rank}(\pi(g)^2 - \mathrm{id}) = 1$. Thus $\pi(g)^2$ is a pseudo-reflection.

Example 3.3. Let $G = \mathbb{Z}/8\mathbb{Z}$ and $R = k[x_1, \ldots, x_n]$ with $\operatorname{char} k = 2$. Consider the action of G on R represented by $V_1 \oplus V_2$ with $\dim V_1 = 5$, $\dim V_2 = 2$, and the following Jordan block decomposition

$$\pi(g) = \left[\begin{array}{ccccc|cc} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

We have

$$\pi(g)^4 = \left[\begin{array}{ccccc|cc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

and therefore $\operatorname{rank}(\pi(g)^4 - \mathrm{id}) = 1$. Thus $\pi(g)^4$ is a pseudo-reflection.

Before giving a general characterization of which actions do not have pseudo-reflections, we introduce the following well-known theorem due to Lucas which we will use in the proof.

Theorem 3.9. *[24, Lucas, 1878] For non-negative integers u and n and a prime p, we have*

$$\binom{u}{n} \equiv \prod_{i=0}^{s} \binom{u_i}{n_i} \bmod p$$

where

$$u = u_0 + u_1 p^1 + u_2 p^2 + \cdots + u_s p^s$$

and

$$n = n_0 + n_1 p^1 + n_2 p^2 + \cdots + n_s p^s$$

are the base p expansions of u and n respectively.

We now demonstrate which actions of $G = \mathbb{Z}/p^e\mathbb{Z}$ do not have pseudo-reflections in both the decomposable and indecomposable case.

Theorem 3.10. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ with $\operatorname{char} k = p$ by the indecomposable action with $n > 2$. The representation $G \subseteq \mathrm{GL}_n(k)$ has an element that is a pseudo-reflection if and only if $n = p^{e-1} + 1$. More generally, if G acts on R with* *representation $V = V_1 \oplus \cdots \oplus V_\ell$, then G has a pseudo-reflection if and only if V_1 is the unique summand with $p^{e-1} < n_i \le p^e$ (i.e., $n_i \le p^{e-1}$ for all $i > 1$) and $n_1 = p^{e-1} + 1$.*

Proof. We first deal with the indecomposable action. Let $g \in G$ be a generator. Recall that,

$$g^m = \begin{bmatrix} 1 & \binom{m}{1} & \binom{m}{2} & \binom{m}{3} & \cdots & \binom{m}{n-1} \\ 0 & 1 & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{n-2} \\ 0 & 0 & 1 & \binom{m}{1} & \cdots & \binom{m}{n-3} \\ \vdots & \vdots & \vdots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \binom{m}{1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}. \tag{7}$$

and by Theorem 2.3, $p^{e-1} + 1 \le n \le p^e$, that is, $p^{e-1} \le n-1 \le p^e - 1$. It is an observation from (7) that if g^m is a pseudo-reflection, i.e. $\operatorname{rank}(g^m - \mathrm{id}) = 1$, then $\binom{m}{t} = 0$ for $1 \le t < n-1$ and $\binom{m}{n-1} \ne 0$. We will use Theorem 3.9 to show first that $m = cp^{e-1}$ for some $1 \le c \le p-1$ and then to show that we must have $n = p^{e-1} + 1$. If $t = p^j$ with $j < e-1$, then by Theorem 3.9

$$0 \equiv \binom{m}{t} \equiv \prod_{i=0}^{e} \binom{m_i}{t_i} \equiv \binom{m_e}{0}\binom{m_{e-1}}{0} \cdots \binom{m_t}{1} \cdots \binom{m_0}{0} \bmod p$$

where m_i is the ith digit in the base p representation of m and similarly for t. But this equation holds if and only if $\binom{m_t}{1} \equiv 0 \bmod p$, that is, $m_t = 0$ since $0 \le m_t < p$. Thus $m = cp^{e-1}$ with $1 \le c \le p-1$ or $m = p^e$. If $m = p^e$, then $g^m = \mathrm{id}$ is not a pseudo-reflection. Hence we must have $m = cp^{e-1}$, that is,

$$(m_e, m_{e-1}, \ldots, m_0) = (0, c, 0, \cdots, 0).$$

By Theorem 3.9

$$\binom{m}{n-1} \equiv \prod_{i=1}^{e} \binom{m_i}{n_i} \equiv \binom{0}{0}\binom{c}{(n-1)_{e-1}}\binom{0}{(n-1)_{e-2}}\cdots\binom{0}{(n-1)_0} \bmod p.$$

Thus we have $\binom{m}{n-1} \not\equiv 0 \bmod p$ if and only if

$$((n-1)_e, \ldots, (n-1)_0) = (0, q, 0, \cdots, 0)$$

for some $0 < q \leq c$. Moreover, if $q \neq 1$, then $\binom{m}{(q-1)p^{e-1}} \not\equiv 0 \bmod p$, whence $q = 1$. Thus $n - 1 = p^{e-1}$ and therefore $n = p^{e-1} + 1$ as desired. Conversely, if $n = p^{e-1} + 1$, then Theorem 3.9 and the formula above for g^m immediately gives $g^{p^{e-1}}$ is a pseudo-reflection.

For the more general case, with a representation of G given by $V_1 \oplus \cdots \oplus V_\ell$ and associated Jordan block decomposition

$$\pi(g) = \begin{bmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_\ell \end{bmatrix},$$

from Theorem 2.3, it suffices to note that a Jordan block can contribute a pseudo-reflection if and only if it is the unique Jordan block with dimension greater than p^{e-1} and, in particular, of dimension $p^{e-1} + 1$. $\square$

We make special note of the following corollary regarding the subgroup $H \leq G$ of pseudo-reflections which we will use in the proof of Theorem 4.10 regarding the structure of R^H.

Corollary 3.11. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ with $\operatorname{char} k = p$. Any pseudo-reflection of G is of the form $g^{cp^{e-1}}$ where $1 \leq c \leq p - 1$. Moreover, if $H \leq G$ is the subgroup of G generated by pseudo-reflections, then $H = \langle g^{p^{e-1}} \rangle$.*

Proof. The first claim follows from the proof of Theorem 3.10. The second claim follows from the fact that any generator of H is of the from $g^{cp^{e-1}} = \left(g^{p^{e-1}}\right)^c$ where $1 \leq c \leq p-1$, i.e. any pseudo-reflection may be written as $g'\left(g^{p^{e-1}}\right)$ for some $g' \in G$. □

Applying Theorem 3.8, we get the following corollary to Theorem 3.10 regarding R^G.

Corollary 3.12. *If $G = \mathbb{Z}/p^e\mathbb{Z}$ acts on $R = k[x_1, \ldots, x_n]$ with $n > 2$, then R^G is a unique factorization domain.*

Proof. If G does not contain any pseudo-reflections, then this follows immediately from Theorem 3.8. Thus we may assume that G has pseudo-reflections, i.e., $n = p^{e-1} + 1$. If $g \in G$ is a generator, then by Corollary 3.11, $g^{p^{e-1}}$ is a pseudo-reflection and the subgroup of pseudo-reflections is given by $H = \left\langle g^{p^{e-1}} \right\rangle$. Consider $G/H = \langle g \rangle / \left\langle g^{p^{e-1}} \right\rangle$. By Theorem 3.8, R^G is a unique factorization domain if and only if there are no non-trivial homomorphism $\varphi\colon G/H \to k^\times$. Assume such a non-trivial homomorphism exists. We have $G/H \cong \mathbb{Z}/p^{e-1}\mathbb{Z}$ via the map $\overline{g} \mapsto 1$. Thus any non-trivial homomorphism $\varphi\colon G/H \to k^\times$ gives a non-trivial one-dimensional representation of $G/H = \mathbb{Z}/p^{e-1}\mathbb{Z}$ which contradicts the relationship between p^{e-1} and the dimension of the representation required by Theorem 2.3. □

Remark 4. We note here that this gives a large collections of rings which are examples of unique factorization domains that are not Cohen-Macaulay.

Remark 5. Recall that the canonical module is isomorphic to an unmixed ideal of height 1 and can be identified with a divisor on $\operatorname{Spec}(R^G)$. With Corollary 3.12 in hand, we can see that $R^G \cong \omega_{R^G}$ by noting that once we know R^G is a unique factorization domain, it has trivial divisor class group as mentioned before. This implies that the canonical module for R^G has order 1, i.e., that R^G is quasi-Gorenstein. We give another proof with the next lemma utilizing duality.

Set S to be the set of primary invariants when $G = \mathbb{Z}/p^e\mathbb{Z}$ acts on $R = k[x_1, \ldots, x_n]$.

Recall, if G acts by the indecomposable action, then

$$S = \left\{ \prod_{d=1}^{\ell_i} g^d \cdot x_i \mid 1 \leq i \leq n, \ell_i = \min\{p^e \mid i \leq p^e\} \right\}.$$

If G is represented by $V_1 \oplus V_2 \oplus \cdots \oplus V_\ell$, then a set of primary invariants for R^G is given by $S = \{S_1, \ldots, S_\ell\}$ where each S_i is the set of primary invariants for V_i as above since each V_i is indecomposable. In either case, $k[S] \cong R$; in particular, $k[S]$ is Gorenstein, i.e. $k[S] = \omega_{k[S]}$. Since both R^G and $k[S]$ are normal domains and in particular, $k[S]$ is Gorenstein, it follows that

$$\omega_{R^G} \cong \mathrm{Hom}_{k[S]}(R^G, \omega_{k[S]}) \cong \mathrm{Hom}_{k[S]}(R^G, k[S])$$

We now will use the fact that R^G is a unique factorization domain to show explicitly that $R^G \cong \mathrm{Hom}_{k[S]}(R^G, k[S])$.

Lemma 3.13. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$. Let S denote the set of primary invariants for R^G. As R^G-modules, $R^G \cong \mathrm{Hom}_{k[S]}(R^G, k[S])$.*

Proof. Denote by $(-)^\vee := \mathrm{Hom}_{k[S]}(-, k[S])$, and consider $(R^G)^\vee$. As $k[S]$ and R^G are both domains, let $K \subseteq L$ be the corresponding fields of fractions. Let $R^G_L := R^G \otimes_{R^G} L$ and $R^G_K := R^G \otimes_{k[S]} K$. We have $(R^G)^\vee$ is reflexive as an $k[S]$-module. Moreover $\mathrm{rank}_{k[S]}(R^G) = \dim_K(R^G_K) = [L : K]$. To see this, let $b_1 \ldots, b_n$ be a basis in R^G for R^G_L over L and $a_1, \ldots, a_m$ a K-basis for L. We have $R^G_K = \langle b_1, \ldots, b_m\rangle \,/\, \langle a_1, \ldots, a_m\rangle$ as K-vector spaces and so $\dim_K(R^G_K) = \#(\langle b_1, \ldots, b_m\rangle \,/\, \langle a_1, \ldots, a_m\rangle) = [L : K]$. Moreover, since the basis for R^G_K over K gives a corresponding dual basis for $(R^G_K)^\vee$ over K, $\mathrm{rank}_{k[S]}(R^G) = \mathrm{rank}_{k[S]}((R^G)^\vee)$.

We now get $(R^G)^\vee$ is reflexive as a R^G-module and $\mathrm{rank}_{R^G}((R^G)^\vee) = \mathrm{rank}_{k[S]}((R^G)^\vee)/\,\mathrm{rank}_{k[S]}(R^G) = 1$ [4, Proposition 18(iii), Proposition 19, pp. 536-537]. Thus $(R^G)^\vee$ is reflexive and rank one, and so it is isomorphic to a divisorial ideal in the divisor class group of R^G [2, Lemma 3.4.1, p. 32]. But since R^G is a unique factorization domain, it follows that any divisorial ideal is principal, whence $(R^G)^\vee$ is free of rank one. $\square$

We now summarize what we know about the canonical module of R^G.

Theorem 3.14. *If $G = \mathbb{Z}/p^e\mathbb{Z}$ acts on $R = k[x_1, \ldots, x_n]$, then $\omega_{R^G} \cong R^G$.*

Proof. When $n \leq 2$, R^G is a polynomial ring. When $n > 2$, this follows from Corollary 3.12. $\square$

Remark 6. Theorem 3.14 gives us the ability to apply local duality when asking questions regarding the local cohomology of R^G. Applications will be given in Chapter 4.

3.3 F-Singularities of Cyclic Rings of Invariants

Having established that R^G is often not Cohen-Macaulay but always quasi-Gorenstein when $G = \mathbb{Z}/p^e\mathbb{Z}$ acts on $R = k[x_1, \ldots, x_n]$, we record some of the known restrictions this puts on their F-singularities.

Definition 3.2. Fix a ring R with $\mathrm{char}(R) = p > 0$. A *Frobenius operator* on an R-module M is a map $\varphi\colon M \to M$ satisfying $\varphi(rm) = r^{p^e}\varphi(m)$ for some $e > 0$.

This is equivalent to giving an $R\{F^e\}$-module structure to M where $R\{F^e\}$ is the non-commutative ring generated over R by F^e satisfying $F^e r = r^{p^e} F^e$. Such a Frobenius operator is said to have degree e. Denoting $\mathcal{F}^e(M)$ the set of all operators of degree e, construct the graded ring $\mathcal{F}(M)$ with degree e component $\mathcal{F}^e(M)$

$$\mathcal{F}(M) = \bigoplus_{i \in \mathbb{Z}_{\geq 0}} \mathcal{F}^i(M).$$

The graded ring $\mathcal{F}(M)$ is called the ring of Frobenius operators. For more information on rings of Frobenius operators and their importance, see [26].

It is natural to ask when $\mathcal{F}(M)$ is finitely generated over $\mathcal{F}^0(M)$. Of particular interest is when the module M is the local cohomology module $H_{\mathfrak{m}}^{\dim R}(R)$ or the injective hull of the residue field $E_R(R/\mathfrak{m}) = E$. We provide a simple example of this when R is a power series ring.

Example 3.4. If $R = k[[x_1, \ldots, x_n]]$, then $\mathcal{F}(E)$ is finitely generated over $\mathcal{F}^0(E)$ and the ring of Frobenius operators of $E = E_R(k)$ is given by

$$\mathcal{F}(E) = k[[x_1, \ldots, x_n]] \left\{ \frac{1}{(x_1 \cdots x_n)^{p-1}} F \right\}.$$

As R is Gorenstein, complete, normal, and local, by Proposition 4.1 of [19], $\mathcal{F}(E)$ is a finitely generated ring extension of $\mathcal{F}^0(E)$. In terms of Frobenius complexity, $\mathrm{cx}_F(R) = -\infty$. The canonical module for R is

$$\omega_R \cong (x_1 \cdots x_n)R,$$

and by Theorem 3.3 of [19],

$$\mathcal{F}(E) \cong \bigoplus_{e \geq 0} \omega^{(1-p^e)} F^e.$$

We have that $\omega^{(1-p^e)} = (x_1 \cdots x_n)^{1-p^e} R$. Thus

$$\mathcal{F}^e(E) = \frac{1}{(x_1 \cdots x_n)^{p^e - 1}} F^e.$$

If $q = p^e$ and $z \in E$, we have

$$\begin{aligned}
\frac{1}{(x_1 \cdots x_n)^{p-1}} F \circ \frac{1}{(x_1 \cdots x_n)^{q-1}} F^e(z) &= \frac{1}{(x_1 \cdots x_n)^{p-1}} F \circ \frac{(x_1 \cdots x_n)}{(x_1 \cdots x_n)^q} F^e(z) \\
&= \frac{1}{(x_1 \cdots x_n)^{p-1}} F\left((x_1 \cdots x_n) F^e\left(\frac{1}{(x_1 \cdots x_n)} z\right)\right) \\
&= \frac{(x_1 \cdots x_n)^p}{(x_1 \cdots x_n)^{p-1}} F\left(F^e\left(\frac{1}{(x_1 \cdots x_n)} z\right)\right) \\
&= (x_1 \cdots x_n) F^{e+1}\left(\frac{1}{(x_1 \cdots x_n)} z\right) \\
&= \frac{(x_1 \cdots x_n)}{(x_1 \cdots x_n)^{p^{e+1}}} F^{e+1}(z) = \frac{1}{(x_1 \cdots x_n)^{pq-1}} F^{e+1}(z),
\end{aligned}$$

which yields the desired result.

Notice, the key to the computation in Example 3.4 was that R was quasi-Gorenstein. In general, if $(R, \mathfrak{m})$ is a complete local ring with $\dim R = d > 0$ satisfying Serre's S_2 condition, then $\mathcal{F}(H^d_{\mathfrak{m}}(R)) \cong R\{F\}$, see Example 3.7 in [26]. The process of computing the ring of invariants commutes with completion at the homogeneous maximal ideal, i.e. $\widehat{R^G} \cong \widehat{R}^G$ for any finite group G, so we may consider R^G to be complete. We also want to show that $\widehat{R}^G$ satisfies S_2. It suffices to show that $\widehat{R}^G$ is normal, which follows by a similar argument to the proof of Theorem 2.1. Thus we get the following corollary of Theorem 3.14.

Corollary 3.15. *If $G = \mathbb{Z}/p^e\mathbb{Z}$ acts on $R = k[x_1, \ldots, x_n]$, then the ring of Frobenius operators of E is cyclic.*

We now consider other examples of singularities for rings of characteristic $p > 0$. We first give definitions for F-regularity and F-rationality.

Definition 3.3. Let R be a ring with $\operatorname{char} R = p > 0$. Let $F^e \colon R \to R$ denote the eth iteration of the Frobenius endomorphism, i.e. $r \mapsto r^{p^e}$. For a R-module M, we use $F^e_*(M)$ to denote the corresponding R-module coming from restriction of scalars for F^e. Thus if $m \in M$ and $r \in R$, then $F^e_*(m) \in F^e_*(M)$ and $r \cdot F^e_*(m) = F^e_*(r^{p^e} \cdot m)$.

1. We say R is *F-finite* if $F^e_*(R)$ is finitely generated over R.

2. Suppose R is an F-finite domain. If for every non-zero element $f \in R$ there exists $e \in \mathbb{N}$ and $\phi \in \mathrm{Hom}_R(F^e_*(R), R)$ such that $\phi(F^e_*(f)) = 1$, then we say R is *strongly F-regular*.

3. Suppose that R is a normal, Cohen-Macaulay ring and that $\phi_R : F^e_*(\omega_R) \to \omega_R$ is the canonical dual of Frobenius. We say that R has *F-rational singularities* if there are no non-zero proper submodules $M \subset \omega_R$ such that $\phi_R(F_*(M)) \subseteq M$.

Remark 7. In part (2) of this definition we call R strongly F-regular. There is a notion of weakly F-regular and it is conjectured that weak F-regularity implies strong F-regularity. When R is $\mathbb{N}$-graded, this was proved by Lyubeznik and Smith in [25]; the general case is still open. Since our rings of invariants are all $\mathbb{N}$-graded, no distinction is necessary and we will say R is F-regular instead of weakly or strongly F-regular.

The definitions given here are equivalent to the original definitions given for F-rational and F-regular singularities in Hochster and Huneke's theory of tight closure which we introduce here along with a result regarding tight closure which we will need originally proved by Smith.

Definition 3.4. Suppose that R is an F-finite domain and $I \subseteq R$ is an ideal. The tight closure of I is defined to be the set

$$I^* = \{z \in R \mid \text{ there exists } 0 \neq c \in R \text{ such that } cz^{p^e} \in I^{[p^e]}, e \geq 0\}.$$

1. [6, Definition 10.1.11, Defintion 10.3.1] Let R be an F-finite domain and $I \subseteq R$ an ideal. If R is F-regular, then $I = I^*$ for all ideals I. If R is local, then R is F-rational if and only if $I = I^*$ for all parameter ideals I.

2. [6, Proposition 10.1.5] If $R \subseteq S$ is a finite extension of rings, then $(IS) \cap R \subseteq I^*$ for all ideal $I \subseteq R$.

It is normal to ask when R^G is either F-regular or F-rational. In his dissertation, Jeffries characterized the case when $e = 1$.

Theorem 3.16. *[18, Jeffries] Let $G = \mathbb{Z}/p\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$. The ring of invariants R^G is F-regular if and only if R^G is F-rational if and only if $n = 2$ or G acts with representation $V_1 \oplus \cdots \oplus V_\ell$ where $n_1 = 2$ and $n_i = 1$ for $2 \leq i \leq \ell$.*

Since we have a complete characterization of the Cohen-Macaulay property for our rings of invariants we will use the following theorem to help determine F-regularity when $e > 1$.

Theorem 3.17. *[15, Hochster, Huneke] Let R be a ring of characteristic $p > 0$. If R is strongly F-regular, then R is Cohen-Macaulay and normal.*

It is clear that our rings of invariants are F-finite. Moreover, given the definition of F-rational singularities, our characterization of the Cohen-Macaulay property of R^G when $G = \mathbb{Z}/p^e\mathbb{Z}$ allows us to determine when R^G is not F-rational. Using Theorem 3.17, it is a straightforward application of Corollary 3.6 to see when R^G is neither F-regular nor F-rational. To give a complete characterization of these two types of singularities we need to consider when R^G is Cohen-Macaulay. By Corollary 3.6 we need only determine if R^G is F-rational or F-regular when $G = \mathbb{Z}/4\mathbb{Z}$ and $n = 3$.

Example 3.5. Let $G = \mathbb{Z}/4\mathbb{Z}$ act on $R = k[x, y, z]$ by the indecomposable action where $\operatorname{char} k = 2$. The ring of invariants R^G is neither F-rational nor F-regular.

Proof. We first note that it suffices to consider the indecomposable action since when G acts on R with representation $V_1 \oplus \cdots \oplus V_\ell$ where $n_1 = 3$ and R^G is Cohen-Macaulay, then $n_i = 1$ for $2 \leq i \leq \ell$. Moreover, R^G is Gorenstein and therefore R^G is F-regular if and only if R^G is F-rational. We show that R^G is not F-regular. Recall from Example 2.3 that

$$R^G = k[x, xy + y^2, z^4 + z^2x^2 + zyx^2 + z^2xy + z^2y^2 + zy^2x, xy^2 + y^3 + x^2z + xz^2].$$

Set $I = (x, xy + y^2, z^4 + z^2x^2 + zyx^2 + z^2xy + z^2y^2 + zy^2x) \subseteq R^G$. Notice

$$xy^2 + y^3 + x^2z + xz^2 \notin IR^G.$$

To see this, it suffices to show if $f \in IR^G$ with $\deg f = 3$, then $x \mid f$. Suppose $f \in IR^G$ with $\deg f = 3$, and note $f = g_0x + g_1(xy + y^2)$ where $g_0, g_1 \in R^G$. Since $\deg f = 3$, $\deg g_1 = 1$. Moreover, $g_1 = x$ since the only element of R^G with degree 1 is x. Thus $x \mid f$ as desired. Consider $IR = (x, y^2, z^4 - y^3z)R$. By direct calculation

$$\begin{aligned} xy^2 + y^3 + x^2z + xz^2 &\equiv y^3 \bmod xR \\ &\equiv 0 \bmod (x, y^2)R. \end{aligned}$$

Thus $xy^2 + y^3 + x^2z + xz^2 \in IR$. Since $xy^2 + y^3 + x^2z + xz^2 \in R^G$ with $xy^2 + y^3 + x^2z + xz^2 \notin IR^G$ and $xy^2 + y^3 + x^2z + xz^2 \in IR$, it follows from Definition 3.4 part (2) that $I \neq I^*$ and therefore by Definition 3.4 part (1), R^G is not F-regular. $\square$

Applying Corollary 3.6, Theorem 3.17, Example 3.5, and Theorem 3.16 result we get the following.

Corollary 3.18. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$. The ring of invariants R^G is F-rational if and only if R^G is F-regular if and only if $n = 2$ or G acts by representation $V_1 \oplus \cdots \oplus V_\ell$ with $n_1 = 2$ and $n_i = 1$ for $2 \leq i \leq \ell$.*

Proof. For the case of $e = 1$, this is Theorem 3.16. Suppose $e > 1$. By Theorem 3.17 we only need to check R^G is not Cohen-Macaulay. Moreover by Corollary 3.6 we only need to check the case of $p = 2$ and $e = 2$ which is Example 3.5. $\square$

Recall, if $R \subseteq S$ is a split inclusion of rings and S is F-regular or F-rational then R is F-regular or F-rational respectively. In his dissertation, Chan showed that for a group G with $P \leq G$ a normal p-Sylow subgroup, the inclusion $R^G \subseteq R^P$ is a split inclusion resulting in the following.

Theorem 3.19. *[8, Chan] Let $G \leq \mathrm{GL}_n(k)$ act on $R = k[x_1, \ldots, x_n]$ where $\operatorname{char} k = p$. Let $H \leq G$ be a p-Sylow subgroup of G.*

1. *If R^H is F-regular, then R^G is F-regular.*
2. *If R^H is F-rational, then R^G is F-rational.*

Using this along with Corollary 3.18 we immediate get the following characterization of F-regularity and F-rationality for certain rings of invariants.

Corollary 3.20. *Let $G \leq \mathrm{GL}_n(k)$ act on $R = k[x_1, \ldots, x_n]$ where $\operatorname{char} k = p$. Suppose $H = \mathbb{Z}/p^e\mathbb{Z}$ is a normal p-Sylow subgroup of G. If $n = 2$ or H acts by representation $V_1 \oplus \cdots \oplus V_\ell$ with $n_1 = 2$ and $n_i = 1$ for $2 \leq i \leq \ell$, then R^G is F-regular and F-rational.*

Proof. Under the conditions of the hypothesis, R^H is F-rational and F-regular by Corollary 3.18 so we can apply Theorem 3.19. □

4 Rings of Invariants of Subgroups of $\mathbb{Z}/p^e\mathbb{Z}$

Throughout the section, set $R = k[x_1, \dots, x_n]$ with $\operatorname{char} k = p$, $G = \mathbb{Z}/p^e\mathbb{Z}$, $g \in G$ a generator, and R^G the ring of invariants. If $H \leq G$ is a subgroup, then H acts naturally on R and induces an inclusion of rings $R^G \subseteq R^H$. Recall the Jordan-Hölder filtration of G given by

$$0 = N_e \leq N_{e-1} \leq \cdots \leq N_1 \leq N_0 = G$$

where $N_i = \langle g^{p^i} \rangle$. This yields a chain of subrings of R which are rings of invariants, i.e.,

$$R^G \subseteq R^{N_1} \subseteq \cdots \subseteq R^{N_{e-1}} \subseteq R.$$

Our goal is to study R^G by studying these intermediate subrings.

4.1 Graded Duality and the a-invariant

In this section, we recall an invariant which is useful when determining when a ring has certain F-singularities. For a local ring S and an ideal I, denote by $H^n_I(S)$ the nth local cohomology module of S with respect to I. For details on local cohomology see [17].

Definition 4.1. Let S be a positively graded k-algebra with $\dim S = d$ where k is a field. We define the a-invariant of S to be

$$a(S) := \max\{t \mid (H^d_{\mathfrak{n}}(S))_t \neq 0\}$$

where $\mathfrak{n}$ is the homogeneous maximal ideal of S.

Remark 8. Suppose that S admits a canonical module, ω_S. Let E be the injective hull of the residue field of S and $d = \dim S$. By local duality,

$$H^d_{\mathfrak{n}}(S) \cong \operatorname{Hom}_S(\operatorname{Ext}^{d-d}_S(S, \omega_S), E) \cong \operatorname{Hom}_S(\operatorname{Hom}_S(S, \omega_S), E) \cong \operatorname{Hom}_S(\omega_S, E).$$

Elements in $(H^d_{\mathfrak{n}}(S))_t$ are in correspondence with S-linear maps $(\omega_S)_{-t} \to E$. Thus $(H^d_{\mathfrak{n}}(S))_t \neq 0$ if and only if there exists a non-zero map $(\omega_S)_{-t} \to E$ which happens if and only if $(\omega_S)_{-t} \neq 0$. Thus

$$a(S) = \max\{t \mid (H^d_{\mathfrak{n}}(S))_t \neq 0\} = \max\{t \mid (\omega_S)_{-t} \neq 0\}.$$

We use this formulation when giving bounds on the a-invariant for certain rings of invariants.

The a-invariant has relationships to F-singularities. For example, if S is F-rational, then $a(S) < 0$, see Exercise 10.3.28, page 405, [6]. This reduces the calculation in Example 3.5 to showing that the a-invariant for R^G is greater than or equal to 0. Indeed, R^G in Example 3.5 is Gorenstein and therefore isomorphic to $S = k[a, b, c, d]/(f)$ where $f \in k[a, b, c, d]$ whence an application of Remark 8 shows $3 \leq a(R^G) \leq 4$ which proves R^G is not F-rational.

Our first goal is to relate the a-invariant of R^G with the a-invariant of R^H where $H \leq G$ is a subgroup of G. In the case where R^G is Cohen-Macaulay, we have the following.

Theorem 4.1. *[18, Jeffries] Let k be a field and $R = k[x_1, \ldots, x_n]$ be a polynomial ring. Let G be a finite subgroup of* $\mathrm{GL}(V)$ *and $H \leq G$ a subgroup acting naturally on R. If R^G and R^H are Cohen-Macaulay, then the inequality $a(R^G) \leq a(R^H)$ holds.*

As R^G is rarely Cohen-Macaulay when $G = \mathbb{Z}/p^e\mathbb{Z}$, we would like to establish bounds on the a-invariant independent of the Cohen-Macaulay hypothesis. To do so, we utilize graded duality. Recall for a noetherian graded ring S and M, N S-modules, we define the graded S-module

$$\underline{\mathrm{Hom}}_S(M, N) := \oplus_{n \in \mathbb{Z}} \underline{\mathrm{Hom}}_S(M, N)_n$$

where $\underline{\mathrm{Hom}}_S(M, N)_n$ is the abelian group of homomorphisms of M into $N(n)$. If, in addition, S is quasi-Gorenstein, then we have the following well-known graded duality result.

Lemma 4.2. *If S is a graded ring that admits a cyclic canonical module, ω_S, then $\underline{\mathrm{Hom}}_S(S, \omega_S) \cong \omega_S$.*

Proof. Since ω_S is free of rank one, we have $\omega_S \cong S(-a)$ as graded modules. By direct calculation

$$\begin{aligned}
\underline{\mathrm{Hom}}_S(S, \omega_S) &= \oplus_{n \in \mathbb{Z}} \underline{\mathrm{Hom}}_S(S, \omega_S)_n \\
&\cong \oplus_{n \in \mathbb{Z}} \underline{\mathrm{Hom}}_S(S, S(-a))_n \\
&\cong \oplus_{n \in \mathbb{Z}} S_{n-a} \\
&\cong \oplus_{n \in \mathbb{Z}} (S(-a))_n \\
&\cong \oplus_{n \in \mathbb{Z}} (\omega_S)_n \\
&= \omega_S.
\end{aligned}$$

□

By Theorem 3.14, R^G is quasi-Gorenstein, i.e., $R^G \cong \omega_{R^G}$ where ω_{R^G} is the canonical module for R^G. In particular $\omega_{R^G} \cong R^G(a)$ as graded modules, where a represents a graded shift, i.e., $(R^G(a))_n = (R^G)_{a+n}$, that is, ω_{R^G} is cyclic. A direct application of Lemma 4.2 gives the following.

Corollary 4.3. *If $G = \mathbb{Z}/p^e\mathbb{Z}$ acts on $R = k[x_1, \ldots, x_n]$, then $\underline{\mathrm{Hom}}_{R^G}(R^G, \omega_{R^G}) \cong \omega_{R^G}$.*

Let $H \leq G$ be a subgroup acting naturally on R so that $R^G \subseteq R^H$. We want to show R^H is a unique factorization domain so that we can establish R^H is quasi-Gorenstein. By Lemma 3.8, to show that the ring of invariants R^H is a unique factorization domain, it suffices to show that any homormophism $\varphi\colon H \to k^\times$ such that $\varphi(x) = 1$ for all pseudo-reflections $x \in H$ is trivial. We will use the fact that R^H is quasi-Gorenstein to apply graded duality in the proof of the main result in this subsection.

Lemma 4.4. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ with $g \in G$ a generator. If $H \leq G$ is a subgroup acting naturally on R, then R^H is a unique factorization domain.*

Proof. It suffices to note that for any subgroup $H \leq G$, $H \cong \mathbb{Z}/p^d\mathbb{Z}$ for some $d \leq e$ so we may apply Corollary 3.12. $\square$

We now give some examples where H contains pseudo-reflections.

Example 4.1. Let $p = 3$ and $e = 2$ so that $G = \mathbb{Z}/9\mathbb{Z}$ and let $\operatorname{char} k = 3$. Let $g \in G$ be a generator. For G to have pseudo-reflections when acting by the indecomposable action, by Theorem 3.10, we need $n = 4$. There are two pseudo-reflections in G given by

$$h_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } h_2 = \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Notice $h_1^2 = h_2$ and $h_2^2 = h_1$. Thus if $H \leq G$ is a subgroup and $h_1 \in H$, then $h_2 \in H$ and vice versa. Let $H \leq G$ be a proper non-zero subgroup. We have $\#H = 3$ and $h = g^3 \in H$ is a generator for H. Thus $h = h_1$ and any homomorphism $\varphi\colon H \to k^\times$ with $\varphi(h_1) = 1$ is trivial.

Example 4.2. Let $p = 5$ and $e = 2$ so that $G = \mathbb{Z}/25\mathbb{Z}$ and let $\operatorname{char} k = 5$. Let $g \in G$ be a generator. By Theorem 3.10, in order for G to have pseudo-reflections we must have $n = 6$. There are four pseudo-reflections in G given by

$$h_c = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

where $c \in k^\times$. By direct calculation

$$h_2^3 = h_1, h_3^2 = h_1, h_4^4 = h_1.$$

Thus any subgroup $H \leq G$ which contains a pseudo-reflection must contain h_1 and consequently all of the h_i. Let $H \leq G$ be a proper non-zero subgroup. We have $\#H = 5$ and

$$h = g^5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \in H$$

is a generator for H. Thus $h_1 = h$ and it is clear that any homomorphism $\varphi\colon H \to k^\times$ such that $\varphi(h_c) = 1$ for all c is trivial.

Example 4.3. Let $p = 3$ and $e = 3$ so that $G = \mathbb{Z}/27\mathbb{Z}$ and let $\operatorname{char} k = 3$. Let $g \in G$ be a generator. If we want G to have pseudo-reflections, by Theorem 3.10 we must have $n = 10$.

There are two pseudo-reflections in G given by

$$h_c = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

where $c = 1, 2$. Notice $h_1^2 = h_2$ and $h_2^2 = h_1$ so that if $h_1 \in H$ then $h_2 \in H$ and vice versa. If $H \leq G$ is a proper non-zero subgroup $\#H = 3$ or $\#H = 9$. If $\#H = 3$ then $h = g^9 = h_1$ is a generator for H and it is clear that any homomorphism $\varphi\colon H \to k^\times$ such that $\varphi(h_1) = 1$ for all c is trivial. Suppose $\#H = 9$. We have

$$h = g^3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

is a generator for H. By direct calculation $h^3 = h_1$ and $h^6 = h_2$. If $\varphi\colon\ H \to k^\times$ such that $\varphi(h_1) = 1$ then

$$1 = \varphi(h^3) = \varphi(h)^3 = \varphi(h),$$

that is φ is trivial.

Example 4.4. Let $p = 3$ and $e = 2$ so that $G = \mathbb{Z}/9\mathbb{Z}$ and let $\operatorname{char} k = 3$. Let $g \in G$ be a generator with representation

$$\pi(g) = \left[\begin{array}{cccc|cc|cc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

so that the Jordan Block decomposition of g satisfies the requirements of Theorem 3.10. There are two pseudo-reflections in G given by

$$h_1 = \left[\begin{array}{cccc|cc|cc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right] \text{ and } h_2 = \left[\begin{array}{cccc|cc|cc} 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

satisfying $h_1^2 = h_2$ and $h_2^2 = h_1$. Thus if $H \le G$ and $h_1 \in H$ then $h_2 \in H$ and vice versa. If $H \le G$ is a proper nonzero subgroup, then $\#H = 3$ and $h = g^3 = h_1$ is a generator for H. Thus any homomorphism $\varphi\colon H \to k^\times$ such that $\varphi(x) = 1$ for all pseudo-reflections $x \in H$ is trivial. Moreover, by Theorem 3.8, R^H is a unique factorization domain.

We now highlight some consequences of Lemma 4.4 which we will need to give a relationship between $a(R^G)$ and $a(R^H)$.

Corollary 4.5. *If $H \le G$ is a subgroup acting naturally on R, then $\omega_{R^H} \cong R^H$, $\underline{\mathrm{Hom}}_{R^H}(R^H, \omega_{R^H}) \cong \omega_{R^H}$ and $(R^H)^\vee \cong \omega_{R^H}$ where we define*

$$(-)^\vee = \underline{\mathrm{Hom}}_{R^G}(-, R^G).$$

Proof. By Lemma 4.4 the divisor class group of R^H is trivial and it follows that ω_{R^H} is free of rank one. The second claim follows immediately from Lemma 4.2. For the third part, since R^H is a finitely generated R^G-module,

$$\omega_{R^H} \cong \underline{\mathrm{Ext}}_{R^G}^{\dim R^G - \dim R^H}(R^H, \omega_{R^G})$$

where $\underline{\mathrm{Ext}}^i_{R^G}(-, \omega_{R^G})$ is the graded ith right derived functor of $(-)^\vee$. As R^G and R^H are both normal subrings of R, we get $\dim R^G = \dim R^H$ whence
$\omega_{R^H} \cong \underline{\mathrm{Ext}}^0_{R^G}(R^H, \omega_{R^G}) \cong (R^H)^\vee$ as desired. □

There are well-known invariants which we use in the proof of our next result defined as follows.

Definition 4.2. Let G be a finite group acting on $S = k[x_1, \dots, x_n]$. For $f \in S$, we define the *transfer of f* by

$$\mathrm{Tr}(f) := \sum_{g \in G} g(f).$$

Moreover, given a normal subgroup H we define the *relative transfer map* $\operatorname{Tr}_H^G\colon S^H \to S^G$ by

$$\varphi(f) = \sum_{\overline{g} \in G/H} \overline{g}(f).$$

Notice the transfer of an element $f \in R$ is related the Reynold's operator defined earlier. Although it does not provide a splitting, we demonstrate here that it is still useful. We are now ready to prove a result analogous to Theorem 4.1 which is independent of the Cohen-Macaulay hypothesis.

Theorem 4.6. *If $H \leq G = \mathbb{Z}/p^e\mathbb{Z}$ is a subgroup acting naturally on R, then $a(R^G) \leq a(R^H)$.*

Proof. Let $L = \operatorname{frac} R$ and L^G be the subfield of L consisting of elements fixed by G acting on L. We claim that L/L^G is Galois. Indeed since G is a finite subgroup of automorphisms of L and L^G is the fixed field, every automorphism of L fixing L^G is contained in G, that is, $\operatorname{Aut}(L/L^G) = G$ so that L/L^G is a Galois with Galois group G. By the Fundamental Theorem of Galois, there is an order reversing bijective correpondence between subfields of L and subgroups of G. In particular $\overline{g} \in G/H$ acts on L and $\overline{g}(L^H) \subseteq L^H$ where L^H is the subfield of L fixed by H. Moreover, $\overline{g}\colon (L^G)^\times \to (L^H)^\times$ is an embedding, i.e., is a character of $(L^G)^\times$. Since the $\overline{g}$ are distinct equivalence classes, this gives that they are linearly independent over L^H and hence they are linearly independent over L^G. Recall the relative transfer map $\operatorname{Tr}_H^G\colon R^H \to R^G$, given by

$$\operatorname{Tr}_H^G(r) = \sum_{\overline{g} \in G/H} \overline{g}(r).$$

Since the $\overline{g}$ are linearly independent over L^G, it follows that Tr_H^G is not the zero map. Set $(-)^\vee = \underline{\operatorname{Hom}}_{R^G}(-, \omega_{R^G})$ and consider the exact sequence

$$R^H \xrightarrow{\operatorname{Tr}_H^G} R^G \to R^G/\operatorname{Tr}_H^G(R^H) \to 0. \tag{8}$$

Since $\operatorname{Tr}_H^G \neq 0$, it follows that $R^G/\operatorname{Tr}_H^G(R^H)$ is a torsion module and therefore $(R^G/\operatorname{Tr}_H^G(R^H))^\vee = 0$. Thus applying $(-)^\vee$ to (8) we get

$$\begin{tikzcd}
0 \arrow[r] & (R^G)^\vee \arrow[r, "(\operatorname{Tr}_H^G)^\vee"] \arrow[d, "\cong"] & (R^H)^\vee \arrow[d, "\cong"] \\
0 \arrow[r] & \omega_{R^G} \arrow[r] & \omega_{R^H}
\end{tikzcd}$$

where the vertical isomorphisms follow from Corollaries 4.3 and 4.5. It follows that

$$a(R^G) = \max\{t \mid (\omega_{R^G})_{-t} \neq 0\} \leq \max\{t \mid (\omega_{R^H})_{-t} \neq 0\} = a(R^H).$$

□

We immediately get the following corollary of Theorem 4.6.

Corollary 4.7. *If $H \leq G = \mathbb{Z}/p^e\mathbb{Z}$ is a subgroup acting naturally on R and $N \leq H$ is a subgroup acting naturally on R, then $a(R^H) \leq a(R^N)$.*

Proof. Any subgroup $H \leq G$ is a cyclic p-group of order p^i with $0 \leq i \leq e$. □

As an immediate consequence of Corollary 4.7 and Corollary 4.5 setting $G = \mathbb{Z}/p^e\mathbb{Z}$ we have the following.

Corollary 4.8. *If $0 = N_e \leq N_{e-1} \leq \cdots \leq N_1 \leq N_0 = G = \mathbb{Z}/p^e\mathbb{Z}$ is a composition series of subgroups acting naturally on R, then*

$$a(R^G) \leq a(R^{N_1}) \leq \cdots \leq a(R^{N_{e-1}}) \leq a(R).$$

Proof. For each $1 \leq i \leq e$, N_{i-1} is a subgroup of N_i acting naturally on R and each N_i is quasi-Gorenstein by Corollary 4.5 whence $a(R^{N_{i-1}}) \leq a(R^{N_i})$. □

More generally, if G is a group with $\mathbb{Z}/p^e\mathbb{Z} = H \leq G$ a unique p-Sylow subgroup and R^G quasi-Gorenstein, we can combine this with Theorem 4.6 to get the following.

Corollary 4.9. *Let G be a group with $\mathbb{Z}/p^e\mathbb{Z} = H \leq G$ a unique p-Sylow subgroup and R^G quasi-Gorenstein. Suppose G acts on a ring R with* $\operatorname{char} R = p > 0$. *If* $0 = N_e \leq N_{e-1} \leq \cdots \leq N_1 \leq N_0 = H$ *is a composition series of subgroups acting naturally on R, then*

$$a(R^G) \leq a(R^H) \leq a(R^{N_1}) \leq \cdots \leq a(R^{N_{e-1}}) \leq a(R).$$

Proof. We only need to prove the inequality $a(R^G) \leq a(R^H)$ as the other inequalities follow from Corollary 4.8. Define $(-)^\vee = \underline{\operatorname{Hom}}_{R^G}(-, R^G)$. Since R^G is quasi-Gorenstein, $(R^G)^\vee \cong \omega_{R^G}$. Since $\dim R^G = \dim R^H$ and R^H is a finitely generated R^G-module, it follows that

$$\omega_{R^H} \cong \underline{\operatorname{Ext}}_{R^G}^{\dim R^G - \dim R^H}(R^H, \omega_{R^G}) \cong \underline{\operatorname{Ext}}^0_{R^G}(R^H, \omega_{R^G}) \cong (R^H)^\vee.$$

Using the same Galois theory argument as in the proof of Theorem 4.6, $\operatorname{Tr}_H^G \neq 0$. The rest of the proof follows exactly as in the proof of Theorem 4.6. $\square$

Example 4.5. Let $G = \mathbb{Z}/9\mathbb{Z}$ act on $R = k[x, y, z, w]$ by the indecomposable action with $\operatorname{char} k = 3$. Let $g \in G$ be a generator and $H = \langle g^3 \rangle \leq G$. By direct computation,

$$\pi(g^3) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

We have $R^H = k[x, y, z, x^2w - w^3]$ which is isomorphic to a polynomial ring. Moreover $a(R^H) = 4$ and by Corollary 4.8, $a(R^G) \leq 4$.

Remark 9. When k is a perfect field, the results in this section regarding the a-invariant are an example of a more general result given in Theorem 1.1(1) of [23]. In particular, Theorem 1.1(1) of [23] says that if $A \subseteq B$ is an integral extension of positively graded, noetherian domains over a field k, where A is regular in codimension 1 and $\operatorname{frac}(A) \subseteq \operatorname{frac}(B)$, then $a(A) \leq a(B)$. If we consider $R^H \subseteq R^N$ as in Theorem 4.7, the fact that R^H is normal implies the first hypothesis and the second hypothesis follows from the fact that $\operatorname{frac}(R^N)/\operatorname{frac}(R^H)$ is a Galois extension with Galois group $(G/H)/(G/N)$. The proof in [23] is quite technical and requires the module of kähler differentials to show there is an inclusion $\omega_A \hookrightarrow \omega_B$. In our case we avoid this technicality and give a simpler proof relying on the representation theory for G. Moreover, we do not require k to be perfect.

4.2 A Structure Theorem for R^H with $H \leq G$

In this subsection we use changes of basis to recognize an explicit filtration of $R = k[V]$ in terms of representations associated to subgroups $H \leq G$. We begin with an explicit example to show the types of change of basis we will use. For ease of notation, throughout this subsection when we write V_i we mean the vector space has dimension i, that is, $\dim_k V_i = i$.

Example 4.6. Let $G = \mathbb{Z}/4\mathbb{Z}$ act on $R = k[x, y, z]$ by the indecomposable action with $\operatorname{char} k = 2$. Let $H \leq G$ be the subgroup of G generated by pseudo-reflections. For $g \in G$ a generator, $H = \langle g^2 \rangle$ and setting $h = g^2$, $H = \{h, \mathrm{id}\}$. Consider the map $\varphi\colon V_3 \to V_3$ defined by $e_1 \mapsto e_1$, $e_2 \mapsto e_2 + e_1$ and $e_3 \mapsto e_3 + e_1$ where e_1, e_2, e_3 is a basis for V_3. It is clear φ is an automorphism of V_3. We claim that this change of basis gives us an equivalence between H acting on R naturally and H acting on R with representation $V_2 \oplus V_1$. The representation for $\varphi(h)$ is given by

$$\varphi(h) = \varphi\left(\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

We check that this change of basis preserves the group action. By direct calculation

$$\begin{aligned}
&\varphi(h(e_1)) = \varphi(e_1) = e_1 = h(e_1) = h(\varphi(e_1)),\\
&\varphi(h(e_2)) = \varphi(e_2) = e_2 + e_1 = h(e_2 + e_1) = h(\varphi(e_2)) \text{ and}\\
&\varphi(h(e_3)) = \varphi(e_3 + e_1) = (e_3 + e_1) + e_1 = h(e_3 + e_1) = h(\varphi(e_3)).
\end{aligned}$$

Throughout this section we use changes of bases in the same manner as Example 4.6. As the process of checking the equivalence of group actions will be exactly the same we will omit the computation when it is clear. We have the following result regarding $H \leq G$ the subgroup consisting of all pseudo-reflections.

Theorem 4.10. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ such that the representation of G contains a pseudo-reflection. If $H \leq G$ is the subgroup of G generated by pseudo-reflections, then R^H is a polynomial ring.*

Proof. We start with the case where G acts on R by the indecomposable representation. By Theorem 3.10, we must have $n = p^{e-1} + 1$. Moreover, $h = g^{p^{e-1}}$ is a pseudo-reflection and a generator for H by Corollary 3.11. The induced action on R by $\pi(h)$ is given by

$$x_1 \mapsto x_1 \quad x_2 \mapsto x_2 \quad \cdots \quad x_{n-1} \mapsto x_{n-1} \quad x_n \mapsto x_n + x_1.$$

We claim the natural action of H on R is equivalent to H acting on R with representation $V_2 \oplus V_1 \oplus \cdots \oplus V_1$. Indeed the change of basis $x_i \mapsto x_i$ for $i \neq 2, n$ and $x_2 \mapsto x_2 + x_1$, $x_n \mapsto x_n + (p-1)x_1$, preserves the action of H on R and gives the desired equivalence. This gives $R^H = k[x_1, \ldots, x_{n-1}, x_n^p - x_1^{p-1}x_n]$ which we claim is isomorphic to a polynomial ring. We have $\dim R^H = n$ and R^H has n homogeneous generators, i.e., $S = \{x_1, \ldots, x_{n-1}, x_n^p - x_1^{p-1}x_n\}$ is a set of primary invariants. Thus R^H is its own Noether Normalization and the elements of S are linearly independent over k. Consider the map $\varphi\colon\ k[y_1, \ldots, y_n] \to R^H$ defined by $y_i \mapsto x_i$ for $i = 1, \ldots, n-1$ and $y_n \mapsto x_n^p - x_1^{p-1}x_n$. It is clear that φ is a surjective map of k-algebras so it suffices to show that $\ker\varphi = 0$ which follows from the fact that $\dim k[y_1,\ldots,y_n] = \dim R^H$.

If G acts on R by a decomposable action with representation $V_{j_1} \oplus \cdots \oplus V_{j_\ell}$, then by Theorem 3.10, up to change of basis we must have $j_1 = p^{e-1}+1$ and $j_i \leq p^{e-1}$ for $i = 2,\ldots,\ell$. Set J_{j_i} to be the Jordan block associated to V_{j_i} in the Jordan block decomposition of a representation for $g \in G$ a generator. If $x \in G$ is any pseudo-reflection, then by Corollary 3.11, $x = g^{cp^{e-1}}$. Moreover, by direct calculation, $J_{j_i}^{cp^{e-1}} = \left(J_{j_i}^{p^{e-1}}\right)^c = \mathrm{id}_{j_i}$ for $i = 2,\ldots,\ell$. The result now follows from the indecomposable case. $\square$

Remark 10. There is a more general version of this theorem due to Broer which builds on work of Kemper and Malle and generalizes the well-known Chevalley-Shephard-Todd Theorem [5]. The theorem states that if G is an irreducible group generated by pseudo-reflections acting on a ring of dimension n, then R^G is generated by n algebraically independent elements if and only if there is a surjective map $\varphi : k[V] \to k[V]^G$. Working in the specific case of the pseudo-reflection subgroup of a cyclic p-group allows us to use the known representations of the pseudo-reflections to show that R^G is a polynomial ring rather than using Kemper and Malle's classification of non-coregular rings of invariants for irreducible pseudo-reflection groups.

Here are two illustrative examples.

Example 4.7. Let $p = 3$, $e = 2$, and $n = 4$ so that $G = \mathbb{Z}/9\mathbb{Z}$ and let $\operatorname{char} k = 3$. We have

$$\pi(g) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let $H \leq G$ be the subgroup of G generated by pseudo-reflections. Note, $\#H = 3$ and H is generated by $h = g^3$ with representation

$$\pi(h) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

We apply the change of basis, φ, described in the proof of Theorem 4.10 which is given by

$$x_1 \mapsto x_1 \quad x_2 \mapsto x_2 + x_1 \quad x_3 \mapsto x_3 \quad x_4 \mapsto x_4 + 2x_1.$$

Thus

$$\varphi(\pi(h)) = \left[\begin{array}{cc|c|c} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right].$$

from which we observe $R^H = k[x, y^3 - x^2y, z, w]$, that is, R^H is isomorphic to a polynomial ring.

Example 4.8. Let $p = 3$ and $e = 2$ so that $G = \mathbb{Z}/9\mathbb{Z}$ and let $\operatorname{char} k = 3$. Let $g \in G$ be a generator with representation as given in Example 4.4, i.e. G is represented by $V_4 \oplus V_2 \oplus V_2$. If $H \leq G$ is the subgroup generated by pseudo-reflections, then $g^3 = h_1 \in H$ is a generator. Applying the change of basis φ, given by $x_i \mapsto x_i$ if $i \neq 2, 4$ and

$$x_2 \mapsto x_2 + x_1, \quad x_4 \mapsto x_4 + 2x_1$$

we get

$$\varphi(h_1) = \left[\begin{array}{cc|cccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

This gives $R^H = k[x_1, x_2^3 - x_1^2 x_2, x_3, \ldots, x_8]$ which is isomorphic to a polynomial ring. Notice, the change of basis in this case was the identity map on elements of J_i with $i \neq 1$.

We would like to determine the structure of all the subgroups of G in a manner similar to Theorem 4.10. For $H \leq G$ any subgroup, this will allows us to say, for example, whether R^H is Cohen-Macaulay. We will start by considering $H \leq G$ with $\#H = p$. In this case if $g \in G$ is a generator, then $h = g^{p^{e-1}} \in H$ is a generator. More generally, if $G = \mathbb{Z}/p^e\mathbb{Z}$ with $e > 2$, then we can consider $H \leq G$ with $\#H = p^d$ where $1 \leq d < e$. If $\#H = p^d$, then given $g \in G$ a generator, we have $h = g^{p^{e-d}} \in H$ is a generator. Thus to get similar results for larger subgroups of G we will be able to apply the same techniques as the case when $d = 1$.

Theorem 4.11. *Let G act on $R = k[x_1, \ldots, x_n]$ by the indecomposable action. Let $H \leq G$ with $\#H = p$ act naturally on R.*

1. *If $n = p^{e-1} + 2$, then R^H is Cohen-Macaulay.*

2. *If $p^{e-1} + 2 < n \leq 2p^{e-1}$, then the natural action of H on R is equivalent to H acting on R with representation $V_2^{n-p^{e-1}} \oplus V_1^{2p^{e-1}-n}$.*

3. *If $mp^{e-1} < n \leq (m+1)p^{e-1}$ with $2 \leq m \leq p-1$, then the natural action of H on R is*

equivalent to H acting on R with representation

$$V_{m+1}^{n-mp^{e-1}} \oplus V_m^{(m+1)p^{e-1}-n}.$$

Proof. Throughout the proof let $g \in G$ be a generator so that $h = g^{p^{e-1}} \in H$ is a generator.

1. If $p = 2$ and $e = 2$, then $n = p^{2-1} + 2 = 4$, i.e., we need only consider $n \geq 4$. The generator $h = g^{p^{e-1}} \in H$ has representation given by

$$\pi(h) = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & & & \ddots & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

When $n > 5$, after the change of basis $x_i \mapsto x_i$ for $i \neq 2, 4, n-1, n$ and

$$x_2 \mapsto x_2 + x_1, \quad x_4 \mapsto x_4 + x_3, \quad x_{n-1} \mapsto x_{n-1} + (p-1)x_1, \quad x_n \mapsto x_n + (p-1)x_2,$$

R^H is isomorphic to the ring of invariants of H acting on R with representation $V_2 \oplus V_2 \oplus V_1^{n-4}$ which is Cohen-Macaulay by Corollary 3.6.

If $n = 4$, use the change of basis

$$\begin{aligned} x_1 &\mapsto x_1, \\ x_2 &\mapsto x_2 + x_1, \\ x_3 &\mapsto x_3 + (p-1)x_1, \\ x_4 &\mapsto x_4 + x_3 + (p-1)x_2, \end{aligned}$$

which gives R^H is isomorphic to the ring of invariants of H acting on R with representation $V_2 \oplus V_2$. If $n = 5$, use the change of basis

$$
\begin{aligned}
x_1 &\mapsto x_1, \\
x_2 &\mapsto x_2 + x_1, \\
x_3 &\mapsto x_3, \\
x_4 &\mapsto x_4 + x_3 + (p-1)x_1, \\
x_4 &\mapsto x_5 + (p-1)x_2.
\end{aligned}
$$

which gives R^H is isomorphic to the ring of invariants of H acting on R with representation $V_2 \oplus V_2 \oplus V_1$. In either case, Corollary 3.6 gives R^H is Cohen-Macaulay.

2. The action of h on R is given by

$$
h(x_i) = \begin{cases} x_i, & i = 1, \ldots, p^{e-1}, \\ x_i + x_{i-p^{e-1}}, & i = p^{e-1}+1, \ldots, n. \end{cases}
$$

Set $s = n - p^{e-1}$. We want to show there is a change of basis that witnesses the natural action of H on R as equivalent to H acting on R with representation G' acting on $V_2^{n-p^{e-1}} \oplus V_1^{2p^{e-1}-n}$. Either $2s < p^{e-1}+1$ or $2s \geq p^{e-1}+1$. Suppose $2s < p^{e-1}+1$. The desired equivalence holds after change of basis given by

$$
x_i \mapsto \begin{cases} x_i, & i \text{ odd}, \ i < p^{e-1}+1, \\ x_i + x_{i-1}, & i \text{ even}, \ i \leq 2s, \\ x_i, & i \text{ even}, \ 2s < i < p^{e-1}+1, \\ x_i + (p-1)x_{i-p^{e-1}}, & i \geq p^{e-1}+1. \end{cases}
$$

Suppose $2s \geq p^{e-1} + 1$. The desired equivalence holds after change of basis given by

$$x_i \mapsto \begin{cases} x_i, & i \text{ odd}, \ i < p^{e-1} + 1, \\ x_i + x_{i-1}, & i \text{ even}, \ i < p^{e-1} + 1, \\ x_i + (p-1)x_{i-p^{e-1}}, & i \text{ odd}, \ i \geq p^{e-1} + 1, \\ x_i + x_{i-1} + (p-1)x_{i-p^{e-1}}, & i \text{ even}, \ p^{e-1} + 1 \leq i \leq 2s, \\ x_i + (p-1)x_{i-p^{e-1}}, & i \text{ even } i > 2s. \end{cases}$$

In both cases, after the change of basis the H has representation given by a direct sum of s copies of V_2 and $n - 2s = n - 2(n - p^{e-1}) = 2p^{e-1} - n$ copies of V_1. These changes of basis are demonstrated in Example 4.9.

3. The action of h on R is given by

$$h(x_i) = \begin{cases} x_i, & i = 1, \dots, p^{e-1}, \\ x_i + x_{i-p^{e-1}}, & i = p^{e-1} + 1, \dots, n. \end{cases}$$

Set $s = n - mp^{e-1}$. We again show there is a change of basis witnessing H acting on R as equivalent to $G' = \mathbb{Z}/p\mathbb{Z}$ acting on R with action induced by the action of G' on $V_{m+1}^{n-mp^{e-1}} \oplus V_m^{(m+1)p^{e-1}-n}$. Consider the change of basis maps $\phi\colon V_n \to V_n$ and

$\psi\colon V_n \to V_n$ which induce the following maps on x_i

$$\phi(x_i) = \begin{cases} x_i, & i < p^{e-1}, \\ x_i + (p-1)x_{i-p^{e-1}}, & i \geq p^{e-1}+1 \end{cases}$$

$$\psi(x_i) = \begin{cases} x_i, & i \equiv 1 \bmod (m+1), i \leq (m+1)s, \\ x_i + x_{i-1}, & i \not\equiv 1 \bmod (m+1), i \leq (m+1)s, \\ x_i, & i \equiv 1 \bmod m, i > (m+1)s, \\ x_i + x_{i-1}, & i \not\equiv 1 \bmod m, i > s. \end{cases}$$

The change of basis $\varphi = \psi \circ \phi$ gives the desired equivalence. In particular after the change of basis we have

$$\pi(h) \mapsto \begin{bmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_\ell \end{bmatrix}$$

where $n_i = m+1$ if $i < s$ and $n_i = m$ if $i \geq s$. Thus after the change of basis φ we have G' acting on the direct sum of s copies of V_{m+1} and

$$\frac{n-(m+1)s}{m} = \frac{m^2p^{e-1} + mp^{e-1} - mn}{m} = (m+1)p^{e-1} - n$$

copies of V_m.

$\square$

We now consider an example to illustrate the changes of variable described in the proof of Theorem 4.11.

Example 4.9. Let $G = \mathbb{Z}/49\mathbb{Z}$ act by the indecomposable action and char $k = 7$. If $g \in G$ is a generator, than $h = g^7$ is a generator for $H \leq G$ with $\#H = 7$. We first set $n = 10$ so that a representation for h is given by

$$\pi(h) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

In this case $s = 10 - 7 = 3$ and therefore $2s = 6 < 7 + 1 = 8$. Thus we apply the first change of basis from the proof of part (2) in Lemma 4.11 and $\pi(h) \mapsto h'$ where

$$h' = \left[\begin{array}{cc|cc|cc|cccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

which acts naturally on $V_2^3 \oplus V_1^4$, i.e., $V_2^{10-7} \oplus V_2^{14-10}$. Set $n = 12$ so that a representation of h is given by

$$\pi(h) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

In this case $s = 12 - 7 = 5$ and therefore $2s = 10 \geq 7 + 1 = 8$. Thus we apply the second change of basis from the proof of part (2) in Lemma 4.11 and $\pi(h) \mapsto h'$ where

$$h' = \left[\begin{array}{cc|cc|cc|cc|cc|c|c} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

which acts naturally on $V_2^5 \oplus V_1^2$, i.e., $V_2^{12-7} \oplus V_1^{14-12}$.

Combining Theorem 4.11 with Corollary 3.6 we get the following.

Corollary 4.12. *Let G act on $R = k[x_1, \ldots, x_n]$ by the indecomposable action and let $H \leq G$ a subgroup with $\#H = p$ act naturally on R. If $n > p^{e-1} + 2$, then R^H is not Cohen-Macaulay.*

As mentioned before we would like to generalize Theorem 4.11 to the case where $H \leq G = \mathbb{Z}/p^e\mathbb{Z}$ with $\#H = p^d$ for $2 \leq d \leq e$. To help generalize and illustrate the technique we will use, we look at some examples when $d = 2$.

Example 4.10. Let $G = \mathbb{Z}/2^e\mathbb{Z}$ and $g \in G$ be a generator. We first consider $e = 3$. Set $h = g^2$ and $\langle h \rangle = H \leq G$ so $\#H = 4$. If $n = 5$, then a representation of h is given by

$$\pi(h) = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Consider the elementary matrix operations giving the following equivalences

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Indeed

$$\left(\begin{bmatrix}1&0&0&0&0\\0&0&1&0&0\\0&0&0&0&1\\0&1&0&0&0\\0&0&0&1&0\end{bmatrix}\begin{bmatrix}1&0&1&0&0\\0&1&0&1&0\\0&0&1&0&1\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\right)\begin{bmatrix}1&0&0&0&0\\0&0&0&1&0\\0&1&0&0&0\\0&0&0&0&1\\0&0&1&0&0\end{bmatrix}=\begin{bmatrix}1&1&0&0&0\\0&1&1&0&0\\0&0&1&0&0\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}.$$

Thus the matrix

$$T=\begin{bmatrix}1&0&0&0&0\\0&0&0&1&0\\0&1&0&0&0\\0&0&0&0&1\\0&0&1&0&0\end{bmatrix}\begin{bmatrix}1&1&0&0&0\\0&1&1&0&0\\0&0&1&0&0\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}^{-1}\begin{bmatrix}1&0&0&0&0\\0&0&1&0&0\\0&0&0&0&1\\0&1&0&0&0\\0&0&0&1&0\end{bmatrix}\begin{bmatrix}1&1&0&0&0\\0&1&1&0&0\\0&0&1&0&0\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}=\begin{bmatrix}1&1&1&0&1\\0&1&1&1&1\\0&0&1&0&1\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}$$

gives a change of basis after which the first, third, and fifth columns of $\pi(h)$, i.e. the columns with index equivalent to 1 mod 2, form a Jordan block and the second and fourth columns of $\pi(h)$, i.e. the columns with index equivalent to 0 mod 2, form a Jordan block. Notice T corresponds to the change of basis

$$x_1 \mapsto x_1, \quad x_2 \mapsto x_2+x_1, \quad x_3 \mapsto x_3+x_2+x_1, \quad x_4 \mapsto x_4+x_2, \quad x_5 \mapsto x_5+x_4+x_3+x_2+x_1,$$

and allows us to view $\pi(h)$ as

$$h' = \left[\begin{array}{ccc|cc} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

Thus the natural action of H on R is equivalent to the action of H on R with representation $V_3 \oplus V_2$. If $n = 7$, then representations for h and h', where h' is the image of $\pi(h)$ after a change of basis, are given by

$$\pi(h) = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, h' = \left[\begin{array}{cccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

Thus the natural action of H on R is equivalent to the action of H on R with representation $V_4 \oplus V_3$.

We now consider $e = 4$. Set $h = g^4$ and $\langle h \rangle = H \leq G$. If $n = 9$, then a representation for h is given by

$$\pi(h) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and after an appropriate change of basis, we may view $\pi(h)$ as

$$h' = \left[\begin{array}{ccc|cc|cc|cc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

Thus the natural action of H on R is equivalent to the action of H on R with representation $V_3 \oplus V_2^3$.

Example 4.11. Let $p = 3$, $e = 3$ and $g \in G = \mathbb{Z}/27\mathbb{Z}$ be a generator. Set $h = g^3$ and

$\langle h \rangle = H \leq G$. If $n = 10$, a representation for h is given by

$$\pi(h) = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and after an appropriate change of basis, we may view $\pi(h)$ as

$$\pi(h) = \left[\begin{array}{cccc|ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

Hence the natural action of H on R is equivalent to the action of H on R with representation $V_4 \oplus V_3^2$.

With these examples in mind, we now prove the following lemma regarding when $H \le G$ with $\#H = p^d$.

Theorem 4.13. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ by the indecomposable action and let $H \le G$ a subgroup with $\#H = p^d$, $0 < d < e$, act naturally on R. Let $g \in G$ be a generator so that $H = \langle g^{p^{e-d}} \rangle$. If $p^{e-1} + mp^{e-d} < n \le p^{e-1} + (m+1)p^{e-d}$ with $0 \le m \le p^d - p^{d-1} - 1$, then natural action of H on R is equivalent to the action of H on R with representation*

$$V_{p^{d-1}+m+1}^{n-p^{e-1}-mp^{e-d}} \oplus V_{p^{d-1}+m}^{p^{e-1}+(m+1)p^{e-d}-n}.$$

Proof. Recall that

$$g^m = \begin{bmatrix} 1 & \binom{m}{1} & \binom{m}{2} & \binom{m}{3} & \cdots & \binom{m}{n-1} \\ 0 & 1 & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{n-2} \\ 0 & 0 & 1 & \binom{m}{1} & \cdots & \binom{m}{n-3} \\ \vdots & \vdots & \vdots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \binom{m}{1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

By Lucas' Theorem, $\binom{p^{e-d}}{i} \equiv 0 \bmod p$ when $i \ne p^{e-d}$ so a representation of $g^{p^{e-d}}$ is given by a matrix, $\pi(g^{p^{e-d}}) = (a_{j,i})$, with 1's along the main diagonal, 1's along the diagonal $a_{p^{e-d}+i+1,i}$ with $i = 0, \ldots, n - p^{e-d}$ and 0's elsewhere. We want to show there is a change of basis witnessing the natural action of H on R as equivalent to the action of H on R with representation $V_{p^{d-1}+m+1}^{n-p^{e-1}-mp^{e-d}} \oplus V_{p^{d-1}+m}^{p^{e-1}+(m+1)p^{e-d}-n}$. The action of H is given by

$$x_i \mapsto \begin{cases} x_i, & i \le p^{e-d}, \\ x_i + x_{i-p^{e-d}}, & i > p^{e-d} \end{cases}.$$

There exists a change of basis taking the given representation of $g^{p^{e-d}}$ to the representation where the Jordan blocks are created from the columns corresponding to the equivalence classes of p^{e-d}, i.e., J_{j_1} will be formed by taking all columns whose index is equivalent to 1 mod p^{e-d}, see Example 4.10. This yields p^{e-d} Jordan blocks with each Jordan block an indecomposable representation. To determine the size of the Jordan blocks write $n = ap^{e-d} + b$, and note that each Jordan block will have rank either a or $a+1$. In particular, there will be b Jordan blocks of rank $a+1$. By hypothesis, $n = p^{e-1} + mp^{e-d} + c$ for some $c = 1, \ldots, p^{e-d}$. Thus

$$p^{e-1} + mp^{e-d} + c = ap^{e-d} + b$$

and therefore $a = p^{d-1} + m$. We now observe that there will be

$$b = n - ap^{e-d} = n - (p^{d-1} + m)p^{e-d} = n - p^{e-1} - mp^{e-d}$$

Jordan blocks of rank $a + 1 = p^{d-1} + m + 1$ and

$$p^{e-d} - b = p^{e-d} - (n - p^{e-1} - mp^{e-d}) = p^{e-1} + (m+1)p^{e-d} - n$$

Jordan blocks of rank $a = p^{d-1} + m$. This gives the desired equivalence. $\square$

Recall the filtration of G given by

$$0 = \left\langle g^{p^e} \right\rangle \leq \left\langle g^{p^{e-1}} \right\rangle \leq \cdots \leq \left\langle g^{p^1} \right\rangle \leq \left\langle g^{p^0} \right\rangle = G$$

which yields a chain of subrings of R

$$R^G \subseteq R^{\left\langle g^{p^1} \right\rangle} \subseteq \cdots \subseteq R^{\left\langle g^{p^{e-1}} \right\rangle} \subseteq R.$$

Using Theorem 4.13 we can now give a more descriptive picture of this chain of subrings.

For $p^{e-1} + m_i p^i < n \leq p^e(m_i+1)p^i$ with $0 \leq m_i \leq p^{e-i} - p^{e-i-1} - 1$ and $i = 1, \ldots, e$, set

$$a_t = n - p^{e-1} - m_t p^t, \quad b_t = p^{e-1} + (m_t+1)p^t - n, \quad c_t = p^{e-t-1} + m_t.$$

For $1 \leq i \leq e$, by Theorem 4.13, there is an induced map
$\varphi\colon\ k[V]^{\left\langle g^{p^{i-1}}\right\rangle} \to k[V_{c_i+1}^{a_i} \oplus V_{c_i}^{b_i}]^{\left\langle g^{p^i}\right\rangle}$ such that the following diagram commutes.

$$\begin{tikzcd}
 & k[V_{c_{i-1}+1}^{a_{i-1}} \oplus V_{c_{i-1}}^{b_{i-1}}]^{\left\langle g^{p^{i-1}}\right\rangle} \arrow[d, "\sim"] & \\
0 \arrow[r] & k[V]^{\left\langle g^{p^{i-1}}\right\rangle} \arrow[r] \arrow[dr, dashed] & k[V]^{\left\langle g^{p^i}\right\rangle} \arrow[d, "\sim"] \\
 & & k[V_{c_i+1}^{a_i} \oplus V_{c_i}^{b_i}]^{\left\langle g^{p^i}\right\rangle}
\end{tikzcd}$$

Moreover, this gives an injective map $k[V_{c_{i-1}+1}^{a_{i-1}} \oplus V_{c_{i-1}}^{b_{i-1}}]^{\left\langle g^{p^{i-1}}\right\rangle} \hookrightarrow k[V_{c_i+1}^{a_i} \oplus V_{c_i}^{b_i}]^{\left\langle g^{p^i}\right\rangle}$ for $1 \leq i \leq e$. This yields the following corollary to Theorem 4.13.

Corollary 4.14. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ by the indecomposable action. Let $g \in G$ be a generator. For $p^{e-1} + m_i p^i < n \leq p^e + (m_i+1)p^i$ with $0 \leq m_i \leq p^{e-i} - p^{e-i-1} - 1$ and $i = 1, \ldots, e-1$, set*

$$a_t = n - p^{e-1} - m_t p^t, \quad b_t = p^{e-1} + (m_t+1)p^t - n, \quad c_t = p^{e-t-1} + m_t.$$

We have

$$k[V_n]^G \hookrightarrow k[V_{c_1+1}^{a_1} \oplus V_{c_1}^{b_1}]^{\left\langle g^{p^1}\right\rangle} \hookrightarrow \cdots \hookrightarrow k[V_{c_{e-1}+1}^{a_{e-1}} \oplus V_{c_{e-1}}^{b_{e-1}}]^{\left\langle g^{p^{e-1}}\right\rangle} \hookrightarrow k[V_n].$$

5 Noether Numbers, Multiplicity, and p-Sylow Subgroups

5.1 Noether Numbers for Modular Ring of Invariants

We open this chapter by introducing a result due to Benson which is analogous to Noether's bound on the top degree of a homogeneous generating set for the ring of invariants. We start by giving some definitions from invariant theory which will be useful.

Definition 5.1. Let G be a group acting on a ring R with $\mathfrak{m}$ the homogeneous maximal ideal of the ring of invariants. The *Hilbert ideal* is the ideal $\mathcal{H} := \mathfrak{m}R$, i.e., the ideal of R generated by the homogeneous invariants of positive degree. The *ring of coinvariants* is the quotient

$$R_G := R/\mathcal{H}.$$

Moreover, R_G is a module over the group ring kG. The *Noether number*, denoted $\beta(V)$ or $\beta(R^G)$, is the least integer d such that R^G is minimally generated by homogeneous elements of degree less than or equal to d.

We use $\mathrm{td}(R_G)$ to denote the largest degree in which $f \in R_G$ is non-zero. It is a well-known fact that R_G is a finite dimensional k-vector space and therefore $\mathrm{td}(R^G) < \infty$, see for example [22].

Definition 5.2. Let G be a group acting on a ring R. For an ideal $I \subseteq R$ we define the invariants of I to be $I^G := \{r \in I \mid g(r) = r \text{ for all } g \in G\}$. We say I is *G-stable* provided $ga \in I$ for all $g \in G$ and $a \in I$.

Example 5.1. Recall that $\mathrm{B}_n(k) \subseteq \mathrm{GL}_n(k)$, the Borel subgroup of $\mathrm{GL}_n(k)$, is comprised of all the upper triangular matrices. By Theorem 2.3, the representation of any element $g \in G = \mathbb{Z}/p^e\mathbb{Z}$ is in the Borel subgroup, that is, $\pi(g) \in \mathrm{B}_n(k)$. Thus any ideal which is Borel fixed is also fixed by the group action. In particular, this gives a class of examples of G-stable ideals.

Lemma 5.1. *[29, Benson, Lemma 2.3.1] Let S be a commutative ring with identity and $\pi\colon G \to \mathrm{Aut}(S)$ be a representation of G by automorphisms of S. If $\#G$ is invertible in S and $I \subset S$ is a G-stable ideal then $I^{\#G} \subset I^G \cdot S$.*

Notice, Lemma 5.1 requires the action of G on A to be non-modular, indeed a crucial step in the proof requires division by $\#G$. We do not, in general, get the same result in the modular case as the following example shows.

Example 5.2. Let $G = \mathbb{Z}/4\mathbb{Z}$ act on $R = k[x, y, z]$ by the indecomposable action with $\operatorname{char} k = 2$. Let $\mathfrak{m} \subseteq R$ be the homogeneous maximal ideal. We want to show $\mathfrak{m}^4 \not\subseteq \mathfrak{m}^G R$. From Example 2.3,

$$R^G = k[x, xy + y^2, z^4 + z^2x^2 + zyx^2 + z^2xy + z^2y^2 + zy^2x, xy^2 + y^3 + x^2z + xz^2].$$

It is clear that $\mathfrak{m}$ is G-stable. By direct calculation $\mathfrak{m}^G R = (x, y^2, z^4)$ and therefore $yz^3 \in \mathfrak{m}^4$ but $yz^3 \notin \mathfrak{m}^G R$.

Let R be a graded ring with $\operatorname{char} R = p > 0$ and $R_0 = k$, G a group such that $p \mid \#G$ and G act on R by a degree-preserving k-algebra homomorphism. If $P \lneq G$ is a normal p-Sylow subgroup, then $[G : P]$ is invertible in R. Recall the relative transfer map $\mathrm{Tr}_P^G\colon\ R^P \to R^G$ is defined by

$$\mathrm{Tr}_P^G(r) = \sum_{\overline{g} \in G/P} \overline{g}(r)$$

where the sum ranges over the distinct equivalence classes of G/P. The image of the relative transfer map is contained in R^G. Combining all these facts we get the following extension of Lemma 5.1.

Lemma 5.2. *Let R be a ring with $\operatorname{char} R = p > 0$ and G a group such that $p \mid \#G$. Let $P \lneq G$ be a normal p-Sylow subgroup acting naturally on R. If $I \subseteq R^P$ is G-stable, then $I^{[G:P]} \subset I^G \cdot R^P$.*

Proof. Set $s = [G : P]$. Since P is normal, it is the unique p-Sylow subgroup and therefore $\#G/P = s \in R^{\times}$. Fix $\overline{g}_1, \ldots, \overline{g}_s \in G/P$ a complete set of distinct equivalence classes and set $T = \{\overline{g}_1, \ldots, \overline{g}_s\}$. Choose s elements of I and index them by T, that is, choose $\{f_{\overline{g}_i} \mid i = 1, \ldots, s\} \subseteq I$. For any $\overline{h} \in G/P$, since T is a complete set of representatives for G/P, it follows that

$$\prod_{\overline{g}_i \in T} (\overline{h}\overline{g}_i f_{\overline{g}_i} - f_{\overline{g}_i}) = 0.$$

Indeed, there exists $\overline{g_i} \in T$ such that $\overline{g}_i = \overline{h}^{-1}$ and therefore $\overline{h}\overline{g}_i f_{\overline{g}_i} - f_{\overline{g}_i} = 0$. Summing over the distinct equivalence classes $\overline{h} \in G/P$ and expanding yields

$$\begin{aligned} 0 &= \sum_{\overline{h} \in G/P} \prod_{\overline{g}_i \in T} (\overline{h}\overline{g}_i f_{\overline{g}_i} - f_{\overline{g}_i}) \\ &= \sum_{S \subseteq T} (-1)^{\#(T \setminus S)} \left(\sum_{\overline{h} \in G/P} \prod_{\overline{g}_i \in S} \overline{h}\overline{g}_i f_{\overline{g}_i} \right) \left(\prod_{\overline{g}_i \in T \setminus S} f_{\overline{g}_i} \right). \end{aligned} \tag{9}$$

We claim $\pm s \left(\prod_{\overline{g}_i \in T} f_{\overline{g}_i} \right) \in I^G \cdot R^p$. It suffices to show, this term is, up to a unit, a generic element of I^s. The term on the right of (9) corresponding to $S = \emptyset$ is $\pm s \left(\prod_{\overline{g}_i \in T} f_{\overline{g}_i} \right)$. All other terms on the right hand side of (9) are in $I^G \cdot R^P$ since I is G-stable and $\left(\sum_{\overline{h} \in G/P} \prod_{\overline{g}_i \in S} \overline{h}\overline{g}_i f_{\overline{g}_i} \right)$ is invariant. In particular, if $S = \{\overline{g}_{\alpha_1}, \ldots, \overline{g}_{\alpha_\ell}\}$, then

$$\begin{aligned} \left(\sum_{\overline{h} \in G/P} \prod_{\overline{g}_{\alpha_i} \in S} \overline{h}\overline{g}_{\alpha_i} f_{\overline{g}_{\alpha_i}} \right) &= \sum_{\overline{h} \in G/P} \overline{h}(\overline{g}_{\alpha_1} f_{\overline{g}_{\alpha_1}}) \cdots h(\overline{g}_{\alpha_\ell} f_{\overline{g}_{\alpha_\ell}}) \\ &= \sum_{\overline{h} \in G/P} \overline{h}(\overline{g}_{\alpha_1} f_{\overline{g}_{\alpha_1}} \cdots \overline{g}_{\alpha_\ell} f_{\overline{g}_{\alpha_\ell}}). \end{aligned}$$

Since I is G-stable, the product $\overline{g}_{\alpha_1} f_{\overline{g}_{\alpha_1}} \cdots \overline{g}_{\alpha_\ell} f_{\overline{g}_{\alpha_\ell}} \in I$. Thus

$$\sum_{\overline{h} \in G/P} \overline{h}(\overline{g}_{\alpha_1} f_{\overline{g}_{\alpha_1}} \cdots \overline{g}_{\alpha_\ell} f_{\overline{g}_{\alpha_\ell}}) = \mathrm{Tr}_P^G(\overline{g}_{\alpha_1} f_{\overline{g}_{\alpha_1}} \cdots \overline{g}_{\alpha_\ell} f_{\overline{g}_{\alpha_\ell}}) \in I^G.$$

Moreover,

$$\pm s\left(\prod_{\overline{g}_i\in T\setminus S} f_{\overline{g}_i}\right)=\sum_{\substack{S\subseteq T\\ S\neq\emptyset}}(-1)^{\#(T\setminus S)}\left(\sum_{\overline{h}\in G/P}\prod_{\overline{g}_i\in S}\overline{h}\overline{g}_i f_{\overline{g}_i}\right)\left(\prod_{\overline{g}_i\in T\setminus S} f_{\overline{g}_i}\right)\in I^G\cdot R^P.$$

□

Remark 11. The key step in the proof of Lemma 5.2 requires us to divide by $[G:P]$. In the proof of the original lemma due to Benson, there is an analogous step requiring division by $\#G$ which is the obstruction to a similar lemma when G is a p-group.

As a consequence of this lemma, we get the following well-known analogue of Noether's bound on the top degree of a homogeneous generating set for certain modular rings of invariants.

Corollary 5.3. *Let R be a ring with* $\operatorname{char} R = p > 0$ *and G a group such that $p \mid \#G$. If $P \lneq G$ is a normal p-Sylow subgroup acting naturally on R, then $\beta(R^G)\leq [G:P]\beta(R^P)$.*

Proof. Denoting $\mathfrak{n}$ the homogeneous maximal ideal for R^P and similarly for $\mathfrak{m}$ and R^G, it is clear that $\mathfrak{n}^G=\mathfrak{m}$. Moreover, $\mathfrak{n}$ is G-stable and therefore $\mathfrak{n}^{[G:P]}\subseteq \mathfrak{n}^G\cdot R^P$. We want to show that $\mathfrak{n}^G\cdot R^P$ is generated as an ideal by G-invariants of degree at most $[G:P]$. Consider f a monomial in the generators of R^P with $\deg f = s\geq [G:P]$. We have f is a product of s elements of $\mathfrak{n}$ and therefore $f\in\mathfrak{n}^G\cdot R^P$. If $s>[G:P]$, then we can write $f=gh$ with $\deg g=[G:P]$ and $\deg h>1$, i.e., f is not part of a minimal generating set for $n^G\cdot R^P$.

Recall the relative transfer map $\mathrm{Tr}^G_P: R^P\to R^G$ defined by $\mathrm{Tr}^G_P(r)=\frac{1}{[G:P]}\sum_{\overline{g}\in G/P}\overline{g}(r)$. Since $\mathfrak{m}\cdot R^P=\mathfrak{n}^G\cdot R^P$, it follows that $\mathrm{Tr}^G_P|_{\mathfrak{n}^G\cdot R^P}\colon \mathfrak{n}^G\cdot R^P\to R^G$ is a surjection. Moreover, the relative transfer gives a R^G-module homomorphism and the generators for $\mathfrak{n}^G\cdot R^P$ are mapped to generators for $\mathfrak{m}$ which generate R^G as an algebra. This gives that $R^G=(R^P)^{(G/P)}$ is generated by elements of degree at most $[G:P]$ when considered as the rings of invariants for G/P acting on R^P and the result now follows. □

Remark 12. This was first shown in [11] using a somewhat technical linear algebra argument to show the generators of the Hilbert ideal for R^G in R^P have degree at most $[G : P]$. We avoid this by applying Lemma 5.2 to show the desired degree result and then use the surjectivity of the restricted relative transfer map. Notably, Fleischmann's work provides an algorithm for writing arbitrary degree G-invariants in terms of invariants of degree at most $[G : P]\beta(R^P)$ without knowing an explicit generating set for R^G.

Example 5.3. We claim this bound is sharp. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Let $R = \mathbb{F}_3[x, y]$ and $P = \langle(0, 1)\rangle$. Since G is abelian, any subgroup of G is normal, i.e. P is a normal 3-Sylow subgroup. Suppose G acts by the representation

$$\pi((1, 0)) = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \text{ and } \pi((0, 1)) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

We have $[G : P] = 2$ and the representation of P is the indecomposable representation of $\mathbb{Z}/3\mathbb{Z}$. Thus we have seen $R^P = \mathbb{F}_3[x, y^3 - x^2y]$, and $\beta(R^P) = 3$. This gives $\beta(R^G) \leq 2\beta(R^P) = 6$.

Using the algorithm outlined in Chapter 2, we can compute R^G directly. In particular, $S = \{x^2, y^6 + x^2y^4 + x^4y^2\}$ forms a set of primary invariants for R^G and applying the algorithm yields

$$R^G = \mathbb{F}_3[x^2, y^6 + x^2y^4 + x^4y^2, xy^3 - x^3y]$$

whence $\beta(R^G) = 6$.

Since we can bound the Noether number for a modular ring of invariants by the Noether number of a normal p-Sylow subgroup, a natural question to ask is for G a p-group acting on $R = k[x_1, \ldots, x_n]$ is there an explicit value or bound for $\beta(R^G)$? In the case where G is cyclic, i.e. $G = \mathbb{Z}/p^e\mathbb{Z}$, this is a long standing question which has been answered when $e = 1$ by the following. For the remainder of this chapter, we again use the convention of writing V_i to mean the vector space of dimension i, that is, $\dim_k V_i = i$.

Theorem 5.4. *[10, Fleischmann, Sezer, Shank, Woodcock] Let $G = \mathbb{Z}/p\mathbb{Z}$ act on $k[V]$ with* $\operatorname{char} k = p$*. Suppose that $k[V]_G$ is a reduced finite dimensional kG-module, where kG denotes the usual group ring. Set s to be the number of non-trivial indecomposable Jordan blocks in the representation of G.*

1. *If the representation of G contains a summand isomorphic to V_i with $i > 3$, then*

$$\beta(V) = (p-1)s + p - 2.$$

2. *If G has representation $mV_2 \oplus \ell V_3$ with $\ell > 0$, then*

$$\beta(V) = (p-1)s + 1.$$

Note, it is well known that $\beta(V_2) = \beta(V_3) = \beta(2\beta V_2) = p$. It follows from [7] and [31] that $\beta(tV_2) = t(p-1)$ for $t > 2$. Applying these facts and Theorem 5.4 gives the following refinement of Corollary 5.3 when $G = \mathbb{Z}/p\mathbb{Z}$.

Corollary 5.5. *Let G be a group acting on $k[V]$ with* $\operatorname{char} k = p > 0$ *such that $p \mid \#G$. If $\mathbb{Z}/p\mathbb{Z} = P \lneq G$ is a normal p-Sylow subgroup acting naturally on R, then setting s to be the number of non-trivial indecomposable Jordan blocks in the representation of P, the following hold.*

1. *If P has representation V_2 or $2V_2$, then*

$$\beta(R^G) \leq [G : P]p.$$

2. *If P has representation sV_2 with $s > 2$, then*

$$\beta(R^G) \leq [G : P]s(p-1).$$

3. *If the representation of P contains a summand isomorphic to V_i with $i > 3$, then*

$$\beta(R^G) \leq [G:P]((p-1)s + p - 2).$$

4. *If P has representation $mV_2 \oplus \ell V_3$ with $\ell > 0$, then*

$$\beta(R^G) \leq [G:P]((p-1)s + 1).$$

Notice that Example 5.3 is a consequence of part (1) of this corollary. More generally, if $G = (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$ acts on $\mathbb{F}_p[x,y]$, then by part (1), $\beta(R^G) \leq p(p-1)$.

5.2 Hilbert-Kunz Multiplicity

As mentioned in the introduction we are interested in describing the geometric singularities of R^G. To this end, we now introduce two notions of multiplicity. The first is the well-known Hilbert-Samuel multiplicity.

Definition 5.3. The Hilbert-Samuel mutliplicity of a local ring $(R, \mathfrak{m}, k)$ along an $\mathfrak{m}$-primary ideal I is given by

$$e(I,R) = e(I) := \lim_{n\to\infty} \frac{d!}{n^d}\lambda(R/I^n)$$

where $d = \dim R$ and $\lambda(R/I^n)$ denotes the length of R/I^n. If $I = \mathfrak{m}$, $e(\mathfrak{m}, R) = e(\mathfrak{m}) = e(R)$ is called the Hilbert-Samuel multiplicity of R.

The Hilbert-Samuel multiplicity measures the asymptotic growth of the colength of powers of I. The function $n \mapsto \lambda(R/I^n)$ is eventually a polynomial-like function and it is well-known that $e(I) \in \mathbb{Z}$. The following theorem, due to Rees, relates Hilbert-Samuel multiplicity to integral closure.

Theorem 5.6. *[30, Rees] Let $(R, \mathfrak{m}, k)$ be a formally equidimensional local ring. If $J \subseteq I$*

are $\mathfrak{m}$-primary ideals of R, then $\overline{I} = \overline{J}$ if and only if $e(I) = e(J)$ where $\overline{I}$ represents the integral closure of I and similarly for J.

In the setting where char $R = p > 0$, there is another multiplicity. For an ideal $I \subseteq R$, the Frobenius powers of I are given by $I^{[p^e]} = (i^{p^e} \mid i \in I)$ for $e \geq 0$. This leads to the following definition.

Definition 5.4. Let R be a local ring of characteristic $p > 0$. The *Hilbert-Kunz multiplicity* of an R-module M with respect to an $\mathfrak{m}$-primary ideal $I \subseteq R$ is defined to be

$$e_{HK}(I, M) := \lim_{e \to \infty} \frac{\lambda_R(M/I^{[p^e]}M)}{p^{de}}$$

where $d = \dim R$ and λ denotes length. When $I = \mathfrak{m}$, we write $e_{HK}(\mathfrak{m}, R) = e_{HK}(\mathfrak{m}) = e_{HK}(R)$, and call this number the *Hilbert-Kunz multiplicity of R*.

It is a theorem of Monsky that this limit exists [27]. Notice, the limit defining the Hilbert-Kunz multiplicity is similar to the Hilbert-Samuel multiplicity. The difference is the Hilbert-Kunz multiplicity measures the asymptotic growth rate of the colength of Frobenius powers of an ideal. Moreover, the Hilbert-Kunz function of an ideal I, $e \mapsto \lambda(R/I^{[p^e]})$, differs from the Hilbert-Samuel function of I in that it has non-polynomial behavior. Also, $e_{HK}(I, R)$ need not be an integer as defined.

Example 5.4. [12, Han, Monsky] Let $R = (\mathbb{F}_5[x, y, z, w]/(x^4 + y^4 + z^4 + w^4))_{(x,y,z,w)}$. Han and Monsky showed that

$$\lambda_R\left(R/\mathfrak{m}^{[p^e]}\right) = \frac{168}{61}(5^e)^3 - \frac{107}{61}3^e$$

and, in particular, $e_{HK}(R) = \frac{168}{61}$.

It is a conjecture that there exists R with $e_{HK}(R)$ irrational or even transcendental [28]. Despite the difficulty of computing it, Hochster and Huneke showed an analogous statement to Theorem 5.6 relating Hilbert-Kunz multiplicity to tight closure.

Theorem 5.7. *[16, Hochster, Huneke] Let $(R, \mathfrak{m})$ be a complete equidimensional local ring. If $I \subseteq J$ are $\mathfrak{m}$-primary ideals, then $I^* = J^*$ if and only if $e_{HK}(I) = e_{HK}(J)$.*

We use Lemma 5.2 to give a bound on $e_{HK}(R^G)$ under some mild assumptions. To this end, we relate $e_{HK}(R^G)$ and $e_{HK}(R^P)$ using the following result. Recall, we localize R^G at the homogeneous maximal ideal $\mathfrak{m}$ when we require R^G to be local.

Theorem 5.8. *[33, Watanabe, Yoshida, Theorem 2.7] [34, Watanabe, Yoshida, Theorem 1.1] Let $(R, \mathfrak{m}) \subset (S, \mathfrak{n})$ be an extension of local domains where S is a finite R-module of rank r and $R/\mathfrak{m} \cong S/\mathfrak{n}$. For every $\mathfrak{m}$-primary ideal I we have the following.*

1. *The Hilbert-Kunz multiplicity*

$$e_{HK}(I, R) = \frac{e_{HK}(IS, S)}{r}.$$

2. *If S is regular, then*

$$e_{HK}(I, R) = \frac{\lambda_S(S/IS)}{r}.$$

3. *If R is noetherian, then for any $n \in \mathbb{Z}_{\geq 0}$,*

$$\frac{e(I^n)}{d!} \leq e_{HK}(I^n, R) \leq \frac{\binom{n+d-1}{d}}{n^d} e(I^n).$$

When a group G acts by a non-modular action, Asgharzadeh applied Theorem 5.8 with Benson's Lemma to give an estimate for $e_{HK}(R^G)$.

Theorem 5.9 (Asgharzadeh, [1])**.** *If G is a group acting on a ring $R = k[x_1, \ldots, x_n]$ with $\operatorname{char} k = p > 0$ and $\#G$ is not divisible by p, then*

$$e_{HK}(R^G) \leq \frac{\binom{n-1+\#G}{n}}{\#G}.$$

In order to use Theorem 5.8, we need to know $\operatorname{rank}_{R^G}(R)$. If $\#G < \infty$ and the action of G on R is faithful, then $\operatorname{rank}_{R^G}(R) = \#G$. We outline the argument here and defer details to [2]. Let $p(R,t)$ denote the Poincaré series for R and similarly for R^G. We define the degree of R, denoted $\deg R$ to be the value of the rational function $(1-t)^{\dim R}p(R,t)$ at $t=1$ and similarly for R^G. In general, if S is an integral domain and M is an S-module, then $\deg(M) = \operatorname{rank}_S(M)\deg(S)$ by Lemma 2.4.1(iii), page 20, [2]. As $R^G \subseteq R$ is a finite extension of graded integral domains which are are finitely generated over $R_0 = k$, $\deg(R) = [\operatorname{frac}(R) : \operatorname{frac}(R^G)]\deg(R^G)$ by Proposition 2.4.2, page 21, [2]. The extension $\operatorname{frac}(R)/\operatorname{frac}(R^G)$ is Galois with Galois group G and therefore $[\operatorname{frac}(R) : \operatorname{frac}(R^G)] = \#G$. Moreover, since $\deg(R) = 1$, this gives $\frac{\deg(R^G)}{\deg(R)} = \frac{1}{\#G}$ so $\operatorname{rank}_{R^G}(R) = \frac{\deg(R)}{\deg(R^G)} = \#G$.

Throughout the remainder of this section we will assume that $P \le G$ is a normal, proper, p-Sylow subgroup acting in a degree preserving manner on a ring R and we denote the respective rings of invariants R^P and R^G with homogeneous maximal ideals $\mathfrak{n}$ and $\mathfrak{m}$ respectively. Set $s = [G : P]$. Following Asgharzadeh's approach with Lemma 5.2 in place of Benson's lemma, we get the following.

Theorem 5.10. *Let R be a graded domain with $\operatorname{char} R = p > 0$, $R_0 = k$ a field and $d = \dim R$. Let G act on R by a degree preserving k-algebra homomorphisms with $p \mid \#G$, $P \le G$ be a p-Sylow subgroup acting naturally on R, and $s = [G : P]$. If P is normal and $I \subseteq R^P$ is a G-stable $\mathfrak{n}$-primary ideal, then*

$$e_{HK}(R^G) \le \frac{\binom{s+d-1}{d} e(I, R^P)}{s}.$$

Proof. By Lemma 5.2 $I^s \subset I^G R^P \subset \mathfrak{m}R^P$ and therefore for all $e \ge 0$, $(I^s)^{[p^e]} \subseteq \mathfrak{m}^{[p^e]}R^P$ which induces a surjection $R^P/(I^s)^{[p^e]}R^P \to R^P/\mathfrak{m}^{[p^e]}R^P \to 0$. Thus $\dim_k(R^P/\mathfrak{m}^{[p^e]}R^P) \le \dim_k(R^P/(I^s)^{[p^e]}R^P)$. Note, $\mathfrak{n}$ is G-stable and therefore $\mathfrak{n}^s \subseteq \mathfrak{n}^G R^P \subseteq \mathfrak{m}R^P$. Since $\mathfrak{n}^s \subseteq \mathfrak{m}R^P$, it follows that both $\mathfrak{m}$ and $\mathfrak{m}^{[p^e]}$ are $\mathfrak{n}$-primary. By

Theorem 5.8(3),

$$\begin{aligned}
e_{HK}(\mathfrak{m}R^P, R^P) = \lim_{e\to\infty} \frac{\lambda_{R^P}(R^P/\mathfrak{m}^{[p^e]}R^P)}{p^{ed}} &= \lim_{e\to\infty} \frac{\dim_k(R^P/\mathfrak{m}^{[p^e]}R^P)}{p^{ed}} \\
&\leq \lim_{e\to\infty} \frac{\dim_k(R^P/(I^s)^{[p^e]}R^P)}{p^{ed}} \\
&= e_{HK}(I^s, R^P) \\
&\leq \frac{\binom{s+d-1}{d}}{s^d} e(I^s, R^P).
\end{aligned}$$

As

$$\begin{aligned}
e(I^s, R^P) = \lim_{e\to\infty} d! \frac{\lambda_{R^P}(R^P/I^{se}R^P)}{e^d} &= \lim_{e\to\infty} d! \frac{\lambda_{R^P}(R^P/I^{se}R^P)}{e^d}\frac{s^d}{s^d} \\
&= s^d \lim_{e\to\infty} d! \frac{\lambda_{R^P}(R^P/I^{se}R^P)}{(se)^d} = s^d e(I, R^P)
\end{aligned}$$

it follows that

$$e_{HK}(\mathfrak{m}R^P, R^P) \leq \binom{s+d-1}{d} e(I, R^P).$$

Since $\mathrm{rank}_{R^G}(R^P) = \#G/P = s$, applying Theorem 5.8(1) yields

$$e_{HK}(R^G) = \frac{e_{HK}(\mathfrak{m}R^P, R^P)}{\mathrm{rank}_{R^G}(R^P)} \leq \frac{\binom{s+d-1}{d} e(I, R^P)}{s}.$$

□

Corollary 5.11. *Let R be a graded domain with $\operatorname{char} R = p > 0$, $R_0 = k$ a field and $d = \dim R$. Let G act on R by a degree preserving k-algebra homomorphisms. Let $P \leq G$ be a p-Sylow subgroup acting naturally on R with $s = [G : P]$. If P is normal, then*

$$e_{HK}(R^G) \leq \frac{\binom{s+d-1}{d} e(\mathfrak{n}, R^P)}{s}.$$

Example 5.5. We want to show that our bound is sharp. To do so, we again consider

$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ acting on $R = \mathbb{F}_3[x, y]$ with representation

$$\pi((1,0)) = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \text{ and } \pi((0,1)) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Let $P = \langle (0, 1) \rangle$. Since G is abelian, any subgroup of G is normal, i.e. P is a normal 3-Sylow subgroup. We have $[G : P] = 2$ and $\dim R = 2$ therefore

$$e_{HK}(R^G) \leq \frac{\binom{2+2-1}{2} e(\mathfrak{n}, R^P)}{2} = \frac{\binom{3}{2} e(\mathfrak{n}, R^P)}{2} = \frac{3}{2} e(\mathfrak{n}, R^P).$$

Recall $R^P = \mathbb{F}_3[x, y^3 - x^2 y]$, i.e., R^P is isomorphic to a polynomial ring and has $e(\mathfrak{n}, R^P) = 1$. This gives $e_{HK}(R^G) \leq \frac{3}{2}$. Using the algorithm outlined in Chapter 2,

$$R^G = k[x^2, y^6 + x^2 y^4 + x^4 y^2, xy^3 - x^3 y].$$

We have $R^G \cong k[a, b, c]/(ab - c^2)$ with the isomorphism given by $x^2 \mapsto a$, $y^6 + x^2 y^4 + x^4 y^2 \mapsto b$, and $xy^3 - x^3 y \mapsto c$. Thus R^G is the coordinate ring of a toric variety. Moreover, using techniques developed in [13], we get $e_{HK}(R^G) = \frac{3}{2}$ and our bound is sharp.

Example 5.6. More generally, let $G = (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$. Let $R = \mathbb{F}_p[x, y]$ and $P = \langle (1, 1) \rangle$. We again have G is abelian and hence P is normal. Suppose G acts by the representation

$$\pi((c,0)) = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} \text{ and } \pi((1,1)) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

where c is a primitive $(p-1)$st root of unity. We have $R^P = \mathbb{F}_p[x, y^p - x^{p-1} y]$, i.e. R^P is isomorphic to a polynomial ring and $e(R^P) = 1$. Since $\dim R = 2$ and $[G : P] = p - 1$, it follows that

$$e_{HK}(R^G) \leq \frac{\binom{p-1+2-1}{2} e(\mathfrak{n}, R^P)}{p-1} = \frac{\binom{p}{2}}{p-1} = \frac{(p)(p-1)}{2(p-1)} = \frac{p}{2}.$$

Example 5.7. Let $G = (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$, $R = \mathbb{F}_p[x, y, z]$, and $P = \langle (1, 1) \rangle$. We have

$\dim R = 3$, $[G : P] = p - 1$, and G is abelian therefore P is normal. If G acts with representation

$$\pi((c,0)) = \begin{bmatrix} c & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{bmatrix} \text{ and } \pi((1,1)) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

where c is a primitive $(p-1)$st root of unity, then

$$e_{HK}(R^G) \leq \frac{\binom{p-1+3-1}{3} e(\mathfrak{n}, R^P)}{p-1} = \frac{\binom{p+1}{3}}{p-1} e(\mathfrak{n}, R^P) = \frac{(p+1)(p)}{6} e(\mathfrak{n}, R^P).$$

Example 5.8. Let $G = D_3 = \langle r, f \mid r^3 = f^2 = 1, rf = fr^2 \rangle$ the dihedral group on 3 vertices. Let $R = \mathbb{F}_3[x, y]$ and G act on R by

$$r = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } f = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

We have $\langle r \rangle = P \leq G$ is the unique 3-Sylow subgroup of G. Moreover $[G : P] = 2$ and $\dim R = 2$ therefore

$$e_{HK}(R^G) \leq \frac{\binom{2+2-1}{2} e(\mathfrak{n}, R^P)}{2} = \frac{\binom{3}{2} e(\mathfrak{n}, R^P)}{2} = \frac{3}{2} e(\mathfrak{n}, R^P).$$

In this case $P \cong \mathbb{Z}/3\mathbb{Z}$ and the representation of r is given by the indecomposable representation of $\mathbb{Z}/3\mathbb{Z}$. Thus

$$R^P = \mathbb{F}_3[x, y^3 - x^2 y],$$

i.e., R^P is isomorphic to a polynomial ring and has $e(R^P) = 1$. This gives $e_{HK}(R^G) \leq \frac{3}{2}$.

Remark 13. For a group G with $\#G = cp^e$, a Hall subgroup $H \leq G$ is a subgroup with $\#H = ap^e$ where $ap^e \mid cp^e$. A p-Sylow subgroup is the simplest example of a Hall subgroup. The results of this section easily extend to Hall subgroups, i.e., we may take $H \leq G$ to be a Hall subgroup and prove analogous results to Lemma 5.2, Theorem 5.10, and Corollary

5.11.

5.3 Upper Bounds for the Hilbert-Kunz Multiplicity of Rings of Invariants for Cyclic p-Groups

The key to Theorem 5.10 is Lemma 5.2 which requires $[G:P] \in R^\times$; in particular, $G \neq P$. Are there cases when a bound similar to the bound in Theorem 5.10 holds for G a p-group? The answer is yes and we first provide two examples.

Example 5.9. Let $G = \mathbb{Z}/p\mathbb{Z}$ act on $R = \mathbb{F}_p[x, y, z]$ by the indecomposable action. Let $\mathfrak{m}$ denote the homogeneous maximal ideal for R^G and $\mathfrak{n}$ denote the homogeneous maximal ideal for R. It is clear that $\mathfrak{n}$ is G-stable and that $\mathfrak{n}^G \cdot R = (x, y^2, z^p)$ is $\mathfrak{n}$-primary. We claim that $\mathfrak{n}^{p+1} \subseteq \mathfrak{n}^G \cdot R$. Indeed, any monomial term in $\mathfrak{n}^{p+1}$ which does not have an x is of the form $y^\alpha z^\beta$ where either $\alpha \geq 2$ or $\beta \geq p$. Thus for all $t \geq 0$, $(\mathfrak{n}^{p+1})^{[p^t]} \subseteq \mathfrak{m}^{[p^t]} \cdot R$ which induces a surjection

$$R/(\mathfrak{n}^{p+1})^{[p^t]}R \to R/\mathfrak{m}^{[p^t]} \cdot R \to 0.$$

By a similar computation to Theorem 5.10, we now have

$$e_{HK}(R^G) \leq \frac{\binom{p+1+3-1}{3}}{p} e(\mathfrak{n}, R) = \frac{\binom{p+3}{3}}{p}.$$

Example 5.10. Let $G = \mathbb{Z}/p\mathbb{Z}$ act on $R = \mathbb{F}_p[x, y, z, w]$ by the indecomposable action with $\mathfrak{m}$ and $\mathfrak{n}$ as in the previous example. By Theorem 3.2 of [32]

$$\mathfrak{n}^G R = (x, y^2, yz^{p-3}, z^{p-1}, w^p).$$

By direct calculation, for $r \geq 2p-2$,

$$\mathfrak{n}^r \subseteq \mathfrak{n}^G R.$$

Indeed, $2p-2$ is sharp since a monomial in $(x, y, z, w)^{2p-2}$ of the form $z^\alpha w^\beta$ must have

$\alpha \geq p-1$ or $\beta \geq p$. Thus, following the computation in Theorem 5.10

$$e_{HK}(R^G) \leq \frac{\binom{2p-2+4-1}{4}}{p} e((x,y,z,w),R) = \frac{\binom{2p+1}{4}}{p}.$$

Generalizing these examples will require us to study $\mathfrak{n}^G \cdot R$ where $\mathfrak{n}$ is the homogeneous maximal ideal of R. We do this through the use of the Hilbert ideal and the ring of coinvariants introduced earlier. Recall that the Hilbert ideal is the ideal in R generated by the homogeneous invariants of positive degree, i.e. $\mathcal{H} = \mathfrak{m} \cdot R$ where $\mathfrak{m}$ is the homogeneous maximal ideal of R^G. Also, we showed previously that $\operatorname{rank}_{R^G}(R) = \#G$. The ring of coinvariants is given by $R_G := R/\mathcal{H}$ and we use $\operatorname{td}(R_G)$ to denote the largest degree in which $f \in R_G$ is non-zero. It is a well-known fact that R_G is a finite dimensional k-vector space and therefore $\operatorname{td}(R^G) < \infty$ (see for example, [22]). Thus, it is clear $\mathfrak{n}^{\operatorname{td}(R_G)+1} \subseteq \mathcal{H} = \mathfrak{m} \cdot R$ which gives the following.

Theorem 5.12. *If G is a p-group acting on $R = k[x_1, \ldots, x_n]$ with* $\operatorname{char} k = p$*, then*

$$e_{HK}(R^G) \leq \frac{\binom{\operatorname{td}(R_G)+n}{n}}{\#G}.$$

Proof. Let $(R^G, \mathfrak{m})$ denote the ring of invariants with associated homogeneous maximal ideal and similarly for $(R, \mathfrak{n})$. Let R_G denote the algebra of coinvariants. We have

$$\mathfrak{n}^{\operatorname{td}(R_G)+1} \subseteq \mathfrak{n}^G R \subseteq \mathfrak{m} R$$

which induces a surjection $R/(\mathfrak{n}^{\operatorname{td}(R_G)+1})^{[p^e]}R \to R/\mathfrak{m}^{[p^e]}R \to 0$ for all $e \geq 0$. Thus by a similar computation as in Theorem 5.10, we get

$$e_{HK}(R^G) \leq \frac{\binom{\operatorname{td}(R_G)+1+n-1}{n}}{\#G} e(\mathfrak{n}, R) = \frac{\binom{\operatorname{td}(R_G)+n}{n}}{\#G}.$$

□

We can combine Theorems 5.10 and 5.12 in the following manner.

Corollary 5.13. *Let R be a graded domain with* $\operatorname{char} R = p > 0$*,* $R_0 = k$ *a field and* $d = \dim R$*. Let G act on R by a degree preserving k-algebra homomorphism with $p \mid \#G$. Let $P \leq G$ be a p-Sylow subgroup acting naturally on R with $s = [G : P]$. If P is normal, then*

$$e_{HK}(R^G) \leq (d!)\frac{\binom{s+d-1}{d}\binom{\operatorname{td}(R_P)+d}{d}}{\#G}.$$

In this corollary and Theorem 5.12, we are relying on the fact that $\operatorname{td}(R_G) < \infty$. Accordingly, we can rephrase our motivating question from earlier. For G a p-group acting on $R = k[x_1, \ldots, x_n]$ is there an explicit value or bound for $\operatorname{td}(k[V]_G)$ or more generally a value or bound for $\operatorname{td}((k[V]^P)_G)$ for a subgroup $P \leq G$? Recall that in Theorem 5.4, Fleischmann, Sezer, Shank, and Woodcock gave a value for the Noether number for any representation of $G = \mathbb{Z}/p\mathbb{Z}$. In particular, this theorem proves the long standing "$2p-3$"-conjecture, that is, when $G = \mathbb{Z}/p\mathbb{Z}$ acts on $k[x_1, \ldots, x_n]$ with $n \geq 4$, $\operatorname{td}(R_G) = 2p - 3$. This gives the following in the case of $P = \mathbb{Z}/p\mathbb{Z} \lneq G$ is a normal p-Sylow subgroup.

Corollary 5.14. *Let R be a graded domain with* $\operatorname{char} R = p > 0$*,* $R_0 = k$ *a field and* $d = \dim R$*. Let G act on R by a degree preserving k-algebra homomorphism with $p \mid \#G$. If $P = \mathbb{Z}/p\mathbb{Z}$ is a proper, normal p-Sylow subgroup acting with representation equivalent to the indecomposable action, then setting $s = [G : P]$, the following hold*

1. *If P has representation V_2, then* $e_{HK}(R^G) \leq (d!)\frac{\binom{s+d-1}{d}\binom{(p-1)+d}{d}}{\#G}$.
2. *If P has representation V_3, then* $e_{HK}(R^G) \leq (d!)\frac{\binom{s+d-1}{d}\binom{p+d}{d}}{\#G}$.
3. *If the representation of P contains a summand isomorphic to V_i with $i > 3$, then* $e_{HK}(R^G) \leq (d!)\frac{\binom{s+d-1}{d}\binom{2p-3+d}{d}}{\#G}$.

Proof. In each case, we need only establish a value for $\operatorname{td}(R_P)$ to apply Corollary 5.13.

1. We have already seen in Example 2.2 that when $P = \mathbb{Z}/p\mathbb{Z}$ acts on $k[x, y]$ by the indecomposable action, $R^P = k[x, y^p - x^{p-1}y]$. It follows that the Hilbert ideal is given by $\mathcal{H} = (x, y^p)k[x, y]$ and therefore $\operatorname{td}(R_P) = p - 1$.

2. The computation in Example 5.9 gives $\operatorname{td}(R_P) = p$.

3. The bounds in Theorem 5.4 give $\operatorname{td}(R_P) = 2p - 3$.

$\square$

Example 5.11. We return to the example of $G = (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$ acting on $R = \mathbb{F}_p[x, y, z]$. If the representation of G is given as in Example 5.7 and $P = \langle(0, 1)\rangle$, then we have established

$$e_{HK}(R^G) \leq \frac{(p+1)p}{6} e(\mathfrak{n}, R^P).$$

We can now use Corollary 5.14 to make this more explicit, that is,

$$e_{HK}(R^G) \leq (3!)\frac{(p+1)p}{6}\frac{\binom{\operatorname{td}(R_P)+3}{3}}{p} = \frac{(p+1)p\binom{p+3}{3}}{p} = \frac{(p+3)(p+2)(p+1)^2}{6}.$$

Suppose that $G = \mathbb{Z}/p^e\mathbb{Z}$ with $e > 1$. Recall that we have the natural composition series of G, $0 \leq \langle g^{p^{e-1}} \rangle \leq \cdots \leq \langle g^{p^1} \rangle \leq \langle g^{p^0} \rangle = G$ with its associated chain of rings of invariants

$$R^G \subseteq R^{\left\langle g^{p^1} \right\rangle} \subseteq \cdots \subseteq R^{\left\langle g^{p^{e-1}} \right\rangle} \subseteq R.$$

Theorem 5.15. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ by the indecomposable action and $g \in G$ be a generator. For ease of notation, set $G_{e-i} = \left\langle g^{p^{e-i}} \right\rangle$ and set $\operatorname{td}_{e,i} := \operatorname{td}(R^{G_{e-(i-1)}})_{G_{e-i}/G_{e-(i-1)}}$. For $1 \leq i \leq e$, we have*

$$e_{HK}\left(R^{G_{e-i}}\right) \leq (n!)^{i-1} \frac{\prod_{j=1}^{i} \binom{\operatorname{td}_{e,i}+n}{n}}{p^i}.$$

Proof. We will use induction on i. When $i = 1$, we have $\#G_{e-1} = p$ and therefore by

Theorem 5.12

$$e_{HK}(R^{G_{e-1}}) = \frac{\binom{\mathrm{td}_{e,1}+n}{n}}{p} = (n!)^0 \frac{\prod_{j=1}^{i} \binom{\mathrm{td}_{e,j}+n}{n}}{p^1}.$$

Suppose the result holds for $1 \leq i < e$. Applying Theorems 5.8 and 5.12 we get

$$\begin{aligned}
e_{HK}(R^{G_{e-(i+1)}}) &\leq \frac{\binom{\mathrm{td}_{e,i+1}+n}{n}}{p} e(R^{G_{e-i}}) \\
&\leq n! \frac{\binom{\mathrm{td}_{e,i+1}+n}{n}}{p} e_{HK}(R^{G_{e-i}}) \\
&\leq n! \frac{\binom{\mathrm{td}_{e,i+1}+n}{n}}{p} \left((n!)^{i-1} \frac{\prod_{j=1}^{i} \binom{\mathrm{td}_{e,j}+n}{n}}{p^i} \right) = (n!)^i \frac{\prod_{j=1}^{i+1} \binom{\mathrm{td}_{e,j}+n}{n}}{p^{i+1}}.
\end{aligned}$$

□

In general, the values of $\mathrm{td}_{e,i}$ with notation as in the theorem may be difficult to compute. We now give an example with $e > 1$ where our bound can be made explicit.

Example 5.12. Let $G = \mathbb{Z}/4\mathbb{Z}$ act on $R = \mathbb{F}_2[x, y, z]$ by the indecomposable action. For $g \in G$ a generator, consider $H = \langle g^2 \rangle \leq G$. We want to give values for $\mathrm{td}((R^H)_G)$ and $\mathrm{td}(R_H)$ so that we may apply Theorem 5.15. In particular,

$$e_{HK}(R^G) = (3!)^1 \frac{\binom{\mathrm{td}((R^H)_G)+3}{3} \binom{\mathrm{td}(R_H)+3}{3}}{2^2}$$

It is not difficult to see that the natural action of H on R gives $R^H = \mathbb{F}_2[x, y, z^2 + xz]$ which gives $R_H = R/(x, y, z^2)R$ and therefore $\mathrm{td}(R_H) = 1$. By Example 2.3,

$$R^G = \mathbb{F}_2[x, xy + y^2, z^4 + z^2x^2 + zyx^2 + z^2xy + z^2y^2 + zy^2x, xy^2 + y^3 + x^2z + xz^2]$$

and therefore the homogeneous maximal ideal of R^G is given by

$$\mathfrak{m} = (x, xy + y^2, z^4 + z^2x^2 + zyx^2 + z^2xy + z^2y^2 + zy^2x, xy^2 + y^3 + x^2z + xz^2).$$

By direct calculation

$$\begin{aligned} xy + y^2 &\equiv y^2 \bmod x \cdot R^H, \\ z^4 + z^2x^2 + zyx^2 + z^2xy + z^2y^2 + zy^2x &= (z^2+xz)^2 + xy(z^2+xz) + y^2(z^2+xz) \\ &\equiv (z^2+xz)^2 \bmod (x, y^2) \cdot R^H, \\ xy^2 + y^3 + x^2z + xz^2 &= xy^2 + y^3 + x(xz+z^2) \\ &\equiv 0 \bmod (x, y^2) \cdot R^H. \end{aligned}$$

Thus $(R^H)_{G/H} \cong R^H/(x, y^2, (xz+z^2)^2)R^H$, and $\operatorname{td}((R^H)_G) = 2$. Moreover, $e_{HK}(R^G) \leq 3!\frac{\binom{5}{3}\binom{4}{3}}{2^2} = 60$.

We can combine Corollary 5.13 and Theorem 5.15 to get the following result regarding groups with a normal, cyclic p-Sylow subgroup.

Theorem 5.16. *Let R be a graded domain with $\operatorname{char} R = p > 0$, $R_0 = k$ a field and $d = \dim R$. Let G act on R by a degree preserving k-algebra homomorphisms. Let $P \leq G$ be a p-Sylow subgroup acting naturally on R with $s = [G : P]$. For ease of notation, set $G_{e-i} = \left\langle g^{p^{e-i}} \right\rangle$ and set $\operatorname{td}_{e,i} := \operatorname{td}(R^{G_{e-(i-1)}})_{G_{e-i}/G_{e-(i-1)}}$. If $P = \mathbb{Z}/p^e\mathbb{Z}$ and P is normal, then for $1 \leq i \leq e$, we have*

$$e_{HK}(R^G) \leq \frac{\binom{s+d-1}{d}}{s}(n!)^{e-1}\frac{\prod_{j=1}^{e}\binom{\operatorname{td}_{e,j}+n}{n}}{p^e}.$$

Example 5.13. Consider $\mathrm{GL}_3(\mathbb{F}_2)$. It is well known that $\#\,\mathrm{GL}_3(\mathbb{F}_2) = \prod_{i=1}^{3}(2^3 - 2^{i-1}) = (7)(6)(4)$. Since 4 and 3 both divide $\#\,\mathrm{GL}_3(\mathbb{F}_2)$, by Cauchy's theorem there exists elements $A, B \in \mathrm{GL}_3(\mathbb{F}_2)$ of orders 4 and 3 respectively. Let $G = \langle A \rangle \times \langle B \rangle$ and note that the 2-Sylow subgroup $P = \langle A, 1 \rangle$ is normal in G. In an appropriate basis $\langle A, 1\rangle$ acts on $R = \mathbb{F}_2[x, y, z]$ with representation

$$\pi((A, 1)) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Since $\dim R = 3$ and $[G : P] = 3$, applying Theorem 5.16 and using the computation in Example 5.12 we get

$$e_{HK}(R^G) \leq \frac{\binom{3+3-1}{3}}{3} 60 = 200.$$

Remark 14. We can use Corollary 4.14 and Theorems 5.4 and 5.8 to give another form of our bound. If $G = \mathbb{Z}/p^e\mathbb{Z}$ and $g \in G$ is a generator, then $\langle g^{p^{e-1}}\rangle \cong \mathbb{Z}/p\mathbb{Z}$. Set $d = \dim R$, $\mathfrak{m} \subseteq R^G$ the homogeneous maximal ideal, and $P = \langle g^{p^{e-1}}\rangle$. By Theorem 5.8 part (1),

$$e_{HK}(R^G) = \frac{e_{HK}(\mathfrak{m}R^P, R^P)}{p^{e-1}}$$

and a similar argument as in the proof of Theorem 5.12 yields

$$e_{HK}(R^G) \leq \frac{\binom{\mathrm{td}((R^P)_G)+d}{d} e_{HK}(R^P)}{p^e}$$

We can now apply Corollary 4.14 and Theorem 5.4 to give an explicit bound for $e_{HK}(R^P)$ and consequently a bound for $e_{HK}(R^G)$. However, we still need to compute $\mathrm{td}((R^P)_G)$ which, in general, can be quite difficult.

Remark 15. The bounds we have computed here are quite large. As there is not currently an explicit bound for the Hilbert-Kunz multiplicity for modular rings of invariants taking advantage of the representation theory for G, we have given a general formula to provide a starting point for as many cases as possible. Our hope is that there is a way to apply Theorem 4.13 and Corollary 4.14 to give explicit computations for these bounds using only the representation theory of the group. More specific formulae may help reduce the bound.

Also, the relation between the Hilbert-Samuel and Hilbert-Kunz multiplicity is scaled by a factorial and this causes our bounds to grow very quickly.

5.4 Lower Bounds for the Hilbert-Kunz Multiplicity of Rings of Invariants

We have discussed at length an upper bound for the Hilbert-Kunz multiplicity of various rings of invariants. It is well known that for a ring R with $\operatorname{char} R = p > 0$, R is regular if and only if $e_{HK}(R) = 1$. Thus, for a non-regular ring R, one interesting question is to find a lower bound for $e_{HK}(R)$. In some regards, this bound is a measurement of how far R is from being regular. A result of Blickle and Enescu tells us that if R is not Cohen-Macualay or not F-rational, then

$$e_{HK}(R) > 1 + \max\left\{\frac{1}{d!}, \frac{1}{e(R)}\right\} \tag{10}$$

where $d = \dim R$ and $e(R)$ denotes the Hilbert-Samuel multiplicity of R [3]. If we consider the ring of invariants for a group G with a normal p-Sylow subgroup acting on $R = k[x_1, \ldots, x_n]$ with $\operatorname{char} k = p > 0$, then we can use Lemma 5.2 to give a lower bound for the Hilbert-Kunz multiplicity in certain cases.

Theorem 5.17. *Let R be a graded domain with $\operatorname{char} R = p > 0$, $R_0 = k$ a field and $d = \dim R$. Let G act on R with $p \mid \#G$, $P \leq G$ a normal p-Sylow subgroup acting naturally on R and $s = [G : P]$. If $d! \geq s^d e(R^P)$ and R^G is not Cohen-Macaulay, then*

$$e_{HK}(R^G) > 1 + \frac{1}{e(R^G)} \geq 1 + \frac{1}{s^d e(R^P)}.$$

Proof. It suffices to show $e(R^G) \leq s^d e(R^P)$, as under the hypotheses

$$\frac{1}{d!} \leq \frac{1}{s^d e(R^P)} \leq \frac{1}{e(R^G)}$$

and the result would follow immediately from (10). Since $\mathfrak{n}$, the homogeneous maximal ideal of R^P, is G-stable, by Lemma 5.2, $\mathfrak{n}^s \subset \mathfrak{n}^G R^P \subset \mathfrak{m}R^P$. Thus for all $n \geq 0$, $(\mathfrak{n}^s)^n \subseteq \mathfrak{m}^n R^P$ which induces a surjection $R^P/(\mathfrak{n}^s)^n R^P \to R^P/\mathfrak{m}^n R^P \to 0$. Thus $\dim_k(R^P/\mathfrak{m}^n R^P) \leq \dim_k(R^P/(\mathfrak{n}^s)^n R^P)$. Since $\mathfrak{n}^s \subseteq \mathfrak{m}R^P$, it follows that both $\mathfrak{m}$ and $\mathfrak{m}^e$ are $\mathfrak{n}$-primary. By direct calculation,

$$
\begin{aligned}
e(\mathfrak{m}R^P, R^P) = \lim_{n\to\infty} \frac{d!\lambda_{R^P}(R^P/\mathfrak{m}^n R^P)}{n^d} &= \lim_{n\to\infty} \frac{d!\dim_k(R^P/\mathfrak{m}^n R^P)}{n^d} \\
&\leq \lim_{n\to\infty} \frac{d!\dim_k(R^P/(\mathfrak{n}^s)^n R^P)}{n^d} \\
&= e(\mathfrak{n}^s, R^P) \\
&= s^d e(R^P).
\end{aligned}
$$

Since Hilbert-Samuel multiplicity is additive on short exact sequences and we have an inclusion $R^G \subseteq R^P$ giving a natural short exact sequence, it follows that $e(R^G) \leq e(\mathfrak{m}R^P, R^P)$, that is, $e(R^G) \leq s^d e(R^P)$. $\square$

Example 5.14. Suppose $G = (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p^e\mathbb{Z}$ acts on $R = \mathbb{F}_p[x_1, \ldots, x_n]$ by $\pi((c,0)) = cI_n$ and $\pi((1,1)) = J_n$ where c is a primitive $(p-1)$st root of unity, I_n is the rank n identity matrix, and J_n is the Jordan block representation for the indecomposable representation of $\mathbb{Z}/p^e\mathbb{Z}$. Recall that $p^{e-1} < n \leq p^e$. The subgroup $P = \langle (1,1) \rangle$ is a normal p-Sylow subgroup of G. If $n \geq 4$, then G is not generated by bireflections and therefore by Theorem 3.3, R^G is not Cohen Macaulay. Thus Theorem 5.17 applies provided $n! \geq (p-1)^n e(R^P)$. Since $e(R^P)$ is fixed, there exists some $n > 0$ for which this inequality holds and this provides a class of examples for which our lower bound applies.

In the case where the p-Sylow subgroup is a cyclic p-group, we can give a more explicit estimate using our understanding of the structure of the subgroups of G. Let $G = \mathbb{Z}/p^e\mathbb{Z}$. For $g \in G$ a generator and $0 \leq j \leq e-1$, define

$$
\mathrm{td}_{j,j+1} := \mathrm{td}\left(\left(R^{\langle g^{p^{j+1}}\rangle}\right)_{\langle g^{p^j}\rangle/\langle g^{p^{j+1}}\rangle}\right).
$$

Theorem 5.18. *Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ with $\operatorname{char} k = p$ with $n \geq 4$. Let $g \in G$ be a generator. For $1 \leq i \leq e-1$, if*

$$n! \geq \left(\prod_{j=0}^{i-1} (\operatorname{td}_{j,j+1} + 1)^n\right) e\left(R^{\langle g^{p^i}\rangle}\right),$$

then $e_{HK}(R^G) > 1 + \frac{1}{e(R^G)}$. In particular,

$$e_{HK}(R^G) > 1 + \frac{1}{\left(\prod_{j=0}^{i-1} (\operatorname{td}_{j,j+1} + 1)^n\right) e\left(R^{\langle g^{p^i}\rangle}\right)}.$$

Proof. Denote the homogeneous maximal ideal of $R^{\langle g^{p^i}\rangle}$ by $\mathfrak{n}_i$ for $0 \leq i \leq e$. We have

$$\mathfrak{n}_{i+1}^{\operatorname{td}_{i,i+1}+1} R^{\langle g^{p^{i+1}}\rangle} \subseteq \mathfrak{n}_{i+1}^G R^{\langle g^{p^{i+1}}\rangle} \subseteq \mathfrak{n}_i R^{\langle g^{p^{i+1}}\rangle}$$

which induces a surjection

$$\frac{R^{\langle g^{p^{i+1}}\rangle}}{\left(\mathfrak{n}_{i+1}^{\operatorname{td}_{i,i+1}+1}\right)^t R^{\langle g^{p^{i+1}}\rangle}} \to \frac{R^{\langle g^{p^{i+1}}\rangle}}{(\mathfrak{n}_i)^t R^{\langle g^{p^{i+1}}\rangle}} \to 0$$

for all $t \geq 0$ and $0 \leq i \leq e-1$. Thus applying the same argument as in the proof of Theorem 5.17, for $0 \leq i \leq e-1$ we have

$$e\left(R^{\langle g^{p^i}\rangle}\right) \leq (\operatorname{td}_{i,i+1} + 1)^n e\left(R^{\langle g^{p^{i+1}}\rangle}\right).$$

An induction on i yields

$$e(R^G) \leq \left(\prod_{j=0}^{i-1} (\operatorname{td}_{j,j+1} + 1)^n\right) e\left(R^{\langle g^{p^i}\rangle}\right). \tag{11}$$

By the hypothesis and (11), for $1 \leq i \leq e-1$ we get

$$\frac{1}{d!} \leq \frac{1}{\left(\prod_{j=0}^{i-1} (\operatorname{td}_{j,j+1} + 1)^n\right) e\left(R^{\langle g^{p^i} \rangle}\right)} \leq \frac{1}{e(R^G)}.$$

The result now follows by (10). $\square$

As an immediate consequence of this theorem, we get the following.

Corollary 5.19. *Let R be a graded domain with $\operatorname{char} R = p > 0$, $R_0 = k$ a field and $d = \dim R$. Let G act on R with $p \mid \#G$, $P = \mathbb{Z}/p^e\mathbb{Z} \leq G$ a normal p-Sylow subgroup acting naturally on R and $s = [G : P]$. Let $g \in P$ be a generator. For $1 \leq i \leq e-1$, if R^G is not Cohen-Macaulay and*

$$d! \geq s^d \left(\prod_{j=0}^{i-1} (\operatorname{td}_{j,j+1} + 1)^d\right) e\left(R^{\langle g^{p^i} \rangle}\right)$$

then

$$e_{HK}(R^G) > 1 + \frac{1}{e(R^G)} \geq 1 + \frac{1}{s^d \left(\prod_{j=0}^{i-1} (\operatorname{td}_{j,j+1} + 1)^d\right) e\left(R^{\langle g^{p^i} \rangle}\right)}.$$

Remark 16. Notice that this theorem and corollary hold for $1 \leq i \leq e-1$. In particular, if there is a value of i for which we can easily compute $e\left(R^{\langle g^{p^i} \rangle}\right)$ and the necessary values of $\operatorname{td}_{j,j+1}$ and hypotheses hold, then we can give a numerical bound for $e_{HK}(R^G)$. Also note that the hypotheses of the corollary require R^G to not be Cohen Macaulay.

To apply Theorem 5.18 or Corollary 5.19, we need to know values for the $\operatorname{td}_{j,j+1}$ which are, in general, difficult to compute returning us to the following question. For G a p-group acting on $R = k[x_1, \ldots, x_n]$ is there an explicit value or bound for $\operatorname{td}(k[V]_G)$? Recall that Theorem 5.4 answers this when $G = \mathbb{Z}/p\mathbb{Z}$ acts by the indecomposable representation and $n > 3$. In this case, $\operatorname{td}(R_G) = 2p - 3$. The assumption that $k[V]_G$ is reduced is equivalent to assuming there are no trivial summands in the representation of G. Indeed, $\beta(V \oplus V_1^t) = \beta(V)$ for all t. Moreover, $\operatorname{td}(k[V \oplus V_1^t]_G) = \operatorname{td}(k[V]_G)$ for all t. Applying these facts allows us to explicitly apply Theorem 5.18 and Corollary 5.19 in special cases.

Example 5.15. Let $G = \mathbb{Z}/5\mathbb{Z}$ act on $\mathbb{F}_5[x_1, \ldots, x_n]$ with representation $V_4 \oplus V_1^{n-4}$. We have $\operatorname{td}(R_G) = \operatorname{td}((\mathbb{F}_5[V_4])_G) = 2(5) - 3 = 7$. For $n \geq 20$, we have $n! \geq (7+1)^n e(R) = 8^n$ and we can apply Theorem 5.18, that is, for $n \geq 20$, $e_{HK}(R^G) > 1 + \frac{1}{8^n}$. More generally, suppose $\mathbb{Z}/p\mathbb{Z}$ acts on $\mathbb{F}_p[x_1, \ldots, x_n]$ with representation $V_4 \oplus V_1^{n-4}$. We have $\operatorname{td}(R_G) = 2p - 3$ and therefore for values of n with $n! \geq (2p-3)^n e(R) = (2p-3)^n$, we have $e_{HK}(R^G) > 1 + \frac{1}{(2p-3)^n}$.

We now return to Example 5.14. Consider the specific case of $G = (\mathbb{Z}/5\mathbb{Z})^\times \times \mathbb{Z}/5\mathbb{Z}$ acting on $R = \mathbb{F}_5[x_1, \ldots, x_n]$ with $n \geq 4$ and action defined by $\pi((c, 0)) = cI_4$ and the representation of $(1, 1)$ given by $V_4 \oplus V_1^{n-4}$. Consider $P = \langle (1, 1) \rangle$ which is a normal 5-Sylow subgroup of G. Theorem 5.17 gives $e_{HK} > 1 + \frac{1}{4^n e(R^P)}$ whenever $n! \geq 4^n e(R^P)$. Since we may not know what $e(R^P)$ is, we can apply Corollary 5.19 when $n! \geq 4^n 8^n e(R) = 12^n$. This inequality holds when $n \geq 30$ and the corollary yields $e_{HK}(R^G) \geq 1 + \frac{1}{12^n}$. More generally, if $G = (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$ acts on R in a similar way and $n! \geq (p-1)^n (2p-3)^n$, then we can apply Corollary 5.19 to get $e_{HK}(R^G) \geq 1 + \frac{1}{(p-1)^n (2p-3)^n}$. In particular, we get $1 + \frac{1}{(p-1)^n (2p-3)^n} \geq 1 + \frac{1}{n!}$ improving on the bound of Blickle and Enescu using the representation theory for G.

6 A Formula for the Norm of x_4

Let $R = k[x_1, \ldots, x_n]$ with $n \geq 4$ and $\operatorname{char} k = p > 0$. Let $G = \mathbb{Z}/p^e\mathbb{Z}$ act on R by the indecomposable action. We begin by defining another well-known set of invariants.

Definition 6.1. Let G be a finite group acting on $R = k[x_1, \ldots, x_n]$. For $f \in R$, we define the *norm of f* by

$$\mathrm{N}(f) = N(f) := \prod_{g \in G} g(f).$$

Note that $N(x_4)$ is part of a system of primary invariants for R^G. In this section we prove a combinatorial form for $N(x_4)$ inspired by the work of Sezer and Shank who proved a combinatorial form for $N(x_3)$ in [32]. Along the way, we demonstrate some combinatorics which we believe are interesting in their own right. Throughout, let $P = \{0, \ldots, p-1\}$ be a chosen set of equivalence classes of k. We also assume throughout that $p \geq 5$ so that $e = 1$. In order to give a formula for $N(x_4)$, we need to introduce several combinatorial tools. We first introduce the following well-known result. Note, throughout the chapter we use results from [32] that only appear in its arXiv version (arXiv:math/0409107v1).

Lemma 6.1. *For $t \in \mathbb{Z}^+$, we have*

$$\sum_{i \in P} i^t = \begin{cases} -1 & p-1 \mid t \\ 0 & \textit{else} \end{cases} \mod p.$$

Proof. See, for example [32]. $\square$

We define the sets $S_i := \{A \subseteq P \mid |A| = i\}$, $S_{i,j} := \{A \subseteq P \mid |A| = i, j \notin A\}$, and for $\alpha \subseteq P$, $S_{i,\alpha} := \{A \subseteq P - \alpha \mid |A| = i\}$. For $\alpha \subseteq P$ let $\sigma_q(\alpha)$ denote the qth elementary symmetric polynomial in the elements of α and we will use $\pi(\alpha)$ to denote $\sigma_i\alpha$ for $\alpha \in S_i$. For convenience, we set $\sigma_0(\alpha) = 1$. We use $b_{q,j} \colon P \to P$ and $d_{q,j}$ as defined in [32] as well as the combinatorial results therein. As such, we include these definitions and results here and note we use d and b when the context is understood.

For $j \leq q$ define function $b_{q,j}\colon P \to P$ by

$$b_{q,j}(t) := \sum_{\alpha \in S_{q-1,t}} t\pi(\alpha)\sigma_j(\alpha \cup \{t\})$$

and set $d_{q,j} := \sum_{\alpha \in S_q} \pi(\alpha)\sigma_j(\alpha)$.

Example 6.1. Set $P = \{0, 1, 2\}$, a set of distinct equivalence classes for $\mathbb{F}_3$. If $k = 2$ and $j = 1$, then

$$d_{2,1} = 0 \cdot 1(0+1) + 0 \cdot 2(0+2) + 1 \cdot 2(1+2) \equiv 0 \bmod 3$$

and $b_{2,1}(1) = 1 \cdot 0(1+0) + 1 \cdot 2(1+2) \equiv 0 \bmod 3$. If $k = 1$ and $j = 1$, then $d_{1,1} = 0^2 + 1^2 + 2^2 \equiv 2 \bmod 3$ and $b_{1,1}(1) = 1^2 \equiv 1 \bmod 3$.

Lemma 6.2. *[32, Sezer, Shank, Lemmas 2.3 and 2.4] With d and b as defined above we have the following.*

1. $\sum_{i \in P} b_{q,j}(t) = qd_{q,j}$.

2. $d_{q,j} = b_{q,j}(t) + \sum_{\alpha \in S_{q,t}} \pi(\alpha)\sigma_j(\alpha)$.

3. *For $1 \leq q < p$, $b_{q,0}(t) = (-1)^{q+1}t^q$ and*

$$d_{q,j} = \begin{cases} 0, & \text{if } q < p-1 \\ -1, & \text{if } q = p-1 \end{cases}.$$

   Further, $b_{p,0}(i) = t^p - t$ and $d_{p,0} = 0$.

Lemma 6.3. *[32, Sezer, Shank, Lemmas 2.4 and 2.5] With d and b as defined above we have the following.*

1. *For* $1 \leq q+j < p$, *with* $0 \leq j \leq q$, $b_{q,j}(t) = (-1)^{q+1}\binom{q}{j}t^{q+j}$ *and*

$$d_{q,j} = \begin{cases} 0, & \text{if } q+j < p-1 \\ (-1)^q \binom{q}{j}\frac{1}{k}, & \text{if } q+j = p-1 \end{cases}.$$

2. *If* $p-1 < q+j < 2p-2$, *then* $b_{q,j}(t) = (-1)^q\binom{q}{j}t^{q+j} + f(t)$, *where* $f(t)$ *is a polynomial of degree less than or equal to* $q+j-(p-1)$, *and* $d_{q,j} = 0$.

Lemma 6.4. *[32, Sezer, Shank, Lemma 2.7] With* d *as defined above*

$$\sum_{\substack{\alpha \in S_{q_1} \\ \beta \in S_{q_2,\alpha}}} \pi(\alpha)\pi(\beta)\sigma_j(\alpha) = \binom{q_1+q_2-j}{q_2} d_{q_1+q_2,j}.$$

We now define a new object in the spirit of d above that we need for the computation. Define

$$\hat{d}_{q_1,q_2,j_1,j_2,j_3} := \sum_{\substack{\alpha \in S_{q_1} \\ \beta \in S_{q_2,\alpha}}} \pi(\alpha)\pi(\beta)\sigma_{j_1}(\alpha)\sigma_{j_2}(\alpha)\sigma_{j_3}(\beta).$$

Example 6.2. Set $P = \{0, 1, 2, 3, 4\}$, a set of distinct equivalence classes for $\mathbb{F}_5$. If $q_1 = j_1 = j_2 = 2$ and $q_2 = 1$, then

$$\begin{aligned} \hat{d}_{2,1,2,2,0} = & 3(1\cdot 2)^3 + 4(1\cdot 2)^3 + 2(1\cdot 3)^3 + 4(1\cdot 3)^3 + 2(1\cdot 4)^3 + 3(1\cdot 4)^3 \\ & + 1(2\cdot 3)^3 + 4(2\cdot 3)^3 + 1(2\cdot 4)^3 + 3(2\cdot 4)^3 + 1(3\cdot 4)^3 + 2(3\cdot 4)^3 \\ \equiv & 4+2+4+3+3+2+4+1+2+1+3+1 \equiv 0 \bmod 5. \end{aligned}$$

Notice, a monomial term of $\hat{d}$ can contain cubed digits which drastically changes the computation since monomial terms of d cannot contain cubed digits. We are now ready to give the formula for $N(x_4)$.

Theorem 6.5 (Norm Formula). *Let* $G = \mathbb{Z}/p\mathbb{Z}$ *act on* $R = k[x_1, \ldots, x_n]$ *with* $\operatorname{char} k = p$

and $n \geq 4$. *Write* $N(x_4) = \beta_0 + \beta_1 x_1 + \cdots + \beta_{p-(n+1)} x_1^{p-3}$, *with* $\beta_i \in k[x_2, x_3, x_4]$ *and for all* i

$$\beta_i = \gamma_{i,0} + \gamma_{i,1} x_2 + \cdots + \gamma_{i,p-(n+2)-i} x_2^{p-2-i}$$

with $\gamma_{i,j} \in k[x_3, x_4]$. *We have*

$$\gamma_{i,j} = \begin{cases} \sum_{\ell=1}^{j+1} \xi_{i,j,\ell} x_4^{\ell} x_3^{p-i-j-\ell} & \text{for } 1 \leq j \leq \frac{p-1}{2} \\ \sum_{\ell=1}^{p-j} \xi_{i,j,k} x_4^{\ell} x_3^{p-i-j-\ell} & \text{for } \frac{p+1}{2} \leq j \end{cases}$$

where

$$\xi_{i,j,\ell} = \sum_{s=0}^{i} \sum_{t=0}^{i} \sum_{u=0}^{j} \frac{(-1)^{j-(s+t+u)}}{3^i 2^{j+s}} \binom{p-i-\ell-u}{p-i-j-\ell} \hat{d}_{i,p-i-\ell,s,t,u}.$$

Before proving the theorem we prove the following lemma which will be needed in the final step of the proof. We note here that throughout this chapter we will use counting arguments to prove combinatorial lemmas. To help clarify these arguments, we have included several examples to illustrate them.

Lemma 6.6. *Let* $\hat{d}$ *be defined as above. We have*

$$\sum_{\bar{i} \in S_a} \sum_{\bar{j} \in S_{b,\bar{i}}} \sum_{\bar{q} \in S_{b,\bar{i} \cup \bar{j}}} \pi(\bar{i}) \pi(\bar{j}) \pi(\bar{q}) \sigma_s(\bar{i}) \sigma_t(\bar{i}) \sigma_u(\bar{j}) = \binom{b+c-u}{c} \hat{d}_{a,b+c,s,t,u}.$$

As mentioned, before proving Lemma 6.6 we provide an example to illustrate the desired equality.

Example 6.3. Fix $P = \{x, y, z, w, u\}$ and set $a = 2$, $b = c = s = t = u = 1$. Applying Lemma 6.6, we have

$$\sum_{\bar{i} \in S_2} \sum_{\bar{j} \in S_{1,\bar{i}}} \sum_{\bar{q} \in S_{1,\bar{i} \cup \bar{j}}} \pi(\bar{i}) \pi(\bar{j}) \pi(\bar{q}) \sigma_1(\bar{i}) \sigma_1(\bar{i}) \sigma_1(\bar{j}) = \binom{1}{1} \hat{d}_{2,2,1,1,1}. \tag{12}$$

Consider the monomial x^3yz^2w which occurs in the left hand side of the above equality. To count the number of times x^3yz^2w occurs on the left hand side of (12), we need to find all choices of $\bar{i}, \bar{j}$ and $\bar{k}$ which produce a product containing this monomial. We must have $x \in \bar{i}$ and $z \in \bar{j}$. Thus we only have freedom to choose the second element of the set $\bar{i}$ to be either y or w and the desired monomial can only occur in the products,

$$(xw)(x+w)(x+w)(z)(z)(y), (xy)(x+y)(x+y)(z)(z)(w),$$

that is, the desired monomial occurs twice.

We now want to count the number of times x^3yz^2w occurs on the right hand side of (12). This monomial only occurs in the products

$$(xy)(x+y)^2(zw)(z+w), (xw)(x+w)^2(zy)(z+y).$$

Thus x^3yz^2w occurs twice on the right hand side as well.

Now suppose $a = 2$, $b = c = 1$, and $s = t = u = 0$. By Lemma 6.6,

$$\sum_{\bar{i} \in S_2} \sum_{\bar{j} \in S_{1,\bar{i}}} \sum_{\bar{q} \in S_{1,\bar{i}\cup\bar{j}}} \pi(\bar{i})\pi(\bar{j})\pi(\bar{q}) = \binom{2}{1} \hat{d}_{2,2,0,0,0}. \tag{13}$$

Consider the monomial $xyzw$. To count the number of ways this monomial occurs on the left hand side of (13) choose two of the letters to form the set $\bar{i}$ and then one from the remaining two to form the set $\bar{j}$. Thus this monomial occurs $\binom{4}{2}\binom{2}{1}\binom{1}{1} = 12$ times on the left hand side. To count the number of ways $xyzw$ occurs on the right hand side of (13), we first choose two of the letters to form the subset of size two and then take the remaining two for the other subset. Multiplying by $\binom{2}{1}$, this gives $\binom{2}{1}\binom{4}{2}\binom{2}{2} = 12$ ways for $xyzw$ to occur on the right hand side as desired.

Proof of Lemma 6.6. Each monomial of $\hat{d}_{a,b+c,s,t,u}$ is of the form $\pi(\alpha)\pi(\theta)\pi(\tau_1)\pi(\tau_2)\pi(\tau_3)$ where $\alpha \in S_a$, $\theta \in S_{b+c}$, $\tau_1, \tau_2 \subseteq \alpha$ with $\#\tau_1 = s$ and $\#\tau_2 = t$, $\tau_3 \subseteq \theta$ with $\#\tau_3 = u$, and

$\alpha \cap \theta = \emptyset$. Each of these monomials occurs $\binom{b+c-u}{c}$ on the left hand side, once for each choice of $\overline{q} \in \theta - \tau_3$. $\square$

Proof of Theorem 6.5. Recall that

$$g^d(x_4) = x_4 + dx_3 + \binom{d}{2}x_2 + \binom{d}{3}x_1.$$

Note, this immediately gives bounds of $p-3$ and $p-2$ on the powers of x_1 and x_2 respectively in any monomial term of $N(x_4)$ and hence the degree bound on the β_i. We want to determine the coefficient, $A = A_{a,b,c}$, of $x_1^a x_2^b x_3^c x_4^{p-a-b-c}$ in $N(x_4)$. If we identify the terms of $N(x_4)$ that contribute to $x_1^a x_2^b x_3^c x_4^{p-a-b-c}$, then

$$A = \sum_{\overline{i} \in S_a} \sum_{\overline{j} \in S_{b,\overline{i}}} \sum_{\overline{q} \in S_{c,\overline{i}\cup\overline{j}}} \left[\binom{i_1}{3} \cdots \binom{i_a}{3} \binom{j_1}{2} \cdots \binom{j_b}{2} q_1 \cdots q_c \right] \tag{14}$$

where $\overline{i} = \{i_1, \ldots, i_1\}$, $\overline{j} = \{j_1, \ldots, j_b\}$, and $\overline{q} = \{q_1, \ldots, q_c\}$. By direct computation

$$\begin{aligned} \binom{i_1}{3} \cdots \binom{i_a}{3} &= \frac{1}{3^a 2^a} \prod_{s=1}^{a} i_s(i_s-1)(i_s-2) \\ &= \frac{1}{3^a 2^a} \pi(\bar{i}) \sum_{\eta \subseteq \bar{i}} (-1)^{|\bar{i}-\eta|} 2^{|\bar{i}-\eta|} \pi(\eta) \sum_{\eta \subseteq \bar{i}} (-1)^{|\bar{i}-\eta|} \pi(\eta) \end{aligned}$$

where the first sum in the last equality comes from the product of all the $(i_s - 2)$ terms and the second sum comes from the product of all the $(i_s - 1)$ terms. Furthermore

$$\sum_{\eta \subseteq \bar{i}} (-1)^{|\bar{i}-\eta|} 2^{|\bar{i}-\eta|} \pi(\eta) = \sum_{s=0}^{a} (-1)^{a-s} 2^{a-s} \sigma_s(\bar{i})$$

and

$$\sum_{\eta \subseteq \bar{i}} (-1)^{|\bar{i}-\eta|} \pi(\eta) = \sum_{s=0}^{a} (-1)^{a-s} \sigma_s(\bar{i})$$

whence

$$\binom{i_1}{3}\cdots\binom{i_a}{3} = \frac{1}{3^a 2^a}\pi(\bar{i})\sum_{s=0}^{a}(-1)^{a-s}2^{a-s}\sigma_s(\bar{i})\sum_{s=0}^{a}(-1)^{a-s}2^{a-s}\sigma_s(\bar{i})$$
$$= \frac{1}{3^a 2^a}\pi(\bar{i})\sum_{s=0}^{a}\sum_{t=0}^{a}(-1)^{-s-t}2^{a-s}\sigma_s(\bar{i})\sigma_t(\bar{i}). \tag{15}$$

A similar computation shows

$$\binom{j_1}{2}\cdots\binom{j_b}{2} = \frac{1}{2^b}\pi(\bar{j})\sum_{u=0}^{b}(-1)^{b-u}\sigma_u(\bar{j}). \tag{16}$$

Combining (14), (15), and (16) yields

$$\begin{aligned} A &= \sum_{\bar{i}\in S_a}\sum_{\bar{j}\in S_{b,\bar{i}}}\sum_{\bar{q}\in S_{b,\bar{i}\cup\bar{j}}}\frac{1}{3^a 2^{a+b}}\pi(\bar{i})\pi(\bar{j})\pi(\bar{q})\left[\sum_{s=0}^{a}\sum_{t=0}^{a}\sum_{u=0}^{b}(-1)^{b-(s+t+u)}2^{a-s}\sigma_s(\bar{i})\sigma_t(\bar{i})\sigma_u(\bar{j})\right] \\ &= \sum_{s=0}^{a}\sum_{t=0}^{a}\sum_{u=0}^{b}\frac{(-1)^{b-(s+t+u)}}{3^a 2^{b+s}}\left[\sum_{\bar{i}\in S_a}\sum_{\bar{j}\in S_{b,\bar{i}}}\sum_{\bar{q}\in S_{b,\bar{i}\cup\bar{j}}}\pi(\bar{i})\pi(\bar{j})\pi(\bar{q})\sigma_s(\bar{i})\sigma_t(\bar{i})\sigma_u(\bar{j})\right] \\ &= \sum_{s=0}^{a}\sum_{t=0}^{a}\sum_{u=0}^{b}\frac{(-1)^{b-(s+t+u)}}{3^a 2^{b+s}}\binom{b+c-u}{b}\hat{d}_{a,b+c,s,t,u}. \end{aligned} \tag{17}$$

where the last equality follows from Lemma 6.6. □

While Theorem 6.5 does give a formula for computing $N(x_4)$ and, in particular, individual coefficients of monomials in $N(x_4)$, $\hat{d}$ is in general difficult to compute. The remainder of this chapter is devoted to giving closed forms for various combinations of the q_i and j_i in $\hat{d}$ being zero or non-zero.

6.1 Closed Forms for $\hat{d}_{q_1,q_2,j_1,j_2,j_3}$

We open this section by noting that, $\hat{d}_{0,0,0,0,0} = 1$ so we will assume either $q_1 \neq 0$ or $q_2 \neq 0$. Further, if $q_1 = 0$, then $\hat{d}$ becomes d as defined above and Lemmas 6.2 and 6.3 hold. Thus throughout this section we will assume $q_1 \neq 0$. We will write $\hat{d}$ if the context is understood.

Using work of Sezer and Shank, we can immediately give formulae for $\hat{d}$ when

$j_1 = j_2 = j_3 = 0$ or when only one of the j_i is non-zero. In the case where one of the j_i is non-zero, without loss of generality, we assume j_1 is non-zero which gives $\hat{d}_{q_1,q_2,j_1,0,0} = \sum_{\substack{\alpha \in S_{q_1} \\ \beta \in S_{q_2,\alpha}}} \pi(\alpha)\pi(\beta)\sigma_{j_1}(\alpha)$.

Lemma 6.7. *For $1 \leq q_1 + q_2 + j_1 < 2p - 2$, we have*

1. $\hat{d}_{q_1,q_2,j_1,0,0} = \binom{q_1+q_2-j_1}{q_2} d_{q_1+q_2,j_1}$.

2.
$$\hat{d}_{q_1,q_2,j_1,0,0} = \begin{cases} 0 & q_1 + q_2 + j_1 < p - 1 \\ \binom{q_1+q_2-j_1}{q_2}\binom{q_1+q_2}{j_1}(-1)^{q_1+q_2}\frac{1}{q_1+q_2} & q_1 + q_2 + j_3 = p - 1 \\ 0 & p \leq q_1 + q_2 + j_1 < 2p - 2 \end{cases}.$$

3. *If $j_1 = 0$, then*
$$\hat{d}_{q_1,q_2,0,0,0} = \begin{cases} 0 & q_1 + q_2 < p - 1 \\ -\binom{q_1+q_2}{q_1} & q_1 + q_2 = p - 1 \\ 0 & p \leq q_1 + q_2 < 2p - 2 \end{cases}.$$

Similar formulae hold when $j_2 \neq 0$ and $j_1 = j_3 = 0$ or $j_3 \neq 0$ and $j_1 = j_2 = 0$.

Proof. Part (1) is Lemma 6.4. For part (2), apply Lemma 6.3 to part (1) and for part (3), set $j_1 = 0$ in part (2). $\square$

Suppose now that $j_3 \neq 0$ and either $j_1 \neq 0$ or $j_2 \neq 0$ but not both. In either of these cases, we get the following formula for $\hat{d}$.

Lemma 6.8. *With $\hat{d}$ defined as above, suppose that $j_3 \neq 0$ and only of j_1 and j_2 is non-zero. For $1 \leq k_1 + k_2 + j_3 + j_1 < 2p - 2$*

1. $\hat{d}_{k_1,k_2,j_1,0,j_3} = \binom{k_1+k_2-(j_1+j_3)}{k_1-j_1}\binom{j_1+j_3}{j_1} d_{k_1+k_2,j_1+j_3}$

2.

$$\hat{d}_{k_1,k_2,j_1,0,0} = \begin{cases} 0 & k_1+k_2+j_1 < p-1 \\ \binom{k_1+k_2-(j_1+j_3)}{k_1-j_1}\binom{j_1+j_2}{j_1}\binom{k_1+k_2}{j_1}(-1)^{k_1+k_2}\frac{1}{k_1+k_2} & k_1+k_2+j_3 = p-1 \\ 0 & p \leq k_1+k_2+j_1 < 2p-2 \end{cases}.$$

Similar formulae hold when $j_2 \neq 0$ and $j_1 = 0$.

Example 6.4. Let $P = \{x, y, z, w, u\}$ and suppose $q_1 = q_2 = j_1 = j_3 = 1$. Any monomial term of $\hat{d}_{1,1,1,0,1}$ is of the form r^2s^2 where $r, s \in P$. This term can occur twice in $\hat{d}$ by choosing either $\{r\} = \alpha$ or $\{s\} = \alpha$. On the other hand this term only occurs once in $d_{2,2}$ by choosing $\{r, s\} = \alpha$. Note, $\binom{1+1-(1+1)}{1-1}\binom{1+1}{1} = 2$, i.e., the formula in part (1) of Lemma 6.8 holds.

Example 6.5. Suppose $q_1 = q_2 = 2$, $j_1 = j_3 = 1$, and $\#P \geq 5$, i.e., P is sufficiently large. We will be comparing $\hat{d}_{2,2,1,0,1}$ and $d_{4,2}$. First note that $\binom{2+2-(1+1)}{2-1}\binom{1+1}{1} = 4$. Any monomial in $\hat{d}$ is of the form x^2y^2zw where $x, y, z, w \in P$. We must have either $x \in \alpha$ or $y \in \alpha$ and then we may choose either $z \in \alpha$ or $w \in \alpha$. Once α is chosen, there is no choice for β, i.e., this monomial occurs $\binom{2}{1}\binom{2}{1} = 4$ times in $\hat{d}$. Consider $d_{4,2}$. The term x^2y^2zw can only occur once in d by choosing $\{x, y, z, w\} = \alpha$ and taking the monomial term $xy \in \sigma_2(\alpha)$, i.e., the formula in part (1) of Lemma 6.8 holds.

Proof of Lemma 6.8. For part (1), note that any term on the right hand side is of the form $\pi(\theta)\pi(\tau)$ where $\tau \subseteq \theta$ with $\#\tau = j_1 + j_3$. Similarly, any term on the left hand side is of the form $\pi(\alpha)\pi(\gamma_1)\pi(\beta)\pi(\gamma_2)$ where $\gamma_1 \subseteq \alpha$ with $\#\gamma_1 = j_1$, $\gamma_2 \subseteq \beta$ with $\#\gamma_2 = j_3$, and $\alpha \cap \beta = \emptyset$. We need to choose $\gamma_1 \subseteq \tau$ and $\alpha - \gamma_1 \subseteq \theta - \tau$. These choices are independent hence each term on the left hand side occurs $\binom{k_1+k_2-(j_1+j_3)}{k_1-j_1}\binom{j_1+j_3}{j_1}$ times on the left hand side. For part (2), apply Lemma 6.3 to part (1). $\square$

We can use the above lemmas giving closed forms for $\hat{d}$ to show examples of computing coefficients in $N(x_4)$. We will use x, y, z, w in place of x_1, x_2, x_3, x_4 respectively for ease of notation.

Example 6.6. Consider $G = \mathbb{Z}/5\mathbb{Z}$ acing on $\mathbb{F}_5[x, y, z, w]$. We have

$$N(w) = (w + z)(w + 2z + y)(w + 3z + 3y + x)(w + 4z + y + x)(w).$$

Consider the monomial xz^3w appearing in $N(w)$. Expanding $N(w)$ gives the coefficient of xz^3w as 2. According to Theorem 6.5, this coefficient is given by

$$\xi_{1,0,1} = \sum_{s=0}^{1}\sum_{t=0}^{1}\sum_{u=0}^{0} \frac{(-1)^{-(s+t+u)}}{3^1 2^s}\binom{3}{3}\hat{d}_{1,3,s,t,u}.$$

By the above lemmas, excepting the case where $s = t = 1$ not consider in the lemmas, $\hat{d}_{1,3,s,t,u}$ is non-zero only when $1 + 3 + s + t + u$ is divisible by 4 which occurs when $s = t = u = 0$. Thus applying the formulae above

$$\begin{aligned}\xi_{1,0,1} = \frac{(-1)^0}{3}\hat{d}_{1,3,0,0,0} + \frac{(-1)^2}{3(2)}\hat{d}_{1,3,1,1,0} &\equiv 2(-1)\binom{1+3}{1} + \hat{d}_{1,3,1,1,0} \\ &= 2(-4) + \hat{d}_{1,3,1,1,0} \\ &\equiv 2(1) + \hat{d}_{1,3,1,1,0} = 2 + \hat{d}_{1,3,1,1,0} \bmod 5.\end{aligned}$$

To complete the computation, we take $\{0, 1, 2, 3, 4\}$ to be a set of equivalence classes for $\mathbb{F}_5$ and compute $\hat{d}_{1,3,1,1}$ directly as follows

$$\hat{d}_{3,1,1,1} = 1^3(2\cdot 3\cdot 4) + 2^3(1\cdot 3\cdot 4) + 3^3(1\cdot 2\cdot 4) + 4^3(1\cdot 2\cdot 3) \equiv 4 + 1 + 1 + 4 \equiv 0 \mod 5.$$

Example 6.7. We again consider $G = \mathbb{Z}/5\mathbb{Z}$ acting on $R = \mathbb{F}_5[x, y, z, w]$. Consider the monomial x^2zw^2 appearing in $N(w)$. Expanding $N(w)$ gives the coefficient of x^2zw^2 as 2.

By Theorem 6.5, this coefficient is given by

$$\xi_{2,0,2} = \sum_{s=0}^{2}\sum_{t=0}^{2}\sum_{u=0}^{0} \frac{(-1)^{-(s+t+u)}}{3^2 2^s}\binom{1}{1}\hat{d}_{2,1,s,t,u}.$$

We first find the values of $\hat{d}$ when s and t are both non-zero. Fix $\{0,1,2,3,4\}$ a set of equivalence classes for $\mathbb{F}_5$. By direct calculation

$$\hat{d}_{2,1,1,1,0} \equiv \hat{d}_{2,1,2,1,0} = \hat{d}_{2,1,1,2,0} \equiv \hat{d}_{2,1,2,2,0} \equiv 0 \bmod 5.$$

For example the case of $\hat{d}_{2,1,2,2,0}$ was computed in Example 6.2. By the above lemmas, if one or both of s and t are zero, then $\hat{d}_{2,1,s,t,u}$ is non-zero only when $2+1+s+t+u$ is divisible by 4 which occurs when either $s=1$ or $t=1$. Thus applying the formulae from the lemmas and the above computation gives

$$\begin{aligned}
\xi_{2,0,2} &= \frac{(-1)^1}{3^2 2^1}\binom{1}{1}\hat{d}_{2,1,1,0,0} + \frac{(-1)^1}{3^2}\binom{1}{1}\hat{d}_{2,1,0,1,0} \\
&\equiv (-2)\binom{2+1-1}{1}\binom{2+1}{1}(-1)^{1+2}\frac{1}{1+2} + (-4)\binom{2+1-1}{1}\binom{2+1}{1}(-1)^{1+2}\frac{1}{1+2} \\
&= \frac{2^2(3)}{3} + \frac{3(2)4}{3} \equiv 4+3 \equiv 2 \bmod 5.
\end{aligned}$$

There are two more possible combinations of non-zero q_i and j_i. Either $j_1 \neq 0$, $j_2 \neq 0$, and $j_3 = 0$ or all of the j_i are non-zero. Notice, in the above examples we computed these values of $\hat{d}$ directly to exhibit the formula in Theorem 6.5. We note that this is the point where extending the formula given by Sezer and Shank for $N(x_3)$ to a formula for $N(x_4)$ becomes quite difficult, i.e., although we have a closed form for $N(x_4)$, without a closed form for $\hat{d}_{q_1,q_2,j_1,j_2,j_3}$ in these cases the formula is still rather difficult to work with. One outstanding question we have is whether or not in these cases $\hat{d}$ is at least subject to the same constraints as the other cases, i.e., $\hat{d} = 0$ whenever $q_1+q_2+j_1+j_2+j_3$ is not divisible by $p-1$ and non-zero otherwise. This is supported by the computations in the examples however we do not have a proof of this in general.

7 Some Extensions to G an Abelian p-Group

A natural question to ask next is what can we say in the more general case of G an abelian p-group, i.e., a direct product of cyclic p-groups. It is much more difficult in this case to give a complete description of the indecomposable and decomposable representations of G, similar to Theorem 2.3. Further, it is not always obvious when a given representation of G is faithful, i.e., the associated ring of invariants may not be normal.

Example 7.1. Let $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $R = \mathbb{F}_3[x, y, z]$. If G acts on R, then a generator for each cyclic factor must act by one of the representations described in Theorem 2.3. Recall that we use $\pi(g)$ to denote the representation of an element $g \in G$. Consider the action of G on R by

$$\pi((1,0)) = \pi((0,1)) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Notice that the action by each cyclic factor of G on R is faithful, i.e., the induced actions of $\mathbb{Z}/3\mathbb{Z} \times 0 \leq G$ and $0 \times \mathbb{Z}/3\mathbb{Z} \leq G$ are both faithful. However, by direct calculation

$$\pi((2,1)) = \pi((2,0) + (0,1)) = \pi((2,0))\pi((0,1)) = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = I_3,$$

that is, $\mathrm{id} \neq (2,1) \in G$ but $\pi((2,1)) = \mathrm{id} \in \mathrm{GL}_3(\mathbb{F}_3)$ and the action of G on R is not faithful. Consider instead, the action of G on R by

$$\pi((1,0)) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \pi((0,1)) = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Again, the induced action by each cyclic factor of G on R is faithful. Moreover, it is not difficult to see the action of G on R is faithful.

Despite the difficult of classifying the representations of G in the more general setting of an abelian p-group, we can use the group structure of G and representation theory techniques to describe R^G. We start with an example of the simplest case of $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Theorem 7.1. *Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ with $\operatorname{char} k = p$. The ring of invariants, R^G, is a unique factorization domain.*

Proof. Recall that Nakajima's Lemma tells us R^G is a unique factorization domain if and only if there are no non-trivial homomorphisms $G \to k^\times$ taking the value 1 on every pseudo-reflection or equivalently, there are no non-trivial homomorphisms $\varphi\colon\ G/H \to k^\times$ where $H \leq G$ is the subgroup of pseudo-reflections in G. Thus, if G does not contain any pseudo-reflections, the result is immediate and we may assume that G contains a pseudo-reflection, call it, h. Since G is not cyclic, it follows that $\#H = p$ where $H = \langle h \rangle$. Moreover, since G is an $\mathbb{F}_p$-vector space of dimension 2, it can only have sub-vector spaces of dimension 0, 1, or 2. Setting $\widetilde{H} \leq G$ to be the subgroup of G of all pseudo-reflections, we have $H \leq \widetilde{H}$, $\dim_k(\widetilde{H}) \neq 0, 2$, and therefore $\widetilde{H} = H$. Consider G/H. We have $\#G/H = p$ and therefore $G/H \cong \mathbb{Z}/p\mathbb{Z}$. Thus R^G is a unique factorization domain if and only if there are no non-trivial one-dimensional representations of $\mathbb{Z}/p\mathbb{Z}$. Suppose such a representation exists, call it, π. We must have $\pi(g) = x \neq 1 \in k^\times$ where $g \in \mathbb{Z}/p\mathbb{Z}$ is a generator. The characteristic polynomial for $\pi(g)$ must divide $T^P - 1 = (T-1)^P \in k[T]$. But $k[T]$ is a unique factorization domain and the characteristic polynomial for $\pi(g)$ is $T - x$ which is a contradiction. $\square$

Notice that we make no restrictions on the type of action in Theorem 7.1, i.e., we do not require the action to be faithful. In either case, i.e. faithful or not, R^G is of finite type over the field k and therefore has a canonical module. Recall that if the action of G on R is faithful, then R^G is normal and the canonical module is isomorphic to an unmixed ideal of height one in R^G, that is, ω_{R^G} can be identified with a divisor on $\operatorname{Spec}(R^G)$. Thus, when the action of G on R is faithful, we get that ω_{R^G} is cyclic and therefore R^G is quasi-Gorenstein. The next question to ask is if R^G is quasi-Gorenstein when $G = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_t}\mathbb{Z}$. To answer this, we prove once again that R^G is a unique factorization domain.

Theorem 7.2. *Let $G = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_t}\mathbb{Z}$ act on $R = k[x_1, \ldots, x_n]$ with $\operatorname{char} k = p$. The ring of invariants, R^G, is a unique factorization domain.*

Proof. Again, if G does not contain any pseudo-reflections, then the result is immediate so we may assume G contains a pseudo-reflections. Consider the subgroup $H \leq G$ generated by all the pseudo-reflections of G. It is clear $\#H = p^c$ for some $c \leq a_1 + \cdots a_t$ and therefore $\#G/H = p^{a_1 + \cdots a_t - c}$. If G/H is cyclic, then Corollary 3.12 applies and we are done. Suppose G/H is not cyclic and $\varphi\colon\ G/H \to k^\times$ is a non-trivial homomorphism. Since φ is non-trivial, there exists a generator $\overline{g} \in G/H$ such that $\varphi(\overline{g}) = x \neq 1 \in k^\times$. But any generator $\overline{g} \in G/H$ is the image of a generator in G and therefore $\#\langle \overline{g} \rangle = p^b$ with $b \leq a_i$ for some i, that is, $\langle \overline{g} \rangle \cong \mathbb{Z}/p^b\mathbb{Z}$. If $b = 1$, then by the same argument as in the proof of Theorem 7.1 we get a contradiction. If $b \neq 1$, then $\langle g \rangle \cong \mathbb{Z}/p^\alpha\mathbb{Z}$ and this contradicts the relationship between p^α and the dimension of the representation required by Theorem 2.3. □

As before, we make no assumptions in Theorem 7.2 regarding the faithfulness of the action of G. Thus, regardless of the choice of action of G on R, R^G is a unique factorization domain. In addition, since R^G is of finite type over the field k regardless of the choice of action of G on R, R^G admits a canonical module. If we assume the action of G is faithful, then R^G is normal and we can apply Theorem 7.2 to see that R^G is quasi-Gorenstein.

As an application of Theorem 7.2 we again study the a-invariant of R^G. Consider the natural filtration of G given by successively taking a filtration of one factor while holding the others constant. For example, suppose $a_1 = a_2 = a_3 = 2$ and consider the filtration

$$\begin{aligned} G =&\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \geq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \\ &\geq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times 0 \geq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times 0 \geq \cdots . \end{aligned}$$

Note that Theorem 7.2 tells us each of these subgroups gives a ring of invariants which is a unique factorization domain. Moreover, if the action of G is faithful, then the corresponding rings of invariants for each of these subgroups is quasi-Gorenstein. Applying this, the same argument as in Theorem 4.6 gives a bound for the a-invariant of R^G in terms of any one of its subgroups. For example, denoting the subgroups $N_{i,j,\ell} = \mathbb{Z}/p^i\mathbb{Z} \times \mathbb{Z}/p^j\mathbb{Z} \times \mathbb{Z}/p^\ell\mathbb{Z}$ in the previous example, we get

$$a(R^G) \leq a(R^{N_{2,2,1}}) \leq a(R^{N_{2,2,0}}) \leq a(R^{N_{2,1,0}}) \leq a(R^{N_{2,0,0}}) \leq a(R^{N_{1,0,0}}) \leq a(R).$$

Further, if G is any group with a normal, abelian, p-Sylow subgroup and quasi-Gorenstein ring of invariants, then this allows us to bound the a-invariant for R^G which extends Corollary 4.9.

7.1 Bounds for the Hilbert-Kunz Multiplicity of Rings of Invariants for Abelian p-Groups

We now consider extending the results regarding Hilbert-Kunz multiplicity when G is a cyclic p-Group to the more general case of G abelian. Suppose $G = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_t}\mathbb{Z}$ and consider $P = \mathbb{Z}/p^{a_1}\mathbb{Z} \times 0 \times \cdots \times 0 \leq G$. We have $R^G \subseteq R^P$ and we can use this containment to bound the Hilert-Kunz multiplicity of R^G. Moreover, since P is a cyclic p-group, even if R^P is not easily understood we can again apply the same techniques as in Chapter 5 to reduce to the case of a subgroup $N \leq P$ where R^N is understood.

Recall G/P acts naturally on R^P with ring of invariants R^G. The Hilbert ideal of R^G in R^P, that is, the ideal in R^P generated by homogeneous invariants of positive degree, is given by $\mathcal{H} = \mathfrak{m} \cdot R^P$ where $\mathfrak{m}$ is the homogeneous maximal ideal of R^G. Recall we use $\operatorname{td}((R^P)_G)$ to denote the largest degree in which $f \in (R^P)_G$ is non-zero where $(R^P)_G$ is the algebra of coinvariants for the action of G/P on R^P. Denoting the homogeneous maximal ideal of R^P by $\mathfrak{n}$, it is clear that $\mathfrak{n}$ is G/P-stable. As before, since $\operatorname{td}((R^P)_G) < \infty$, it follows that $\mathfrak{n}^{\operatorname{td}((R^P)_G)+1} \subseteq \mathfrak{m} \cdot R^P$. This yields the following result.

Theorem 7.3. *If $G = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_t}\mathbb{Z}$ acts on $R = k[x_1, \ldots, x_n]$ with* $\operatorname{char} k = p$ *and $P = \mathbb{Z}/p^{a_1}\mathbb{Z} \times 0 \times \cdots \times 0 \leq G$, then*

$$e_{HK}(R^G) \leq \frac{\binom{\operatorname{td}((R^P)_G)+n}{n}}{\#(G/P)} e(\mathfrak{n}, R^P).$$

Proof. This follows in a similar manner to the proof of Theorem 5.10. □

Applying this theorem and Theorem 5.12 immediately yields analogues of Corollary 5.13 and Theorem 5.16. Also note, we made a choice to work with the first factor subgroup of G. This theorem holds for any choice of factor subgroup and therefore it may be possible to simplify the computation of the bound by choosing the factor subgroup which has the simplest representation, i.e., the factor group, P, for which computing $e(R^P)$, and hopefully $\operatorname{td}((R^P)_G)$ as well, is the easiest. Note, as in the case of cyclic p-groups, computing $\operatorname{td}((R^P)_G)$ may be quite difficult regardless of which choice of subgroup $P \leq G$ is made.

Example 7.2. Let $G = (\mathbb{Z}/3\mathbb{Z})^\times \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $R = \mathbb{F}_3[x, y, z]$. Suppose G acts by the representation

$$\pi((c,0,0)) = \begin{bmatrix} c & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{bmatrix}, \pi((1,1,0)) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \pi((1,0,1)) = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Notice, the subgroup $N = 1 \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a normal p-Sylow subgroup of G. Applying

Theorem 5.10 yields

$$e_{HK}(R^G) \leq \frac{\binom{2+3-1}{3} e(\mathfrak{n}, R^N)}{2} = 2e(\mathfrak{n}, R^N).$$

To apply Theorem 7.3 we can choose either $P' = 1 \times \mathbb{Z}/3\mathbb{Z} \times 0 \leq N$ or $P = 1 \times 0 \times \mathbb{Z}/3\mathbb{Z} \leq N$. Notice the first option gives P' acting on R by the indecomposable action whereas the second option, after a change of basis, gives P acting on R with representation $V_2 \oplus V_1$. Thus if we choose the second option, then $e(R^P) = 1$ since $R^P \cong k[x, y, z^3 - xz^2]$, whereas we will require additional computations to find $e(R^{P'})$. Choosing P and applying Theorem 7.3 gives

$$e_{HK}(R^G) \leq 2(3!)e_{HK}(\mathfrak{n}, R^N) \leq 12 \frac{\binom{\mathrm{td}((R^P)_N)+3}{3}}{3} e(R^P) = 4\binom{\mathrm{td}((R^P)_N) + 3}{3}.$$

References

[1] M. Asgharzadeh. A Note on Hilbert-Kunz Multiplicity. *arXiv:1603.04297*, 2016.

[2] D.J. Benson. *Polynomial Invariants of Finite Groups.* Cambridge University Press, Cambridge, Great Britain, 1993.

[3] M. Blickle and F. Enescu. On Rings with Small Hilbert-Kunz Multiplicity. *Proc. Amer. Math. Soc.*, 132:2505–2509, 2004.

[4] N. Bourbaki. *Commutative Algebra Chapters 1-7.* Springer, New York, NY, 1989.

[5] Abraham Broer. *On Chevalley–Shephard–Todd's Theorem in Positive Characteristic*, pages 21–34. Birkhäuser Boston, Boston, 2010.

[6] W. Bruns and J. Herzog. *Cohen-Macaulay Rings.* Cambridge University Press, New York, USA, 1993.

[7] H.E.A. Campbell and I.P. Hughes. Vector Invariants of $U_2(\mathbf{F}_p)$: A proof of a conjecture of Richman. *Adv. Math.*, 126:1–20, 1997.

[8] J. Chan. *Integer Torsion in Local Cohomology, and questions on Tight Closure Theory.* ProQuest LLC, University of Utah, 2011.

[9] G. Ellingsrud and T. Skjelbred. Profondeur d'Anneaux d'Invariants en Caractéristique p. *Compos. Math.*, 41:233–244, 1980.

[10] P. Fleischmann, M. Sezer, R.J. Shank, and C.F. Woodcock. The Noether Numbers for Cyclic Groups of Prime Order. *Adv. Math.*, 207:149–155, 2006.

[11] P. Fleishmann. The Noether Bound in Invariant Theory of Finite Groups. *Adv. Math.*, 156:23–32, 2000.

[12] C. Han and P. Monsky. Some Surprising Hilbert-Kunz Functions. *Math. Z.*, 214:119–135, 1993.

[13] D. J. Hernández and J. Jeffries. Local Okounkov Bodies and Limits in Prime Characteristic. *arXiv:math/1701.02575v1*, 2017.

[14] M. Hochster and J.A. Eagon. Cohen-Macualay Rings, Invariant Theory, and the Generic Perfection of Determinental Loci. *Amer. J. Math.*, 93:1020–1058, 1971.

[15] M. Hochster and C. Huneke. Tight Closure and Strong F-regularity. *Mém. Soc. Math. France*, 38:119–133, 1989.

[16] M. Hochster and C. Huneke. Tight Closure, Invariant Theory and the Briançon-Skoda Theorem. *J. Amer. Math. Soc.*, 3:31–116, 1994.

[17] S. B. Iyengar, G. J. Leuschke, A. Leykin, C. Miller, E. Miller, A. K. Singh, and U. Walther. *24 Hours of Local Cohomology.* American Mathematical Society, United States of America, 2007.

[18] J. Jeffries. *Rings of Invariants, F-Regularity, and Local Cohomology.* ProQuest LLC, University of Utah, 2015.

[19] M. Katzman, K. Schwede, A. K. Singh, and W. Zhang. Rings of Frobenius Operators. *Math. Proc. Camb. Phil. Soc.*, 157:151–167, 2014.

[20] G. Kemper. Calculating Invariant Rings of Finite Groups over Arbitrary Fields. *J. of Symbolic Comput.*, 21:351–366, 1996.

[21] G. Kemper. On the Cohen-Macaulay Property for Modular Invariants. *J. Algebra*, 215:330–351, 1999.

[22] M. Kohl and M. Sezer. On the Top Degree of Coinvariants. *Int. Math. Res. Not.*, 22:6079–6093, 2014.

[23] A. Kustin, C. Polini, and B. Ulrich. Integral Extensions and the a-invariant. *J. Pure Appl. Algebra*, 2016:2800–2806, 2012.

[24] É. Lucas. Théorie des Fonctions Numériques Simplement Périodiques. *Amer. J. of Math.*, 1:184–196, 1878.

[25] G. Lyubeznik and K. E. Smith. Strong and Weak F-Regularity are Equivalent for Graded Rings. *Amer. J. Math.*, 121:1279–1290, 1999.

[26] G. Lyubeznik and K. E. Smith. On the Commutation of the Test Ideal with Localization and Completion. *Trans. Amer. Math. Soc.*, 353:3149–3180, 2001.

[27] P. Monsky. The Hilbert-Kunz Function. *Math. Ann.*, 263:43–49, 1983.

[28] P. Monsky. Transcendence of Some Hilbert-Kunz Multiplicities (modulo a conjecture). *arXiv:0908.0971*, 2009.

[29] M. D. Neusel and L. Smith. *Invariant Theory of Finite Groups.* American Mathematical Society, United States of America, 2002.

[30] D. Rees. $\mathfrak{a}$-Transforms of Local Rings and a Theorem on Multiplicities of Ideals. *Proc. Cambridge Phil. Soc.*, 57:8–17, 1961.

[31] D. Richman. On Vector Invariants over Finite Fields. *Adv. Math.*, 81:30–65, 1990.

[32] M. Sezer and R. J. Shank. On the Coinvariants of Modular Representations of Cyclic Groups of Prime Order. *J. Pure Appl. Algebra*, 205:210–225, 2006.

[33] K. Yoshida and K. Watababe. Hilbert-Kunz Multiplicity and an Inequality between Multiplicity and Colength. *J. Algebra*, 230, 2000.

[34] K. Yoshida and K. Watababe. Hilbert-Kunz Multiplicity of Two-Dimensional Local Rings. *Nagoya Math. J.*, 162, 2001.