MODULAR REPRESENTATIONS AND INVARIANTS FOR THE EXTRASPECIAL p-GROUP OF ORDER p^3 AND EXPONENT p

by

Christos Sarakasidis

University of Kent

A thesis submitted for the degree of

Doctor of Philosophy

supervised by

Dr. R. J. Shank

20th March, 2019

Declaration

I hereby declare that the content of this dissertation is my own and where work from outside sources has been used it has been properly and accurately cited.

Christos Sarakasidis
20th March, 2019

Acknowledgements

First and foremost, I thank wholeheartedly my supervisor Dr. R. J. Shank for the endless observations, suggestions and corrections throughout my whole journey. Always available whenever I needed help with an uncanny patience to give a mathematical sense to every erroneous statement I would address.

I would like to thank also professors Eddy Campbell and David Wehlau, for all the inspiring work in [7] and [8]; both have been part of the foundations of the entire thesis by providing an excellent source and reference for many of our ideas and results.

Furthermore, my sincere gratitude to the University of Kent for all the support and excellent working place they provided to me the last four-years.

Thanks to all who made me feel comfortable and welcome from the very first day I stepped into the University of Kent facilities. A special thank goes to Claire Carter who helped out every single time. She has been always there providing continuously guidance and help.

I would like to thank my best friends Dimos and Pantzos who made England looking a fun place to be and soothed the stress all these years. My friend Dimitris for the endless mathematical conversations and shared love for basketball ♣. Michele, Larry and Alan for being the best officemates with a great taste on beer.

The deepest thank and gratitude goes to my parents Ilias and Smaro for their unwavering support throughout my life. No words can describe the meaning of their contribution in all this. Finally, I am deeply indebted for her endless support, patience and how much shiny made this experience look like, to the love of my life Katia.

Abstract

The purpose of this thesis is to investigate modular representations and invariants of the extra-special group of order p^3 and exponent p denoted by H.

The material is organized in four chapters. In Chapter 1 we introduce basic definitions and results from commutative algebra, representation theory and invariant theory that will be used throughout this document and we fix our notation. In Chapter 2 we classify modular representations of H based on their socle-type. In particular, for a field extension $\mathbf{F}_p \subset \mathbf{F}$ we prove the existence of a suitable generating set for the group of representing matrices when V is a three- and four-dimensional $\mathbf{F}H$-module.

Using the classification results, when V is three-dimensional we construct a suitable set of invariants where we apply the SAGBI/divide-by-x algorithm. During the subduction various constraints show up, hence we split this chapter in two cases; generic and non-generic. Regardless the case, SAGBI/divide-by-x algorithm returns a generating set for $\mathbf{F}[V]^H$ and proves that is a complete-intersection ring.

In Chapter 4 representations assumed to be four-dimensional. This time the classification is more complicated and the only possible socle-types are $(1,1,1,1), (1,1,2)$, $(1,2,1)$ and $(2,1,1)$. For each one of them we compute $\mathbf{F}(V)^H$ and we use the invariant field generators to investigate the structure of $\mathbf{F}[V]^H$.

For type-$(1,1,1,1)$ invariants we prove that the group of representing matrices is not generated by bireflections, hence $\mathbf{F}[V]^H$ fails to be Cohen-Macaulay. Also for $p = 5$ we show the existence of a partial hsop which is not a regular sequence. For type-$(1,1,2)$ although the representing matrices form a bireflection group, we construct a partial hsop that we conjecture is not regular sequence for any prime. The classification of type-$(1,2,1)$ representations yields two classes with distinct socle-tabloids. For the first class we collect evidence on MAGMA that for $p = 3, 5$ and 7, $\{x_1, x_2, \mathbf{N}_H(x_3)\}$ is not acting regularly on $\mathbf{F}[V]^H$, hence that $\mathbf{F}[V]^H$ is not Cohen-Macaulay. For the second we apply SAGBI/divide-by-x on the set of invariant field generators, however due to the high complexity in computations generic computations are forbidden. So we present computational evidence that $\mathbf{F}[V]^H$ is complete intersection with embedding dimension six. For the remaining case of type-$(2,1,1)$ representations, $\mathbf{F}[V]^H$ is Cohen-Macaulay. However, evidence collected for $p = 3, 5$ and 7 using MAGMA, indicates that $\mathbf{F}[V]^H$ is not a complete intersection ring. To prove this we count the number of algebraic relations and use a characterization of complete intersection rings in terms of Koszul homology.

Contents

Chapter 1

Introduction

1.1 Overview

Invariant theory is the study of objects that preserve a certain symmetry. Usually this symmetry comes from the action of a group G on a commutative ring R. To comprehend this mathematically we use representation theory. So invariant and representation theory are closely related from this point of view. The contemporary approach of representation theory dictates the usage of modern techniques like derived categories, sheaves and various cohomology theories. However, invariant theorists use commutative theoretic machinery and sometimes develop their own tools when deeper questions come up.

Like representation theory we split invariant theory in modular and non-modular case. Many questions known to be true in the non-modular case, fail dramatically in the modular case. The reason is mainly that modular invariant theory contains classes of groups with wild representation theory and their complexity is reflected to invariant theory too.

In this thesis we study the modular invariant theory of a particular p-group over field extensions $\mathbf{F}_p \subset \mathbf{F}$. A p-group G is called extraspecial if the center $Z(G)$ is cyclic and the quotient $G/Z(G)$ is non-trivial elementary abelian, while the exponent of a finite group is the least common multiple of the orders of all elements. The group of our interest is the extraspecial group of order p^3 and exponent p denoted by H. To study H we use the following presentation

$$H = \langle g_1, g_2 \mid g_1^p = g_2^p = e, [g_1, [g_1, g_2]] = e, [g_2, [g_1, g_2]] = e, [g_1, g_2]^p = e \rangle,$$

while for a more intuitive approach we look at the archetypal representation of extraspecial groups, the finite Heisenberg group

$$H \cong \mathrm{UT}_3(\mathbf{F}_p) = \left\{ \begin{bmatrix} 1 & c_{1,2} & c_{1,3} \\ 0 & 1 & c_{2,3} \\ 0 & 0 & 1 \end{bmatrix} \middle| \, c_{i,j} \in \mathbf{F}_p \right\}.$$

1.2 Preliminaries.

1.2.1 Basic Definitions & Notation.

This chapter is intended to introduce basic definitions and set up the notation that will be used throughout this thesis. We first introduce the main object of study.

Suppose $G \subset \mathrm{GL}(V)$ is a finite group and let $V^* := \mathrm{Hom}(V, \mathbf{F})$ denote the dual vector space of V. Then V^* becomes a right $\mathbf{F}G$-module with $g \in G$ acting on a linear functional $x \in V^*$: $(x \cdot g)(u) = x(g \cdot u)$.

Given an $\mathbf{F}G$-module V, the symmetric algebra of the dual $\mathrm{Sym}(V^*) = T(V^*)/\langle u \otimes w - w \otimes u \,|\, u, w \in V \rangle$, up to graded isomorphism is identified with $\mathbf{F}[V] = \mathbf{F}[x_1, \ldots, x_n]$, the polynomial ring on n-variables. Therefore, the action of G on V^* can extend to an action by degree preserving algebra automorphisms on $\mathbf{F}[V]$.

Definition 1.2.1.1. *Let $\mathbf{F}$ be a field and V an n-dimensional $\mathbf{F}$-vector space. Assume $G \subset \mathrm{GL}(V)$ denotes a finite group. The set of polynomials in $\mathbf{F}[V]$ which are invariant under the G-action form a subalgebra called the invariant ring and is denoted by $\mathbf{F}[V]^G$,*

$$\mathbf{F}[V]^G = \{ f \in \mathbf{F}[V] \mid f \cdot g = f, \forall g \in G \}.$$

Given an element $f \in \mathbf{F}[V]$ it is useful to know how to turn f into an invariant. This can be achieved in two ways.

Definition 1.2.1.2. *Let $f \in \mathbf{F}[V]$ and $G \leq \mathrm{GL}(V)$, we define the* ***stabilizer*** *of f under G by $G_f := \{ g \in G \mid f \cdot g = f \}$. Given a subgroup $H \leq G$, we define the* ***relative norm*** *and* ***relative transfer*** *of f by the formulas*

$$\mathbf{N}_H^G(f) := \prod_{g \in G/H} f \cdot g\,, \;\; \mathbf{Tr}_H^G(f) := \sum_{\sigma \in G/H} f \cdot g.$$

Here $g \in G/H$ represents a coset representative. When $H = G_f$, we call the invariants

$$\mathbf{N}_G(f) := \mathbf{N}_{G_f}^G(f) = \prod_{g \in G/G_f} f \cdot g\,, \;\; \mathbf{Tr}(f) := \sum_{\sigma \in G/G_f} f \cdot g,$$

the norm and transfer of f respectively.

Notice that since the action of G on $\mathbf{F}[V]$ is always assumed to be degree-preserving, the transfer $\mathbf{Tr}(f)$ has the same degree with f, whereas the norm $\mathbf{N}(f)$ greater. Nevertheless, turns out that the norms are quite interesting and useful family of invariants.

A monomial in $\mathbf{F}[V]$ is a term of the form $\mathbf{x}^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, for a vector $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. A **monomial order** on $\mathbf{F}[V]$ is a total ordering on the set of monomials $\mathcal{M} := \{ \mathbf{x}^\alpha \mid \alpha \in \mathbb{N}^n \} \subset \mathbf{F}[V]$. This means given $\mathbf{x}^\alpha, \mathbf{x}^\beta \in \mathcal{M}$, exactly one of the following three relations must hold

$$\mathbf{x}^\alpha < \mathbf{x}^\beta, \; \mathbf{x}^\alpha = \mathbf{x}^\beta \text{ or } \mathbf{x}^\alpha > \mathbf{x}^\beta.$$

Given a polynomial $f \in \mathbf{F}[V]$ we define the **lead monomial**, $\mathrm{LM}_\prec(f)$, to be the largest term appearing in f with respect to that order. The coefficient of this term in f is called **lead coefficient** and is denoted by $\mathrm{LC}_\prec(f)$. Finally, the product of these two is called the **lead term** of f and is denoted by $\mathrm{LT}_\prec(f) = \mathrm{LC}_\prec(f)\mathrm{LM}_\prec(f)$.

Throughout this thesis we fix a specific term order, the graded reverse lexicographical order (**grevlex**) with $x_1 < x_2 < \cdots < x_n$. Thus, $\mathbf{x}^\alpha < \mathbf{x}^\beta$ if $\deg(\mathbf{x}^\alpha) < \deg(\mathbf{x}^\beta)$, or if $\deg(\mathbf{x}^\alpha) = \deg(\mathbf{x}^\beta)$ but the first nonzero element from the left in $\alpha - \beta$ is positive. When that term order is considered, we denote $\mathrm{LT}(f) = \mathrm{LC}(f)\mathrm{LM}(f)$ without explicitly referring to the term order $\prec$.

1.3 Commutative Algebra.

Invariant theory is the study of structure of a specific class of commutative rings. Since $\mathbf{F}[V]^G$ is a subring of $\mathbf{F}[V]$, one naturally asks what nice properties of $\mathbf{F}[V]$ are inherited to $\mathbf{F}[V]^G$. When G is finite, a celebrated theorem of Emmy Noether (1915) (see, [8, Theorem 3.1.2]) shows that $\mathbf{F}[V]^G$ is finitely generated. Thus the ring of invariants $\mathbf{F}[V]^G$ is always Noetherian. However, these are not the only nice properties that $\mathbf{F}[V]^G$ inherits, since forms an example of a graded connective algebra too.

Definition 1.3.0.1. *We call a ring R (positively)* ***graded****, if we can find additive subgroups $R_i \leq R$, for $i \in \mathbb{N}$ such that $R = \oplus_{i\in\mathbb{N}} R_i$ and $R_i R_j \subset R_{i+j}$. Furthermore, we call $r \in R$* ***homogeneous****, if $r \in R_i$ for some $i \in \mathbb{N}$. A graded algebra R is called* ***connective****, if it is a graded ring such that $R_0 = \mathbf{F}$.*

Definition 1.3.0.2. *Assume R is a graded algebra and let $I \triangleleft R$ denote an ideal. We call I* ***homogeneous*** *if it can be generated by homogeneous elements.*

Moreover, for connective algebras there is a unique maximal homogeneous ideal $R_+ \triangleleft R$ generated by all elements of positive degree. The class of *graded local* Noetherian rings is an interesting class for us. Many important theorems of the theory of local rings can be proven to be true in these context too, hence applied to the case $R = \mathbf{F}[V]^G$.

Definition 1.3.0.3. *Let R denote a Noetherian commutative ring and $\mathfrak{p} \triangleleft R$ a prime ideal. We call* ***height*** *of $\mathfrak{p}$ and we denoted by $\mathrm{hg}(\mathfrak{p})$, the length of a maximal chain of prime ideals, $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_i = \mathfrak{p}$.*

We call the maximum height of proper prime ideals the ***Krull dimension*** *of R and we denote it by $\dim(R)$.*

Let $R \subset S$ be an extension of rings. Choose an element $a \in S$. We call this element **integral** over R if there is a monic polynomial $f \in R[x]$, such that $f(a) = 0$. If every element in S is integral over R we say that S is an **integral extension** of R. If S is a finitely generated F-algebra, then S is integral over R if and only if S is a finite R-module. The set of all elements in S integral over R form a subring, denoted by $\overline{R}$. This subring is known as the integral closure of R in S. If $R = \overline{R}$, then R is said to be **integrally closed** in S.

In the following theorem, we prove that $\mathbf{F}[V]^G \subset \mathbf{F}[V]$ is integral.

Theorem 1.3.0.4. *[8, 3.0.4] Let $G \subset \mathrm{GL}(V)$ be a finite group, then the extension $\mathbf{F}[V]^G \subset \mathbf{F}[V]$ is integral.*

Proof. Pick an $h \in \mathbf{F}[V]$ and assume $|G| = n$; it is not difficult to observe, that the monic polynomial

$$F(t) = \prod_{g \in G}(t - h \cdot g) = t^{|G|} + f_{n-1}t^{n-1} \cdots + f_0,$$

has h as a root, i.e., $F(h) = 0$. Now the action of G on $\mathbf{F}[V]$ can be extended to $\mathbf{F}[V][t]$ by setting $t \cdot g = t, \forall g \in G$. Under this action, we get $F(t) \in \mathbf{F}[V][t]^G$. Therefore, $f_i \cdot g = f_i, \forall g \in G, \forall i \in \{1, \dots, n\}$. In other words, $F(t) \in \mathbf{F}[V]^G[t]$. So it follows that the extension $\mathbf{F}[V]^G \subset \mathbf{F}[V]$ is integral. $\square$

An important property of integral extensions is that when $R \subset S$ is integral $\dim(R) = \dim(S)$. Therefore, using the theorem implies $\dim(\mathbf{F}[V]^G) = \dim(\mathbf{F}[V]) = \dim_{\mathbf{F}}(V)$.

Next we introduce a notion that will be used extensively in the entire thesis.

Definition 1.3.0.5. *Let R denote a commutative $\mathbf{F}$-algebra with $\dim(R) = n$. Assume that $S = \{f_1, \dots, f_n\} \subset R$ is a set of homogeneous elements and let $A = \mathbf{F}[f_1, \dots, f_n]$ denote the algebra generated by S. We call S a homogeneous system of parameters (**hsop**), if R is a finitely generated A-module, i.e., $\exists\, g_1, \dots, g_k \in R$ such that $R = \sum_{i=1}^{k} Ag_i$.*

We call A a Noether Normalization of R. Since any two Noether Normalizations are isomorphic up to isomorphism we can talk for *the* Noether Normalization of R.

When the case $R = \mathbf{F}[V]^G$ is considered, any hsop is referred as the **primary invariants** while the corresponding module generators g_i as the **secondary invariants**.

Two questions arising immediately; given an $\mathbf{F}$-algebra R, when such an hsop exists? If we know about its existence, how do we distinguish whether a given subset $\{f_1, \ldots, f_n\} \subset R$ of homogeneous elements is an hsop? Fortunately, in good cases we have an answer for both questions. The first comes from a famous and powerful theorem of Emmy Noether (1926) [17] (originally proved by D. Hilbert) with interesting applications both in algebra and geometry, the so-called Noether Normalization lemma.

Theorem 1.3.0.6 (Noether Normalization Lemma)**.** *[8, Theorem 2.6.1] Assume that R is a finitely generated connected $\mathbf{F}$-algebra. Then R has an hsop.*

The second question when $R = \mathbf{F}[V]^G$, can be answered by giving a geometric criterion in the algebraic closure of $\mathbf{F}$.

Lemma 1.3.0.7. *[8, 2.6.3] Let V be an n-dimensional $\mathbf{F}$-vector space and $\overline{\mathbf{F}}$ the algebraic closure of $\mathbf{F}$. Assume that $f_1, \ldots f_n \in \mathbf{F}[V]^G$ are homogeneous invariants and that $\overline{V} = V \otimes_{\mathbf{F}} \overline{\mathbf{F}}$. Then $\{f_1, \ldots, f_n\}$ forms an hsop if and only of $\mathcal{V}_{\overline{V}}(f_1, \ldots, f_n) = \{0\}$. Here the latter denotes the zero-locus of $f_1, \ldots, f_n$ in the closure of V, that is,*

$$\mathcal{V}_{\overline{V}}(f_1, \ldots, f_n) = \{\, v \in V \mid f_1(v) = \cdots = f_n(v) = 0 \,\}.$$

An interesting aspect of integral extensions is the transitivity property. If $R \subset L \subset S$ are ring extensions with L integral over R and S integral over L, then S is integral over R as well. So if $A = \mathbf{F}[f_1, \ldots, f_n]$ is a Noether normalization of $\mathbf{F}[V]^G$, follows that $A \subset \mathbf{F}[V]$ is integral and A is a Noether normalization of $\mathbf{F}[V]$ too. Based on this fact we obtain the following theorem.

Theorem 1.3.0.8. *[5, Theorem 5, pg.112] If $A = \mathbf{F}[f_1, \ldots, f_n]$ is a Noether normalisation (for some group), then $\mathbf{F}[V]$ is a free graded A-module of rank $\prod_{i=1}^{n} \deg(f_i)$ and top degree $\sum_{i=1}^{n}(\deg(f_i) - 1)$.*

1.3.1 Cohen-Macaulay ring.

An important question for a graded commutative ring R in commutative algebra is whether it has the Cohen-Macaulay property. The standard textbook for Cohen-Macaulay rings is [4].

Definition 1.3.1.1. *Let R denote a commutative ring and M a left R-module. We say that $x \in R$ is M-**regular**, if $x \cdot m = 0$ for $m \in M$ implies $m = 0$, that is, if x is not a zero-divisor for M.*

A sequence $\underline{x} = (x_1, \ldots, x_n)$ of elements in R is called an M-regular sequence if the following two conditions are satisfied:

(1) $\forall i \in \{1, \ldots, n\}$, x_i is an $M/(x_1, \ldots, x_{i-1})M$-regular element,

(2) $M/\underline{x}M$ is not the zero module.

*We call a regular sequence $\underline{x}$ **maximal**, if it cannot be extended to a longer regular sequence.*

Assume that R is additionally Noetherian and let $I \triangleleft R$ be an ideal. If M is an R-module such that $IM \neq M$, then all the maximal M-sequences in I have the same length. We call this common length the depth of M and we denote it by $\operatorname{depth}_I(M)$. In particular, if R is graded local Noetherian with irrelevant ideal $R_+ \triangleleft R$, then length of any maximal M-sequence is called the **depth** of M and is denoted by $\operatorname{depth}_{R_+}(M)$. Since the underlying ring will always be clear from the context, we omit R_+ from the notation and simply write $\operatorname{depth}(M)$.

For the special case $R = M$ we have always $\operatorname{depth}(R) \leq \dim(R)$.

Definition 1.3.1.2. *A commutative graded ring R considered as an R-module is called Cohen-Macaulay if* $\operatorname{depth}(R) = \dim(R)$*.*

Since $\mathbf{F}[V]^G$ is a graded Noetherian finitely generated $\mathbf{F}$-algebra all the above definitions can be applied. In particular, for such algebra we have a very useful criterion to decide whether is Cohen-Macaulay.

Theorem 1.3.1.3. *[8, Theorem 2.8.1] Let A be a finitely generated connected graded $\mathbf{F}$-algebra which is Cohen-Macaulay. Then every hsop for A is a regular sequence for A.*

Equivalently, we can define Cohen-Macaulay rings as free modules over a Noether normalisation.

Theorem 1.3.1.4. *[3, 4.3.5] Let R be a graded connected Noetherian $\mathbf{F}$-algebra. The following are equivalent:*

(1) R is Cohen-Macaulay with $\dim R = n$,

(2) for $\{f_1, \ldots, f_n\} \subset R$ an hsop, R is a free $\mathbf{F}[f_1, \ldots, f_n]$-module,

(3) for any hsop $\{f_1, \ldots, f_n\} \subset R$, R is a free $\mathbf{F}[f_1, \ldots, f_n]$-module.

If $A = \mathbf{F}[f_1, \ldots, f_n] \subset \mathbf{F}[V]^G$ for $\{f_1, \ldots, f_n\}$ a set of primary invariants, then there is a minimal set of secondary invariants $g_1, \ldots, g_m \in \mathbf{F}[V]^G$ such that $\mathbf{F}[V]^G = \sum_{i=1}^{m} Ag_i$. The following theorem implies that the prior knowledge of m suffices to decide whether $\mathbf{F}[V]^G$ is Cohen-Macaulay.

Theorem 1.3.1.5. *[9, 3.7.1] Assume that the action of G on V is faithful and let $f_1, \ldots, f_n \in \mathbf{F}[V]^G$ be primary invariants of degrees $d_1, \ldots, d_n$. Furthermore, assume that $g_1, \ldots, g_m$ is a minimal system of secondary invariants. Then*

$$m \geq \frac{d_1 \cdots d_n}{|G|},$$

with equality if and only if $\mathbf{F}[V]^G$ is Cohen-Macaulay.

Another useful criterion for the Cohen-Macaulay property related with the number of secondary invariants is given in terms of the Hilbert Series.

For a graded $\mathbf{F}$-vector space $M = \oplus_{i=0}^{\infty} M_i$, the **Hilbert Series** of M is the formal power series

$$\mathcal{H}(M,t) := \sum_{i=0}^{\infty} \dim_{\mathbf{F}}(M_i) t^i.$$

Example 1.3.1.6. *A polynomial ring in one variable* $\mathbf{F}[x] = \oplus_{i=0}^{\infty} \mathbf{F}[x]_i$ *is a graded vector space. Assume* $\deg(x) = d$*, then the above formula implies*

$$\mathcal{H}(\mathbf{F}[x],t) = 1 + t^d + t^{2d} + \cdots = \frac{1}{1-t^d}.$$

Since one can prove that for graded vector spaces M, N*,* $\mathcal{H}(M \otimes N, t) = \mathcal{H}(M,t) \cdot \mathcal{H}(N,t)$*, for a given Noether normalisation* $A \subset \mathbf{F}[V]^G$ *with* $\deg(f_i) = d_i$*,*

$$\mathcal{H}(A,t) = \prod_{i=1}^{n} \frac{1}{1-t^{d_i}}.$$

Turns out that the prior knowledge of Hilbert series for $\mathbf{F}[V]^G$, contains very useful information for the primary and secondary invariants.

Theorem 1.3.1.7. *[5, Theorem 7, pg.113] Suppose* $A = \mathbf{F}[f_1, \ldots, f_n]$ *is a Noether normalisation of* $\mathbf{F}[V]^G$ *with* $\deg(f_i) = d_i$*. Then*

$$\mathcal{H}(\mathbf{F}[V]^G, t) = \frac{f(t)}{\prod_{i=1}^{n}(1-t^{d_i})},$$

for some polynomial $f(t)$ *with integer coefficients. If* $\mathbf{F}[V]^G$ *is Cohen-Macaulay then the coefficients of* $f(t)$ *are non-negative and* $\mathbf{F}[V]^G$ *is generated, as a A-module, by* $r := (\prod_{i=1}^{n} d_i)/|G|$ *homogeneous invariants.*

Given a subspace of an n-dimensional vector space $H \leq V$, the **codimension** of H is defined by $\operatorname{codim}(H) = n - \dim_{\mathbf{F}}(H)$. If G is acting on V, then we define the fixed point subspace $V^G = \{ v \in V \mid g \cdot v = v \}$.

Theorem 1.3.1.8. *[8, Theorem 3.9.2] Let* $G \leq \mathrm{GL}(V)$ *denote an arbitrary subgroup over a field* $\mathbf{F}$ *and* $\dim_{\mathbf{F}}(V) = n$*. Then*

(1) if $\dim_{\mathbf{F}}(V^G) = n-1$*, then* $\mathbf{F}[V]^H$ *is a polynomial algebra.*

(2) if $\dim_{\mathbf{F}}(V^G) = n-2$*, then* $\mathbf{F}[V]^H$ *is Cohen-Macaulay.*

We close this section by introducing a homological characterization for regular sequences. For this we follow the notation of [13].

For R a commutative ring and $x_1, \ldots, x_n \in R$ a sequence of arbitrary elements, we define the complex $K_\bullet := \{K_r, d_r\}$, $K_0 = R$, and $K_r = 0$ if r is not in the range $0 \leq r \leq n$. For $1 \leq r \leq n$, we set $K_r = \oplus Re_{i_1 .. i_r}$ to be the free R-module of rank $\binom{n}{r}$, with basis $\{e_{i_1 \ldots i_p} \mid 1 \leq i_1 < \cdots < i_p \leq n\}$. It can be proven that this module is isomorphic with the r-th exterior power of R, $\bigwedge^r R$. Furthermore, we define the boundary operators $d_r : K_r \to K_{r-1}$ on the basis elements by setting

$$d_r(e_{i_1 \cdots _r}) := \sum_{j=0}^{n} (-1)^{j-1} x_{i_j} e_{i_1 \ldots \hat{i_j} \cdots _r},$$

and extend this R-linearly on the entire K_r. Someone can verify that $d \circ d = 0$.

Definition 1.3.1.9. *We call the resulting chain complex the* ***Koszul complex*** *associated to* $\underline{x} := (x_1, \ldots, x_n)$ *and is denoted by* $K_\bullet(\underline{x}) := K_\bullet(x_1, \ldots, x_n)$*. For an* R*-module* M*, we set* $K_\bullet(\underline{x}, M) := K_\bullet(\underline{x}) \otimes_R M$ *for the complex obtained after applying* $- \otimes_R M$ *on the Koszul complex* $K_\bullet(\underline{x})$*.*

Notice that up to isomorphism of complexes the Koszul complex is independent of the choice of a minimal generating set. Let (R, R_+) be a graded local ring and $\{x_1, \ldots, x_n\}$ a minimal generating set of R_+. We call the number of elements occurring is such a minimal set the **embedding dimension** of R and we denote it by emb.dim(R). If $y_1, \ldots, y_n \in R_+$ is another minimal generating set, then there is a an $n \times n$ invertible matrix over R, $(\alpha_{ij}) \in \mathrm{GL}_n(R)$, such that: $y_i = \sum \alpha_{ij} x_j$. We can exploit this matrix and define an invertible morphism of complexes $f : K_R(y_1, \ldots, y_n) \xrightarrow{\cong} K_R(x_1, \ldots, x_n)$, defined by the rule $f_1(e'_i) = \sum \alpha_{ij} e_j$, and then extended it R-linearly on the basis of the exterior algebras $\bigwedge^r R$, $\{e_{i_1} \wedge \cdots \wedge e_{i_p} \mid 1 \leq i_1 < \cdots < i_p \leq n\}$ for each $r = 1, \ldots, n$. This morphism commutes with the boundary operators d, hence consists a well-defined isomorphism of complexes.

We can measure how far a Koszul complex is from being exact by taking homology at each position. The resulting homology groups of $K_\bullet(\underline{x}, M)$ are denoted by $H_r(K_\bullet(\underline{x}, M))$, or just $H_r(\underline{x}, M)$. We call $H_r(\underline{x}, M)$ the r-th Koszul homology of M associated to $\underline{x}$. From the definition of $K_\bullet(\underline{x}, M)$, we see that:

$$H_0(\underline{x}, M) \cong M/\underline{x}M, \;\; H_n(\underline{x}, M) \cong M/\underline{x}M \cong \{\, m \in M \mid x_1 \cdot m = \cdots = x_n \cdot m = 0 \,\}.$$

Applying an inductive argument we can prove the following theorem which relates regular sequences with Koszul complexes.

Theorem 1.3.1.10. *[13, Theorem 16.5, i] Let R be a ring, M an R-module and $x_1, \ldots, x_n \in R$ an M-sequence; then*

$$H_r(\underline{x}, M) = 0, \;\; \textit{for } r > 0, \;\; \textit{and } H_0(\underline{x}, M) = M/\underline{x}M.$$

So zero Koszul homology implies that the sequence is regular.

1.3.2 Complete Intersections

Following up the previous section, we introduce another class of commutative rings we are interested. The complete intersections rings. It can be proven that this class of rings is contained in the class of Cohen-Macaulay rings introduced before. So complete intersections can be thought as Cohen-Macaulay rings with some additional structure.

Definition 1.3.2.1. *Let R be a finitely generated $\mathbf{F}$-algebra with Krull dimension $\dim(R) = n$. Then R is called **complete intersection** ring if there is a presentation $p : \mathbf{F}[X_1, \ldots, X_k] \twoheadrightarrow R$, such that for $I := \ker(p)$ we can find a homogeneous generating set $r_1, \ldots, r_s$ which forms a regular sequence and additionally we have $k = n + s$.*

If $R = \mathbf{F}[f_1, \ldots, f_k]$, then it is a complete intersection if the ideal of relations consists of $k - \dim(R)$ homogeneous elements which form a regular sequence. From the definition it is clear that being complete intersection is independent of the choice of presentation. When we have a unique syzygy we give to R a special name.

Definition 1.3.2.2. *A complete intersection R such that $k - \dim(R) = 1$ is called* ***hypersurface****.*

There are Cohen-Macaulay rings which are not complete intersections. In [11], an example of a group $G \leq \mathrm{GL}_4(\mathbf{F})$ with this feature is given. However, it is an open question what class of groups gives Cohen-Macaulay invariant rings $\mathbf{F}[V]^G$ but not complete intersections.

Also in [23], Richard Stanley proves that $\mathbf{F}[V]^G$ has a minimal free resolution in a simple explicit form exactly when $\mathbf{F}[V]^G$ is a complete intersection. Generalizing this to arbitrary graded $\mathbf{F}$-algebras yields the following.

Proposition 1.3.2.3. *[23, Proposition 9.1] A graded $\mathbf{F}$-algebra R is a complete intersection if and only if the Koszul complex is a minimal free resolution.*

Finally, when R is an integral domain we obtain a simple counting argument to decide whether it is a complete intersection by looking at the dimension of the first Koszul homology as an $\mathbf{F}$-vector space. Before we prove this, we recall a well-known result that is one of the key ingredients of this proof.

Proposition 1.3.2.4 (Graded Nakayama Lemma)**.** *[8, Proposition 2.10.1] Let R be a finitely generated graded connected $\mathbf{F}$-algebra and M a finitely generated non-negatively graded R-module. Then the homogenous elements $f_1, \ldots, f_r$ generate M as an R-module if and only if their corresponding images span M/R_+M as an $\mathbf{F}$-vector space. Furthermore, they minimally generate M if and only if they form an $\mathbf{F}$-vector space basis of M/R_+M.*

Proposition 1.3.2.5. *Suppose that S is an integral domain minimally generated by k homogeneous generators. Then S is a complete intersection if and only if $\dim_{\mathbf{F}}(H_1(S)) = k - \dim(S)$.*

Proof. Choose a presentation $p : \mathbf{F}[X_1, \dots, X_k] := R \twoheadrightarrow S$. Since S is integral domain $\mathfrak{a} := \ker(p)$ is prime. Denote by $\mu(\mathfrak{a})$ a minimal generating set for $\mathfrak{a}$.

Let $X := (X_1, \dots, X_k)$ denote a regular sequence of R and $f := (f_1, \dots, f_k)$ denote their corresponding image in S. The Koszul complex of R associated to X is by definition

$$0 \to \bigwedge^k R \to \cdots \to \bigwedge^1 R \to R \to 0.$$

Since X is a regular sequence, the complex

$$0 \to \bigwedge^k R \to \cdots \to \bigwedge^1 R \to R \to R/R_+ = \mathbf{F} \to 0,$$

is exact. Therefore $K_R(X)$ is a free resolution of $\mathbf{F}$ as R-module. Tensoring out with $- \otimes_R S$ gives a chain complex

$$0 \to (\bigwedge^k R) \otimes_R S \to \cdots \to (\bigwedge^1 R) \otimes_R S \to R \otimes_R S \cong S \to 0.$$

Looking closer the modules of this complex, we observe that

$$(\bigwedge^k R) \otimes_R S \cong (\bigwedge^k R) \otimes_R R/\mathfrak{a} \cong \bigwedge^k R/\mathfrak{a} \cong \bigwedge^k S.$$

Thus, we obtain an isomorphism of complexes $K_R(X) \otimes_R S \cong K_S(f)$. Furthermore, the short exact sequence $0 \to \mathfrak{a} \to R \to S \to 0$ gives a long exact sequence ending in

$$\cdots \to \mathrm{Tor}_1^R(\mathbf{F}, \mathfrak{a}) \to \mathrm{Tor}_1^R(\mathbf{F}, R) \to \mathrm{Tor}_1^R(\mathbf{F}, S) \to \mathbf{F} \otimes_R \mathfrak{a} \to \mathbf{F} \otimes_R R \to \mathbf{F} \otimes_R S \to 0.$$

Notice that $H_1(R) = \mathrm{Tor}_1^R(\mathbf{F}, R) = 0$ since X is a regular sequence, while $\mathbf{F} \otimes_R R \cong \mathbf{F}$ and $\mathbf{F} \otimes_R S \cong R/R_+ \otimes_R S \cong S/R_+S \cong \mathbf{F}$. Also, $\mathbf{F} \otimes_R \mathfrak{a} = R/R_+ \otimes_R \mathfrak{a} = \mathfrak{a}/R_+\mathfrak{a}$. So the last sequence eventually becomes

$$\cdots \to \mathrm{Tor}_1^R(\mathbf{F}, \mathfrak{a}) \to 0 \to \mathrm{Tor}_1^R(\mathbf{F}, S) \to \mathfrak{a}/R_+\mathfrak{a} \to \mathbf{F} \xrightarrow{\cong} \mathbf{F} \to 0.$$

Therefore, we obtain an isomorphism $H_1(S) = \mathrm{Tor}_1^R(\mathbf{F}, S) \cong \mathfrak{a}/R_+\mathfrak{a}$. From the Graded Nakayama Lemma above we obtain $\dim_{\mathbf{F}}(H_1(S)) = \dim_{\mathbf{F}}(\mathfrak{a}/R_+\mathfrak{a}) = \mu(\mathfrak{a})$. Clearly now our assertion follows. $\square$

1.4 Invariant Theory

1.4.1 Structure of $\mathbf{F}[V]^G$.

As mentioned at the beginning there are huge differences in the structure of $\mathbf{F}[V]^G$ between the modular and non-modular case. For the non-modular case Maschke's Theorem implies that the category of $\mathbf{F}G$-modules is semisimple. Therefore any representation can be split in more handy pieces. For invariant theory, when $|G|$ is invertible in $\mathbf{F}$ we can define the **Reynolds Operator**

$$\begin{aligned} \mathcal{R} : \mathbf{F}[V]^H &\to \mathbf{F}[V]^G, \\ f &\mapsto \mathcal{R}(f) := \frac{1}{[G:H]}\mathrm{Tr}_H^G(f), \end{aligned}$$

for any subgroup $H \leq G$, which serves as a natural projection. In particular, setting $H = \{e_G\}$ yields an epimorphism from $\mathbf{F}[V]$ onto $\mathbf{F}[V]^G$ which yields a nice split: $\mathbf{F}[V] = \mathbf{F}[V]^G \oplus \ker(\mathrm{Tr}^G)$. On the other hand, when $|G|$ is not invertible in $\mathbf{F}$ all the above fall apart, hence we are obliged to use different tools.

Definition 1.4.1.1. *Let V be an $\mathbf{F}G$-module for some group G. We denote the fixed vectors of V by G*

$$V^G = \{\, v \in G \mid g \cdot v = v, \forall g \in G \,\},$$

while for $\sigma \in G$

$$V^\sigma = \{\, v \in G \mid \sigma \cdot v = v \,\}.$$

An element $\sigma \in G$ is called ***reflection*** *if $\dim_{\mathbf{F}}(V^\sigma) = \dim_{\mathbf{F}}(V) - 1$. We call σ* ***bireflection*** *if $\dim_{\mathbf{F}}(V^\sigma) \geq \dim_{\mathbf{F}}(V) - 2$.*

In the non-modular case many questions regarding the structure of $\mathbf{F}[V]^G$ have been answered. The following consists one of the most celebrated results.

Theorem 1.4.1.2 (Chevalley, Shepard, Todd)**.** *If $|G|$ is invertible in $\mathbf{F}^*$, then $\mathbf{F}[V]^G$ is polynomial if and only if G is generated by reflections.*

Although in the modular case the above theorem fails, J.P. Serre (see, [8, Corollary 12.2.5]) proves that one direction is still true.

Theorem 1.4.1.3 (J.P. Serre)**.** *Let G be a finite group. If $\mathbf{F}[V]^G$ is a polynomial ring, then the action of G on V is generated by reflections.*

An important result in non-modular invariant theory due to Hochster and Eagon, see [10], answers the question when $\mathbf{F}[V]^G$ is Cohen-Macaulay. Although the original version talks about a wider class of groups (linearly reductive) we restrict ourselves to the case of finite groups only.

Theorem 1.4.1.4 (Hochster-Eagon)**.** *If G is a finite group with $|G| \in \mathbf{F}^*$, then $\mathbf{F}[V]^G$ is Cohen-Macaulay.*

For the modular case the above fails. However, G. Kemper (see, [12, Corollary 2.7]) proves that one direction is still true when we restrict to the class of p-groups.

Theorem 1.4.1.5 (G. Kemper)**.** *Let $G \leq \mathrm{GL}(V)$ denote a p-group and suppose that $\mathbf{F}[V]^G$ is a Cohen-Macaulay ring. Then G is generated by bi-reflections*

Kemper's theorem provides an easy criterion to decide whether $\mathbf{F}[V]^G$ is not Cohen-Macaulay.

1.4.2 The invariant field $\mathbf{F}(V)^G$.

Since $\mathbf{F}[V]^G$ is always an integral domain we can define the field of fraction $\mathrm{Quot}(\mathbf{F}[V]^G)$. It is not difficult to see that generally $\mathrm{Quot}(\mathbf{F}[V]^G) \subset \mathbf{F}(V)^G$. However, when G is finite we have an equality $\mathrm{Quot}(\mathbf{F}[V]^G) = \mathbf{F}(V)^G$. To see this, observe that

$$\frac{f}{h} = \frac{f \prod\{h \cdot g \mid g \in G - \{1\}\}}{\{h \cdot g \mid g \in G\}}.$$

Then the denominator is the G-orbit of h, thus belongs to $\mathbf{F}[V]^G$. The latter implies that $f \prod\{h \cdot g \mid g \in G - \{1\}\} \in \mathbf{F}[V]^G$ as well. Therefore the equality of fields follows $\mathrm{Quot}(\mathbf{F}[V]^{G)} = \mathbf{F}(V)^G$. Let $\mathbf{F}(V)$ denote the field of fractions of $\mathbf{F}[V]$. Based on the last observation we obtain the following lemma.

Lemma 1.4.2.1. *[8, Lemma 3.0.1] For any finite group G,we have $\mathrm{Quot}(\mathbf{F}[V]^G) = \mathbf{F}(V)^G$. Consequently, the extension $\mathbf{F}(V)^G \subset \mathbf{F}(V)$ is Galois, with group G and so $\mathbf{F}(V)$ has dimension $|G|$ as a $\mathbf{F}(V)^G$ vector space.*

We call $\mathbf{F}(V)^G$ the **invariant field**.

Theorem 1.4.2.2. *[5, Theorem 8, pg.114] Suppose A is a graded subalgebra of $\mathbf{F}[V]^G$ such that A contains an hsop and a generating set for $\mathbf{F}(V)^G$. If A is integrally closed in its field of fractions, then $A = \mathbf{F}[V]^G$.*

Proof. Obviously we obtain $\mathrm{Quot}(A) = \mathbf{F}(V)^G$. Furthermore, since A contains an hsop of $\mathbf{F}[V]^G$, the latter becomes a finite A-module. If A is integrally closed in its field of fractions we have $A = \mathbf{F}[V]^G$. □

Another reason that makes hsop useful is that sometimes suffice to generate $\mathbf{F}[V]^G$. Using the last theorem gives the following.

Theorem 1.4.2.3. *[5, Theorem 9, 4] If V is a faithful representation, $\{f_1, \dots, f_n\}$ is an hsop for $\mathbf{F}[V]^G$, and $\prod_{i=1}^n \deg(f_i) = |G|$, then $\mathbf{F}[V]^G = \mathbf{F}[f_1, \dots, f_n]$.*

Proof. Since $\mathbf{F}[V]$ is a free A-module of rank $|G|$, follows that the field extension $\mathrm{Quot}(A) \subset \mathbf{F}[V]$ has degree $|G|$. However, the field extension $\mathbf{F}(V)^G \subset \mathbf{F}(V)$ is Galois and therefore has degree $|G|$ too. Finally, since every polynomial ring is UFD, A is integrally closed in its field of fraction, hence from the previous theorem we obtain $A = \mathbf{F}[V]^G$. □

Assume that $H \leq G$ is an arbitrary subgroup. Then obviously $\mathbf{F}[V]^G \subset \mathbf{F}[V]^H$. Since $\mathbf{F}[V]$ is integral over $\mathbf{F}[V]^G$ and $\mathbf{F}[V]^H$, implies that $\mathbf{F}[V]^G \subset \mathbf{F}[V]^H$ is integral too. Therefore an hsop for $\mathbf{F}[V]^G$ is also an hsop for $\mathbf{F}[V]^H$. Since $G \subset \mathrm{GL}(V)$, the above comments imply that an hsop of $\mathbf{F}[V]^{\mathrm{GL}(V)}$ is always an hsop of $\mathbf{F}[V]^G$ too. The following example constructs using the last two theorems a famous generating set for $\mathbf{F}[V]^{\mathrm{GL}(V)}$, the so-called Dickson invariants.

Example 1.4.2.4. *Assume that $\mathbf{F}_q$ is a finite field of order $q = p^s$ and let V be an n-dimensional vector space over $\mathbf{F}_q$. The group of invertible transformation of V, $\mathrm{GL}(V)$, is finite and in particular has cardinality $|\mathrm{GL}(V)| = \prod_{i=1}^{n}(q^n - q^{i-1})$. We define the following polynomials*

$$F_n(t) := \prod_{\phi \in V^*}(t - \phi) = \sum_{i=0}^{n}(-1)^{n-i} d_{i,n} t^{q^{n-i}},$$

where V^* denotes the dual space of V. Since V is finite dimensional we have $V \cong \mathbf{F}_q^n$. Therefore $|V| = q^n$ and so $|V^*| = q^n$ too. From the definition of $F_V(t)$ we observe that the coefficients $d_{i,n}$ must have $\deg(d_{i,n}) = q^n - q^{n-i}$. So the product over all i yields $\prod_{i=1}^{n} \deg(d_{i,n}) = |\mathrm{GL}(V)|$. These $d_{i,n}$ are known in the literature as the Dickson invariants. Although not obvious, they form an hsop of $\mathbf{F}[V]^{\mathrm{GL}(V)}$ and by the last theorem we know they form a generating set too. So we have $\mathbf{F}[V]^{\mathrm{GL}(V)} = \mathbf{F}[d_{1,n}, \ldots, d_{n,n}]$ and for any $G \subset \mathrm{GL}(V)$, $\{d_{1,n}, \ldots, d_{n,n}\}$ forms an hsop for $\mathbf{F}[V]^G$.

A special subgroup of $\mathrm{GL}(V)$ is the group of upper-triangular matrices $\mathrm{UT}(V)$ with 1's along the diagonals. We call this the group of **unitriangular matrices**. This group is known to have polynomial ring of invariants [15]. Using ideas similar to the previous example we can construct a special generating set for $\mathbf{F}[V]^{\mathrm{UT}(V)}$ too. We follow [8] for that.

Example 1.4.2.5. *Let again $\mathbf{F}_q$ denote a finite field of order $q = p^s$ and V an n-dimensional $\mathbf{F}_q$-vector space. Choose a basis $V^* = \mathrm{Span}_{\mathbf{F}_q}\{x_1, \ldots, x_n\}$. Note that by the definition of the action of $\mathrm{UT}(V)$ on each x_i, the orbit polynomials defined by the formula*

$$h_i = \prod_{u \in V_{i-1}}(x_i + u), \forall i = \{1, \ldots, n\},$$

are homogeneous of degree q^{i-1}. In particular, it is true that $h_i = F_{i-1}(x_i)$ (the latter is defined in the previous example) and $\{h_1, \ldots, h_n\}$ is an hsop of $\mathbf{F}_q[V]^{\mathrm{UT}(V)}$ with $\prod_{i=1}^{n} h_i = |\mathrm{UT}(V)|$. Therefore, $\mathbf{F}_q[V]^{\mathrm{UT}(V)} = \mathbf{F}_q[h_1, \ldots, h_n]$.

So far we have been dealing with arbitrary finite groups. Assume that $P \leq \mathrm{GL}(V)$ is a p-group. Then it is a well-known fact that the invariant field of P is purely transcendental (see, [14]). Since $\mathbf{F}[V]^P$ is integral domain we can find a transcendence basis for its field of fractions, i.e., algebraically independent invariants $f_1, \ldots, f_n \in \mathbf{F}(V)^P$, such that $\mathbf{F}(V)^P = \mathbf{F}(f_1, \ldots, f_n)$, where $\dim(R) = \mathrm{tr.deg}_{\mathbf{F}}(\mathbf{F}(V)^P)$(= cardinality of a transcendence basis of $\mathbf{F}(V)^P$). It is always useful and sometimes simpler to construct a transcendence basis for $\mathbf{F}(V)^P$, rather than a generating set for $\mathbf{F}[V]^G$. The following theorem consists a constructive approach of this observation and it is a result that will be used repeatedly. For further reading we suggest to see [6].

Theorem 1.4.2.6. *Let $P \leq \mathrm{UT}(V)$ be an upper-triangular p-group representation. Choose homogeneous invariants $\phi_1, \ldots, \phi_n \in \mathbf{F}[V]^P$ such that for each $i = 1, \ldots, n$, $\phi_i \in \mathbf{F}[x_1, \ldots, x_i]^P$ has minimal positive x_i-degree. Then we have $\mathbf{F}(V)^P = \mathbf{F}(\phi_1, \ldots, \phi_n)$. Furtermore, if $\mathrm{LC}_{x_i}(\phi_i)$ denotes the leading coefficient of ϕ_i as polynomial in $\mathbf{F}[x_1, \ldots, x_{i-1}][x_i]$, we have*

$$\mathbf{F}[x_1, \ldots, x_{i-1}]^P[\phi_i, \mathrm{LC}_{x_i}(\phi_i)^{-1}] = \mathbf{F}[x_1, \ldots, x_i]^P[\mathrm{LC}_{x_i}(\phi_i)^{-1}].$$

The above theorem will be used as follows; typically, we shall be able to construct for each variable x_i the corresponding minimum degree invariant ϕ_i and we will know beforehand $\mathbf{F}[x_1, \ldots, x_{n-1}]^P$. Then $\mathrm{LC}_{x_n}(\phi_n) = x_1^{\alpha}$, would imply from the above theorem that $\mathbf{F}[V]^P[x_1^{-1}] = \mathbf{F}[x_1, \ldots, x_{n-1}]^P[\phi_n, x_1^{-1}]$, therefore we will have an equality of localized rings $\mathbf{F}[V]^P[x_1^{-1}] = \mathbf{F}[x_1, \ldots, x_{n-1}]^P[x_1^{-1}]$. Most of the times computing ϕ_i's though is a tough ad hoc procedure which involves numerous complex computations.

1.4.3 SAGBI basis and SAGBI/divide-by-x algorithm.

In this section we introduce one of our main tools, SAGBI bases, and present the SAGBI/divide-by-x algorithm. This algorithm terminates with a SAGBI basis when the $\mathbf{F}$-algebra is finitely generated, hence when applied on $\mathbf{F}[V]^H$ allows us to construct an explicit generating set.

We remind you that given an ideal $I \lhd R$, a **Gröbner basis** $G := \{f_1, \dots, f_n\} \subset I$ is a special generating set of I, such that for any $h \in I$ the lead monomial of h is divisibe by $\mathrm{LM}(f_i)$ for some $i = 1, \dots, n$.

The word SAGBI stands as an acronym of **S**ubalgebra **A**nalogue of **G**robner **B**asis for **I**deals, hence from the name only it is obvious that forms a special generating set. The difference is that in theory of SAGBI basis we deal with $\mathbf{F}$-subalgebras instead of ideals. For what follows let $\mathbf{F}[x_1, \dots, x_n]$ denote a polynomial algebra, $\mathscr{F} \subset \mathbf{F}[x_1, \dots, x_n]$ an arbitrary subset and R an $\mathbf{F}$-subalgebra of $\mathbf{F}[x_1, \dots, x_n]$.

Definition 1.4.3.1. *The **lead term algebra** of R is the $\mathbf{F}$-vector space spanned by the set $\langle \mathrm{LT}(f) \mid f \in R \rangle$, with respect to a fixed term order $\prec$. In other words the lead term algebra is*

$$\mathrm{LT}_{\prec}(R) = \langle\, \mathrm{LT}(f) \mid f \in R\, \rangle_{\mathbf{F}}.$$

Since R is an $\mathbf{F}$-subalgebra, $\mathrm{LT}_{\prec}(R)$ is an $\mathbf{F}$-algebra too. The reason we are interested in the lead term algebra is that contains useful information for the subalgebra itself. For example, the Hilbert series of R and $\mathrm{LT}_{\prec}(R)$ coincide.

Lemma 1.4.3.2. *[8, Lemma 5.1.1] $\mathcal{H}(R, t) = \mathcal{H}(\mathrm{LT}_{\prec}(R), t)$.*

Definition 1.4.3.3. *A subset $\mathscr{F} \subset \mathbf{F}[x_1, \dots, x_n]$ is called SAGBI basis of R, if the set $\mathrm{LT}_{\prec}(\mathscr{F}) = \{\mathrm{LT}(f) \mid f \in \mathscr{F}\}$ forms a generating set of $\mathrm{LT}_{\prec}(R)$ as an $\mathbf{F}$-subalgebra. In other words, if we have*

$$\mathrm{LT}_{\prec}(R) = \mathbf{F}[\mathrm{LT}_{\prec}(\mathscr{F})]\,.$$

Although the idea of SAGBI basis is similar to that of Gröbner basis, they have some important differences. While a Gröbner basis always exists and is finite (under mild assumptions on the underlying ring), the same is not true for a SAGBI basis. Indeed, if our subalgebra R is not finitely generated a SAGBI basis is never finite. Surprisingly though, the latter is not true in the finitely generated case either.

Example 1.4.3.4. *Assume that we have the subalgebra of* $\mathbf{F}[x,y]$*, generated by the set* $\{x+y, xy, xy^2\}$*. Then* $\mathbf{F}[x+y, xy, xy^2]$ *has no finite SAGBI basis with respect any term order. Indeed, we can create from the leading terms of elements of this subalgebra the set* $\{xy, xy^2, \ldots, xy^n, \ldots\}$*. Therefore the lead term algebra should contain all this set inside its generating set since no term can be written in terms of others in* $\mathrm{LT}_{\prec}(\mathbf{F}[x+y, xy, xy^2])$*. Thus in that case the SAGBI basis is* never *finite.*

Example 1.4.3.5. *[24, Chapter 11, Example 1.12]. Another not so obvious example of algebra where the SAGBI basis is not finite with respect some term order is given by the ring of invariants for the three-dimensional permutation representation of the alternating group in three letters* $A_3 = \langle id_{\Sigma_3}, f, f^2\rangle$*,* $R = \mathbf{F}[x,y,z]^{A_3}$*. This is the algebra consisting of invariant polynomials, remaining stable after the action of*

$$\begin{aligned} \varphi : A_3 &\longrightarrow \mathrm{GL}_3(\mathbf{F}) \\ f &\longmapsto \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} . \end{aligned}$$

It is well-known that the ring of invariants induced by the above representation is the following algebra in four generators,

$$R = \mathbf{F}[x+y+z, xy+yz+xz, xyz, (x-y)(x-z)(y-z)],$$

and if we let $\succ$ *be the lexicographic term order with* $x \succ y \succ z$*, then* R *has an infinite SAGBI basis. Assume that* $\mathrm{LT}(R)$ *is finitely generated algebra and let* $\{x^{a_1}z^{b_1}, \ldots, x^{a_s}z^{b_s}\}$ *be a subset of generators which do not contain* y*. Notice this subset is not empty since for* $f \in R$ *and* $\mathrm{LT}(f) = x^{i_1}y^{i_2}z^{i_3}$ *we must have* $i_1 \geq i_2 \geq i_3$ *or* $i_1 > i_3 \geq i_2$*. Think of the planar convex cone spanned by the vectors* $\{(a_1,b_1), \ldots, (a_s,b_s)\}$ *and choose* $\gamma > 1$ *such that* $\forall i = 1, \ldots, s$*,* $a_i \geq C \cdot b_i$*. Then every vector contained in the cone must fulfill this inequality too. Set* $h := x^{d+1}z^d + x^dy^{d+1} + y^dz^{d+1}$*, for some integer* $d > 1/(1-\gamma)$ *such that* $d+1 < \gamma \cdot d$*.*

Observe that $h \in R$ and that due to the lead term $(d+1, d)$ must lie in the cone spanned by the above vectors. However, we derive a contradiction since d has been chosen such that $d+1 < \gamma \cdot d$. Thus R has a SAGBI basis with infinite generating set.

Example 1.4.3.6. *On the other hand, a classical example of ring with a well-behaved SAGBI basis is the invariant ring of the permutation representation of Σ_n. This invariant ring is the algebra generated by the elementary symmetric polynomials, that is $\mathbf{F}[x_1, \ldots, x_n]^{\Sigma_n} = \mathbf{F}[x_1 + \cdots + x_n, x_1x_2 + \cdots + x_{n-1}x_n, \ldots, x_1x_2 \ldots x_n]$. It can be proven that with respect any term order the set of elementary symmetric polynomials forms a SAGBI basis for $\mathbf{F}[x_1, \ldots, x_n]^{\Sigma_n}$.*

By the above example we understand that SAGBI bases are more complicated than Gröbner bases. Many questions around criteria which determine if a SAGBI basis exists or not are still open. However, the following proposition gives necessary and sufficient conditions for a subset to be a SAGBI basis.

Proposition 1.4.3.7. *Let R be a subalgebra of $\mathbf{F}[x_1, \ldots, x_n]$. The following statements are equivalent:*

(1) $\mathrm{LT}_{\prec}(R)$ *is Noetherian.*

(2) $\mathrm{LT}_{\prec}(R)$ *is finitely generated algebra over* $\mathbf{F}$.

(3) The multiplicative monoid of lead terms of R is finitely generated.

(4) R has a finite SAGBI bases.

(5) Every SAGBI basis of R has a finite subset which is also a SAGBI basis for R.

Before we proceed to the next definition we establish some more notation; for an arbitrary finite set $\mathscr{F} = \{f_1, \ldots, f_l\} \subset \mathbf{F}[x_1, \ldots, x_n]$ we denote by f^I the product $\prod_{j=1}^{l} f^{i_j}$, where by $I = (i_1, i_2, \ldots, i_l)$ we mean a sequence of non-negative integers.

The reduction of an S-polynomial is of fundamental importance in the theory of Gröbner bases. The analogous calculation in the theory of SAGBI bases is the subduction of a tête-à-tête .

Definition 1.4.3.8. *Given a finite set* $\mathcal{F} = \{f_1, f_2, \ldots, f_l\} \subset \mathbf{F}[x_1, \ldots, x_n]$*, denote* $f^I = f_1^{i_1} \ldots f_n^{i_n}$ *for* $I = (i_1, \ldots, i_n)$ *a sequence of non-negative integers. A pair* (f^I, f^J) *is called* ***tête-à-tête*** *if* $\mathrm{LM}(f^I) = \mathrm{LM}(f^J)$*, for various sequences* I, J*. We call a tête-à-tête* ***non-trivial*** *if the sequences* I, J *have disjoint support, i.e., if* f^I *and* f^J *share no common factors in* $\mathcal{F}$*.*

Now we have all that we need to give the subduction algorithm.

Algorithm 1 The subduction algorithm for a SAGBI bases

Input: A SAGBI bases $\mathscr{F}$ for a subalgebra $R \subset \mathbf{F}[x_1, \ldots, x_n]$. A polynomial $f \in \mathbf{F}[x_1, \ldots, x_n]$.

Output: An expression of f as a polynomial in the elements of $\mathscr{F}$, provided $f \in R$ and non-constant. While f is not a constant in $\mathbf{F}$ do

(1) Find $f_1, f_2, \ldots, f_n \in R$, exponents $i_1, i_2, \ldots, i_n \in \mathbb{N}$ and $c \in \mathbf{F}^*$ such that

$$\mathrm{LT}_{\prec}(f) = c \ \ \mathrm{LT}_{\prec}(f_1)^{i_1}\mathrm{LT}_{\prec}(f_2)^{i_2} \ldots \mathrm{LT}_{\prec}(f_n)^{i_n}. \quad (*)$$

(2) If no representation (*) exists, then output "f does not lie in R" and STOP.

(3) Otherwise, output $p = c \cdot {f_1}^{i_1} {f_2}^{i_2} \ldots {f_n}^{i_n}$, and replace f by $f - p$.

Output the constant f.

Given a subset $\mathscr{F} \subset \mathbf{F}[x_1, x_2, \ldots, x_n]$, by adjoining every time the subducted non-trivial tête-à-têtes on $\mathscr{F}$ creates a nested sequence of generating sets $\mathscr{F} = \mathscr{F}_0 \subset \mathscr{F}_1 \subset \mathscr{F}_2 \subset \ldots$ for the subalgebra $\mathbf{F}[\mathscr{F}]$. In fact the subduction algorithm works when the subset $\mathscr{F}$ is infinite, though the resulting generating set $\mathscr{F}_\infty = \bigcup_{j \in J} \mathscr{F}_j$ is not finite, hence not really convenient to work out with. For $\mathcal{B} \subset R$ any subset and $f \in R$ arbitrary, we denote by $\textsc{subd}(f, \mathcal{B})$ the subduction of f against this set $\mathcal{B}$.

We fix as term order the graded reverse lexicographic order with $y_n \succ y_{n-1} \succ \cdots \succ x$, for a polynomial algebra $\mathbf{F}[x, y_1, \ldots, y_n]$. Throughout this thesis we make extensive use of a different algorithm known as **SAGBI/divide-by-x algorithm**. This algorithm is an extension of the previous in the following sense: if a non-zero subduction f has lead monomial $x^m y^I$, where $y^I = {y_1}^{i_1}{y_2}^{i_2} \ldots {y_n}^{i_n}$ for a sequence of non-negative integers $I = (i_1, i_2, \ldots, i_n)$, then fx^{-m} is adjoined rather than f. This procedure in contrast with the previous creates a sequence of generating sets $\mathscr{F} = \mathscr{F}_0 \subset \mathscr{F}_1 \subset \mathscr{F}_2 \subset \ldots$ again, but this time in addition we have a sequence of $\mathbf{F}$-algebras $R = R_0 \subset R_1 \subset R_2 \subset \ldots$, each one generated by the corresponding $\mathscr{F}_i$.

The SAGBI/divide-by-x algorithm, in principle, can be used to compute the ring of invariants for any modular representation of a p-group.

Theorem 1.4.3.9. *[8, Theorem 5.2.3] If the action of $G \leq \mathrm{GL}(V)$ on $\mathbf{F}[V]$ is triangular, then $\mathbf{F}[V]^G$ has a finite SAGBI basis.*

Theorem 1.4.3.10. *[7, Theorem 2.1] Assume V is an $\mathbf{F}[P]$-module of dimension n and $\mathcal{B} := \{x, f_1, \ldots, f_k\}$ a SAGBI basis of $A \subset \mathbf{F}[V]^P$, where P denotes some p-group. Furthermore, suppose $A[x^{-1}] = \mathbf{F}[V]^P[x^{-1}]$ and that $\mathbf{F}[V]^P$ is an integral extension of A. Then $A = \mathbf{F}[V]^P$ and $\mathcal{B}$ is a SAGBI basis for $\mathbf{F}[V]^P$.*

Proof. The proof of the theorem is a consequence of [13, Theorem 20.2]. Modular invariant rings of finite p-groups are known to be UFD [8, Theorem 3.8.1]. Therefore $A[x^{-1}] = \mathbf{F}[V]^P[x^{-1}]$ is a UFD too. To prove the equality $A = \mathbf{F}[V]^P$ suffices to show that A is integrally closed in its field of fraction, i.e., a normal domain. From [13, Theorem 20.2] suffices to prove that xA is prime; assume $f, g \in A$ such that $fg \in xA$. Then $xA \subset x\mathbf{F}[V]$ and the last is prime. So we can assume $f \in x\mathbf{F}[V]$ without loss of generality. Due to the term order we use (grevlex with x small), every term of f is divisible by x and $\textsc{subd}(f, \mathcal{B}) = 0$ since $\mathcal{B}$ is SAGBI basis of A. This implies $f \in xA$ and xA is a prime, since at every step of the subduction there is a factor of x. □

Theorem 1.4.3.11. *[7, Theorem 2.2] Suppose that $\mathcal{B}$ is a generating set for $A \subset \mathbf{F}[V]^P$ such that $x \in \mathcal{B}$ and there exist homogeneous $h_1, \ldots, h_{n-1} \in \mathcal{B}$ with $\mathrm{LT}(h_i) = y_i^{a_i}$. If $A[x^{-1}] = \mathbf{F}[V]^P[x^{-1}]$, then the SAGBI/divide-by-x algorithm applied to $\mathcal{B}$ terminates with a SAGBI basis for $\mathbf{F}[V]^P$.*

Proof. $\mathbf{F}[V]$ is a finite module over the lead term algebra of $\mathbf{F}[x, h_1, \ldots, h_{n-1}]$, say L. So it is a Noetherian L-module. Thus the ascending sequence of algebras $A_0 \subset A_1 \subset A_2 \subset \ldots$ generated by the lead terms of elements of $\mathcal{B}_i$ in $\mathbf{F}[V]$ terminates. Assume that it terminates at A_j and let $\mathcal{B}_j$ denote the corresponding SAGBI basis. By assumption the set $\{x, h_1, \ldots, h_{n-1}\}$ forms an hsop for $\mathbf{F}[V]^P$ (follows from Lemma 1.12) and $A_j[x^{-1}] = \mathbf{F}[V]^P[x^{-1}]$. Follows from the previous theorem now $\mathcal{B}_j$ is a SAGBI basis for $\mathbf{F}[V]^G$ too. □

Finally, assume $\mathcal{F} := \{f_1, \ldots, f_n\} \subset \mathbf{F}[\mathbf{t}] = \mathbf{F}[t_1, \ldots, t_n]$ forms a SAGBI basis for the subalgebra $R := \mathbf{F}[\mathcal{F}]$ with respect some term order $\prec$. Let $\mathcal{A} = \{a_1, \ldots, a_n\} \subset \mathbf{N}^n$, denote the set of vectors such that $\mathrm{LT}_\prec(f_i) = \mathbf{t}^{a_i}$. Consider the $\mathbf{F}$-algebra epimorphism $t_i \mapsto f_i$ from $\mathbf{F}[\mathbf{t}]$ onto R with kernel I. Similarly, consider the map from $\mathbf{F}[\mathbf{t}]$ onto the lead term algebra $\mathrm{LT}_\prec(R)$, $t_i \mapsto \mathrm{LT}_\prec(f_i)$. The kernel of this map is the toric ideal $I_\mathcal{A}$.

From the definition of SAGBI basis, there is no guarantee that $\mathbf{F}[\mathcal{F}]$ is minimally generated by $\mathcal{F}$. The reason is that the subduction algorithm does not understand whether a tête-à-tête subduction attached on $\mathscr{F}$ can be written in terms of the other elements when the algorithm has terminated (with a SAGBI basis). Although this is a downside of the algorithm from algebraic point of view, can be proven that the subduction of the non-trivial tête-à-têtes minimally generate the ideal of algebraic relations of R.

Lemma 1.4.3.12. *Using the above notation, the non-trivial tête-à-tête subductions of $\mathcal{F}$ minimally generate the ideal of algebraic relations of R.*

Proof. Pick an element $p(\mathbf{t}) = \sum_{u \in \mathcal{U}} c_u t_1^u \ldots t_n^u \in I$; then $p(f_1, \ldots, f_n) = 0$. When expanding this sum the terms of highest $\prec$-order must cancel out. If $u_1, u_2 \in \mathcal{U}$

such that $\mathrm{LT}(c_{u_1} f_1^{u_1^1} \dots f_n^{u_1^n}) = \mathrm{LT}(c_{u_2} f_1^{u_2^1} \dots f_n^{u_2^n})$ for distinct terms in $p(f_1, \dots, f_n)$, then (f^{u_1}, f^{u_2}) forms a non-trivial tête-à-tête of $\mathcal{F}$. Thus, must exist an element in I which lifts this tête-à-tête subduction. Carry on this procedure for $p(f_1, \dots, f_n)$, implies that any time the highest $\prec$-order is pruned, the corresponding term in $p(\mathbf{t})$ can be written in terms of the corresponding lifting of the subduction of some non-trivial tête-à-tête of $\mathcal{F}$. This yields an expression of $p(\mathbf{t})$ in terms of basis element projecting to tête-à-tête subductions. Hence any member of I can be written in this form and our claim follows. □

1.4.4 Nakajima groups

In this subsection we assume that $P \leq \mathrm{GL}_n(\mathbf{F})$ denotes a p-group and $\mathbf{F}$ a field of positive characteristic $\mathrm{char}(\mathbf{F}) = p$. It is a well-known fact that the fixed-point space V^P is non-zero if $V \neq 0$. Modding out by this subspace V/V^P, we see that $(V/V^P)^P$ is not trivial again. Thus we can construct in this fashion a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V and $\mathcal{B}^* = \{x_1, \dots, x_n\}$ of V^*, such that the representing matrices are in a unitriangular form.

Let $\mathbf{N}(x) := \mathbf{N}_{P_x}^P(x)$ denote the norm of some $x \in V^*$. We recall that by norm, we always mean the product over the stabilizer $P_x = \{\, g \in G \mid x \cdot g = x \,\}$, i.e., $\mathbf{N}(x) = \prod_{y \in xP} y$. Set $P_i := \cap_{j \neq i} P_{x_j}$. Then $P_i \leq P$, and in particular has a very special form. It is an one row-subgroup generated by the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 & \dots & 0 \\ & & & & \vdots & & & & \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & * & * & \dots & * \\ & & & & \vdots & & & & \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \end{bmatrix}$$

Definition 1.4.4.1. *The group P is called **Nakajima** with respect to B if $P = P_n P_{n-1} \dots P_1$.*

When P is known to be Nakajima the ring of invariants $\mathbf{F}[V]^P$ has a very nice description.

Theorem 1.4.4.2. *P is Nakajima with respect to some basis $\mathcal{B}$ if and only if*

$$\mathbf{F}[V]^P = \mathbf{F}[\mathbf{N}_P(x_1), \ldots, \mathbf{N}_P(x_n)].$$

Proof. For a proof, see [8, Theorem 8.0.7]. □

1.5 Extra-special groups

1.5.1 Extra-special groups of order p^3.

In this last section we explore the structure of the group for which the corresponding invariant theory we will attempt to understand.

Extra-special groups form an interesting class of p-groups whose character theory and classification is well-understood. Before we proceed to the definition we introduce a little terminology from group theory.

Definition 1.5.1.1. *Assume that G is a finite group. A series of subgroups*

$$1 = A_0 \triangleleft\ A_1 \triangleleft\ \ldots\ \triangleleft\ A_n = G,\ (*)$$

*is called **normal** if $\forall i = 1, \ldots, n$, A_i is a normal subgroup of A_{i+1}. Furthermore, if each A_i is a maximal strict normal subgroup of A_{i+1} we call $(*)$ **composition series**. Equivalently, a composition series is a normal series such that each factor A_{i+1}/A_i is simple.*

*We call a finite group **nilpotent**, if there is a normal series which is also central, i.e., $A_{i+1}/A_i \triangleleft Z(G/A_i), \forall i$. Finally, if the successive quotients A_{i+1}/A_i are abelian then the group is called **solvable**, while if they are cyclic **supersolvable**.*

Clearly every supersolvable group is solvable and every solvable group is nilpotent. Also it can be proven that any finite group has a composition series. In particular, in case of finite p-groups we have something more, they are supersolvable.

Definition 1.5.1.2. *Suppose G is a finite group. The* ***exponent*** *of G is defined as the least commmon multiple of the orders of all elements of the group.*

A p-group G is called ***extra-special*** *if its center $Z(G)$ is cyclic of order p and the quotient $G/Z(G)$ an elementary abelian group.*

We recall the following construction from group theory which can be found in [19].

Definition 1.5.1.3. *A group G is said to be the (internal)* ***central product*** *of its normal subgroups $G_1, \dots, G_n \lhd G$, if $G = G_1 \dots G_n$, $[G_i, G_j] = 1$ for $i \neq j$, and $G_i \cap \prod_{i \neq j} G_j = Z(G)$ for all i.*

Follows from this definition that since $Z(G_i) \leq Z(G)$ we have $Z(G_i) = Z(G)$.

Every extra-special group has order p^{1+2n} for some positive integer n. Conversely for each such number there are two extra-special groups up to isomorphism. Of major importance are the two extra-special groups when $n = 1$. Define

$$\begin{aligned} G &:= \langle g_1, g_2 \mid g_1^p = g_2^p = [g_1, g_2], [g_1, [g_1, g_2]] = e, [g_2, [g_1, g_2]] = e, [g_1, g_2]^p = e \rangle, \\ H &:= \langle g_1, g_2 \mid g_1^p = g_2^p = e, [g_1, [g_1, g_2]] = e, [g_2, [g_1, g_2]] = e, [g_1, g_2]^p = e \rangle. \end{aligned}$$

These are the only (up to isomorphism) extra-special groups of order p^3. The first has exponent p^2 whereas the second p. The importance of these two groups is depicted in the following theorem.

Theorem 1.5.1.4. *An extra-special p-group P is a central product of n nonabelian subgroups of order p^3 and has order p^{2n+1}. Conversely a finite central product of nonabelian groups of order p^3 is an extra-special p-group.*

In particular, we have the following cases:

(1) if $p := 2$, then P is a central product of D_8's or is a central product of D_8's and a single Q_8.

(2) if $p > 2$, then either P has exponent p, or otherwise it is a central product of nonabelian groups of order p^3 and exponent p and a single non-abelian group of order p^3 and exponent p^2.

The above theorem implies that for $p > 2$, any extra-special group is either the central product of n-copies of H, or the central product of $(n-1)$-copies of H with a copy of G.

1.5.2 Group Structure of H

To understand the group structure of H we look at the prototype example of extra-special groups, the unitriangular matrices over a finite field $\mathbf{F}_p$. This is the non-abelian group of matrices

$$\mathrm{UT}_3(\mathbf{F}_p) = \left\{ \begin{bmatrix} 1 & c_{1,2} & c_{1,3} \\ 0 & 1 & c_{2,3} \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; c_{i,j} \in \mathbf{F}_p \right\}.$$

For the rest of this section we denote $\mathrm{UT}_3(\mathbf{F}_p)$ by U.

A natural generating set for U is

$$x = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

with commutator element

$$[x, y] = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Every matrix

$$\begin{bmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{bmatrix} \in U,$$

can be written in the following form

$$\begin{bmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{bmatrix} = y^{\gamma}\, x^{\alpha}\, [x, y]^{\beta}.$$

Suppose that the following two matrices is a pair of non-commuting matrices of U

$$A = \begin{bmatrix} 1 & \alpha_{1,2} & \alpha_{1,3} \\ 0 & 1 & \alpha_{2,3} \\ 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & \beta_{1,2} & \beta_{1,3} \\ 0 & 1 & \beta_{2,3} \\ 0 & 0 & 1 \end{bmatrix}.$$

We can prove that $\{A, B\}$ forms a generating set. A straightforward computation reveals that A and B commute if and only if $a_{12}\beta_{23} = a_{23}\beta_{12}$. Also the commutator $[A, B] = ABA^{-1}B^{-1}$ lies always in the center; using the formula

$$\begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix}^{-1} = \begin{bmatrix} 1/a & -b/(ad) & (be-cd)/(afd) \\ 0 & 1/d & -e/(fd) \\ 0 & 0 & 1/f \end{bmatrix}$$

for inverses of upper-triangular matrices we see that $[A, B] \in Z(U)$. Since the center is cyclic, we have $Z(U) = \langle [A, B] \rangle$. Due to the isomorphism $U \cong H$, the presentation of the first implies that non-commuting pairs in H form a generating set with their commutator generating the center $Z(H)$.

1.5.3 Structure of $\mathrm{Aut}(H)$.

We want to exploit the isomorphism $U \cong H$ to understand $\mathrm{Aut}(H)$. Fix a non-commuting pair $A, B \in U$ and $f \in \mathrm{End}(U)$ such that

$$f : U \to U, \qquad x \mapsto A,\, y \mapsto B\,.$$

Since our group is finite and every epimorphism in $\mathrm{End}(U)$ is an automorphism, by definition f is an automorphism. Notice that there is an one-to-one correspondence between non-commuting pairs in U and automorphisms.

Because U is a non-abelian group of order p^3 we know that all the maximal subgroups are abelian. In particular, these subgroups are obtained by joining a non-central subgroup of prime order in U and the center. So every maximal abelian subgroup of U is isomorphic to the 2-elementary abelian p-group, $\mathbb{Z}_p \times \mathbb{Z}_p$. Furthermore since every automorphism $\tau \in \mathrm{Aut}(U)$ keeps the center itself stable, that is $\tau(Z(U)) = Z(U)$, by fixing a maximal subgroup and an element of U which does not commute with the non-central generator of the elementary abelian subgroup, then we get a generating set for U. To actually see this assertions, think of the isomorphism from U to the semidirect product $(\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$,

$$U \to (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p,\ x \mapsto ((1,0),0),\ y \mapsto ((0,0),1).$$

Since any maximal subgroup of $(\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, the assertion for U follows too. Regarding the automorphism group $\mathrm{Aut}(U)$ we think the corresponding $\mathrm{Aut}((\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p)$. A simple counting gives $(p^3 - p)$ elements which are not in the center and every such an element is commuting only with the elements of the maximal abelian subgroup generated by the join of the cyclic group it generates and the center. Therefore for such an element we have $p^3 - p^2$ distinct choices of non-commuting elements. Together the above observations imply that these are the only choices of automorphisms. Therefore, $|\mathrm{Aut}(U)| = (p^3 - p^2)\,(p^3 - p)$.

Chapter 2

Classification of modular representations

2.1 Introduction

In this chapter we classify modular representations of H. Before we proceed to the main part we first introduce some of the tools that we will need.

Assume $\mathbf{F}$ is a field of characteristic $p > 0$, G is a p-group and V an n-dimensional $\mathbf{F}G$-module. We define the socle of V to be the sum of all simple submodules and we denote it by $\mathrm{soc}(V)$. It is well known result that the fixed-point space V^G is non-trivial (see, [8, Lemma 4.0.1]) and the only simple submodule is the trivial one-dimensional module (see, [2, Theorem 1.3.2]). Therefore, follows that $\mathrm{soc}(V) = V^G$.

Define $\mathrm{soc}_1(V) := V^G$ and for $i > 1$, $\mathrm{soc}_i(V)$ so that

$$\mathrm{soc}_i(V)/\mathrm{soc}_{i-1}(V) = \mathrm{soc}(V/\mathrm{soc}_{i-1}(V)).$$

Then we obtain an ascending sequence of submodules

$$0 \subset \mathrm{soc}_1(V) \subset \mathrm{soc}_2(V) \subset \ldots \subset \mathrm{soc}_k(V) = V.$$

We call this sequence the socle series and k the socle-length of V correspondingly.

Definition 2.1.0.1. *Define the positive integers*

$$m_1 = \dim_{\mathbf{F}}(\mathrm{soc}_1(V)), m_i = \dim_{\mathbf{F}}(\mathrm{soc}_i(V)/\mathrm{soc}_{i-1}(V)),\ \forall i = 2, \ldots, k.$$

Then we say that V *has socle-type* $(m_1, \ldots, m_k)$*, or simply that is of type-*$(m_1, \ldots, m_k)$.

Since H is a p-group, we can apply the above definitions to finite-dimensional $\mathbf{F}H$-modules. If V denotes such a module, we always fix a basis $\mathscr{B}$ consistent with the socle series, i.e., we extend the basis of $V^G = \mathrm{Span}_{\mathbf{F}}\{u_1, \ldots, u_{m_1}\}$, to a basis of $\mathrm{soc}_2(V) = \mathrm{Span}_{\mathbf{F}}\{u_1, \ldots, u_{m_1}, u_{m_1+1}, \ldots, u_{m_1+m_2}\}$ and iteratively we set

$$\mathrm{soc}_i(V) = \mathrm{Span}_{\mathbf{F}}\{u_1, \ldots, u_{m_1}, \ldots, u_{m_1+\ldots+m_i}\},$$

for all $i \in \{1, \ldots, k\}$. Thus if $\rho_{\mathscr{B}} : H \to \mathrm{GL}_n(\mathbf{F})$ denotes the corresponding linear representation of V, with respect to that basis the representing matrices are upper-triangular unipotent, i.e., $\rho_{\mathscr{B}}(H) \subset \mathrm{UT}_n(\mathbf{F})$. Furthermore, if another choice of basis consistent with the socle series has been made, then the two bases differ by a change of coordinates which stabilises the solce series of V.

2.2 Type-$(1, 1, ..., 1)$ Representations

In this section we investigate n-dimensional faithful $\mathbf{F}H$-modules of type-$(1, 1, ..., 1)$. We prove the existence of a suitable generating set for the group of representing matrices and explicitly describe these representations when $n = 3, 4$.

Below by J_n we denote the maximal Jordan normal form.

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

Theorem 2.2.0.1. *Suppose V is an n-dimensional faithful $\mathbf{F}H$-module of type-$(1,1,...,1)$ with $n \leq p$. Then there is an ordered basis $\mathscr{B}$ for V such that $\rho_{\mathscr{B}}(H) = \langle J_n, B\rangle \leq \mathrm{UT}_n(\mathbf{F})$.*

Proof. We fix a basis $\mathscr{B}'$ of V so that all the representing matrices of $\rho_{\mathscr{B}'} : H \to \mathrm{GL}_n(\mathbf{F})$ are in an upper-triangular form. First we prove that there is a matrix $A \in \rho_{\mathscr{B}'}(H)$ equivalent to J_n. To this end it is enough to show that there is a matrix $L = (l_{i,j}) \in \rho_{\mathscr{B}'}(H)$ with all the superdiagonal entries non-zero, i.e., $l_{i,i+1} \neq 0$, $i = 1, ..., n-1$. Assume that $\rho_{\mathscr{B}'}(H) = \langle M, N\rangle$. If either M or N has all superdiagonal entries non-zero then we are done. Thus we assume that at least one is zero. Observe that M, N can't have same superdiagonal entries zero at the same time. Otherwise, if $i \in \{1, ..., n-1\}$ such that $m_{i,i+1} = n_{i,i+1} = 0$ exists, then the action of H on the quotient $V/\mathrm{soc}_{i-1}(V)$ would define a fixed point subspace with dimension at least two. Therefore, the equality $\mathrm{soc}(V/\mathrm{soc}_{i-1}(V)) = (V/\mathrm{soc}_{i-1}(V))^H$, would imply $m_i = \dim_{\mathbf{F}}(\mathrm{soc}(V/\mathrm{soc}_{i-1}(V))) \geq 2$, contradicting our assumption that the representation is of type-$(1,1,...,1)$.

The superdiagonal of the matrices MN^k, $k < p$, has $n-2$ expressions of the form $m_{i,i+1} + kn_{i,i+1}$. Each of these expressions can be eliminated by at most one k. Since by assumption $n-2 < p-1$, we can choose $k < p$ so that all of these expressions are non-zero. Hence for the right choice of k, the matrix MN^k is equivalent to the maximal n-dimensional Jordan block.

For suitable choice of $k < p$ assume that $\rho_{\mathscr{B}'}(H) = \langle A, B'\rangle$ with $\{A, B'\} = \{MN^k, N\}$ and $A \sim J_n$. If $\mathscr{B}' = \{v_1, ..., v_n\}$, set $\mathscr{B} = \{(A - I_n)^{n-1}v_n, (A - I_n)^{n-2}v_n, ..., (A - I_n)v_n, v_n\}$. Then $\mathscr{B}$ is the seeking choice of basis, since it forms an ordered basis of V such that $\rho_{\mathscr{B}}(H) = \langle J_n, B\rangle \leq \mathrm{UT}_n(\mathbf{F})$. Now our claim follows. □

From now on we fix a basis $\mathscr{B}$ as described in the previous theorem. Denote by $C(M) = \{N \in \mathrm{GL}_n(\mathbf{F}) \mid NM = MN\}$ the centralizer of an invertible matrix $M \in \mathrm{GL}_n(\mathbf{F})$. The presentation of $\rho_{\mathscr{B}}(H)$ imposes the relations $[J_n, B]J_n = J_n[J_n, B], [J_n, B]B = B[J_n, B]$, where $[J_n, B] = J_nBJ_n^{-1}B^{-1}$ denotes the commutator element. Thus, $[J_n, B] \in C(J_n) \cap C(B)$. The next lemma gives a description of the elements in $C(J_n)$.

Lemma 2.2.0.2. *A centralizing matrix $T \in C(J_n)$ has the following form*

$$T = \begin{bmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,n-1} & t_{1,n} \\ 0 & t_{1,1} & \cdots & t_{1,n-2} & t_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & t_{1,1} & t_{1,2} \\ 0 & 0 & \cdots & 0 & t_{1,1} \end{bmatrix},$$

for various $t_{i,j} \in \mathbf{F}, t_{1,1} \in \mathbf{F}^*$.

Proof. Let $T \in \mathrm{GL}_n(\mathbf{F})$ denote an invertible matrix. Then the $(i,j)-$entry of the product TJ_n equals $(TJ_n)[i,j] = \sum_{k=1}^{n} t_{i,k} J_n[k,j]$. Thus, $(TJ_n)[i,1] = t_{i,1}$ while if $j > 1$ we have $(TJ_n)[i,j] = t_{i,j} + t_{i,j-1}$. Similarly, for $i < n$ we obtain $(J_nT)[i,j] = t_{i,j} + t_{i+1,j}$ and $(J_nT)[n,j] = t_{n,j}$. Now the equality $TJ_n = J_nT$ forces T to have the claimed form. □

In $\rho_{\mathscr{B}}(H)$ the derived subgroup coincides with the center. The inclusion $Z(\rho_{\mathscr{B}}(H)) \subset C(J_n) \cap C(B)$ implies $Z(\rho_{\mathscr{B}}(H)) = \langle T \rangle \cong C_p$ for the right choice of $T \in C(J_n) \cap C(B)$. Below we describe T for $n = 3, 4$.

Lemma 2.2.0.3. *For $n = 3, 4$, every matrix $T \in Z(\rho_{\mathscr{B}}(H))$ has the following form*

$$T = \begin{bmatrix} 1 & 0 & \cdots & 0 & t_{1,n} \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, \text{ for } t_{1,n} \in \mathbf{F}.$$

Proof. We present explicitly the equality $BT = TB$ for the cases $n = 3, 4$. Computations on MAGMA yield

$n = 3:$

$$\begin{bmatrix} t_{1,1} & t_{1,1}b_{1,2} + t_{1,2} & t_{1,1}b_{1,3} + t_{1,2}b_{1,2} + t_{1,3} \\ 0 & t_{1,1} & t_{1,1}b_{2,3} + t_{1,2} \\ 0 & 0 & t_{1,1} \end{bmatrix}$$
$$=$$
$$\begin{bmatrix} t_{1,1} & t_{1,1}b_{1,2} + t_{1,2} & t_{1,1}b_{1,3} + t_{1,2}b_{2,3} + t_{1,3} \\ 0 & t_{1,1} & t_{1,1}b_{2,3} + t_{1,2} \\ 0 & 0 & t_{1,1} \end{bmatrix}$$

$n = 4:$

$$\begin{bmatrix} t_{1,1} & t_{1,1}b_{1,2} + t_{1,2} & t_{1,1}b_{1,3} + t_{1,2}b_{1,2} + t_{1,3} & t_{1,1}b_{1,4} + t_{1,3}b_{1,2} + t_{1,2}b_{1,3} + t_{1,4} \\ 0 & t_{1,1} & t_{1,1}b_{2,3} + t_{1,2} & t_{1,1}b_{2,4} + t_{1,2}b_{2,3} + t_{1,3} \\ 0 & 0 & t_{1,1} & t_{1,1}b_{3,4} + t_{1,2} \\ 0 & 0 & 0 & t_{1,1} \end{bmatrix}$$
$$=$$
$$\begin{bmatrix} t_{1,1} & t_{1,1}b_{1,2} + t_{1,2} & t_{1,1}b_{1,3} + t_{1,2}b_{2,3} + t_{1,3} & t_{1,1}b_{1,4} + t_{1,3}b_{3,4} + t_{1,2}b_{2,4} + t_{1,4} \\ 0 & t_{1,1} & t_{1,1}b_{2,3} + t_{1,2} & t_{1,1}b_{2,4} + t_{1,2}b_{3,4} + t_{1,3} \\ 0 & 0 & t_{1,1} & t_{1,1}b_{3,4} + t_{1,2} \\ 0 & 0 & 0 & t_{1,1} \end{bmatrix}$$

The equality $T = [J_n, B]$ yields $t_{1,1} = 1$ in both cases. For $n = 3$, the commutator $C = [A, B]$ becomes

$$C = \begin{bmatrix} 1 & 0 & b_{2,3} - b_{1,2} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The condition $C \neq I_3$ implies $b_{2,3} - b_{1,2} \neq 0$, thus we obtain $t_{1,2} = 0$ and our claim follows. The case $n = 4$ yields the following three equations:

$$t_{1,2}(b_{1,2} - b_{2,3}) = 0,\ t_{1,2}(b_{2,3} - b_{3,4}) = 0,\ t_{1,2}(b_{1,3} - b_{2,4}) + t_{1,3}(b_{1,2} - b_{3,4}) = 0 \qquad (1)$$

and the commutator of $\rho_{\mathscr{B}}(H)$ equals

$$[J_4, B] = J_4 B J_4^{-1} B^{-1} = \begin{bmatrix} 1 & 0 & b_{2,3} - b_{1,2} & (1 + b_{3,4})(b_{1,2} - b_{2,3}) - b_{1,3} + b_{2,4} \\ 0 & 1 & 0 & b_{3,4} - b_{2,3} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Thus, the condition $T = [J_4, B]$ yields $t_{1,2} = 0$, as well as the equalities $t_{1,3} = b_{3,4} - b_{2,3}, t_{1,3} = b_{2,3} - b_{1,2}$. Adding the last two equations gives $2t_{1,3} = b_{3,4} - b_{1,2}$. Applying the last equality to the third condition of (1) gives $t_{1,3} = 0$. Therefore, for $n = 4$ our claim follows too. $\square$

Remark 2.2.0.4. *The above observation cannot generalize directly to higher dimensions. For $n = 5$, the relation $T = [J_5, B]$ yields again $t_{1,1} = 1, t_{1,2} = 0$, however the equality $BT = TB$ implies that the commutator can have the following form*

$$T = \begin{bmatrix} 1 & 0 & 0 & t_{1,4} & t_{1,5} \\ 0 & 1 & 0 & 0 & t_{1,4} \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

with $t_{1,4} \in \mathbf{F}$ not necessarily zero and $[T, J_5] = 0$.

The equality $T = J_4 B J_4^{-1} B^{-1}$ implies $J_4 B - T B J_4 = O_4$. After the matrix multiplication we obtain

$$\begin{bmatrix} 0 & 0 & b_{2,3} - b_{1,2} & b_{2,4} - b_{1,3} - d \\ 0 & 0 & 0 & b_{3,4} - b_{2,3} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = O_4 \implies \quad b_{1,2} = b_{2,3} = b_{3,4},\ b_{2,4} - b_{1,3} \neq 0.$$

The same computation for $n = 3$ gives $b_{2,3} - b_{1,2} \neq 0$.

For $n = 4$, we are able with a consistent change of basis that preserves J_4 to bring B in a more handy form. Since $b_{2,4} - b_{1,3} \neq 0$, set $b = b_{1,4}/(b_{2,4} - b_{1,3})$. If $\mathscr{B} = \{e_1, e_2, e_3, e_4\}$ denotes the basis of V from Theorem 2.2.0.1, then $\mathscr{B}_1 = \{e_1 + be_2, e_2 + be_3, e_3 + be_4, e_4\}$, forms a new basis such that the transition matrix

T' annihilates the $(1,4)$-entry of B:

$$T'^{-1}BT' = \begin{bmatrix} 1 & b_{1,2} & b_{1,3} & 0 \\ 0 & 1 & b_{1,2} & b_{2,4} \\ 0 & 0 & 1 & b_{1,2} \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

When $n = 3$, follows from a routine calculation that $C(J_3) = C(B)$. Hence any consistent with the socle series change of basis preserves both generators of $\rho_{\mathscr{B}}(H)$. So B cannot transform in that case.

Theorem 2.2.0.5. *Suppose* $\mathbf{F}$ *is a field of characteristic* $p \geq 5$ *and* V *a faithful four-dimensional* $\mathbf{F}H$*-module. Then there is a choice of basis* $\mathscr{B}$ *consistent with the socles series such that* $\rho_{\mathscr{B}}(H) = \langle J_4, B \rangle$ *with*

$$B = \begin{bmatrix} 1 & b_{1,2} & b_{1,3} & 0 \\ 0 & 1 & b_{1,2} & b_{2,4} \\ 0 & 0 & 1 & b_{1,2} \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Furthermore, these representations are parameterised by the set $\{(b_{1,2}, b_{1,3}, b_{2,4}) \in \mathbf{F}^3 \mid b_{1,3} \neq b_{2,4}\}$. *Similarly, for* $n = 3$ *we have* $\rho_{\mathscr{B}}(H) = \langle J_3, B' \rangle$ *with*

$$B' = \begin{bmatrix} 1 & b_{1,2} & 0 \\ 0 & 1 & b_{2,3} \\ 0 & 0 & 1 \end{bmatrix},$$

and type-$(1,1,1)$ *representations are parameterised by* $\{(b_{1,2}, b_{2,3}) \in \mathbf{F}^2 \mid b_{1,2} \neq b_{2,3}\}$.

Finally for arbitrary $n \geq 5$, from Theorem 2.2.0.1 we obtain the following proposition.

Proposition 2.2.0.6. *Suppose* $\mathbf{F}$ *is a field of characteristic* $p \geq 5$ *and* V *a faithful* n*-dimensional* $\mathbf{F}H-$*module of type-*$(1,1,...,1)$ *such that* $n \leq p$. *Then there is a choice of basis* $\mathscr{B}$ *consistent with the socle series such that* $\rho_{\mathscr{B}}(V) = \langle J_n, B \rangle$. *Hence, these representations are parameterised by points* $(b_{1,2}, ..., b_{n-1,n}) \in \mathbf{F}^{\frac{n(n-1)}{2}}$, *subject to the relations* $[J_n, [J_n, B]] = 0, [B, [J_n, B]] = 0$.

2.3 Type-$(2, 1, ..., 1)$ Representations

We start this section by describing the matrices with Jordan normal form $J_{1,n-1}$. Let $M \in \mathrm{GL}_n(\mathbf{F})$ denote an invertible matrix, $\lambda_M \in \mathbf{F}$ an eigenvalue and $d_k = \dim_{\mathbf{F}}(\ker(A - \lambda_M I_n)^{k-1})$. We recall by construction of Jordan normal forms that the number of of Jordan blocks of dimension at least k corresponding to λ_M equals $d_k - d_{k-1}$.

Lemma 2.3.0.1. *Let $A \in \mathrm{UT}_n(\mathbf{F})$, then*

$$A \sim J_{1,n-1} \iff (A - I_n)^{n-2} \neq 0 \ \text{ and } \ \mathrm{rank}(A - I_n) = n - 2.$$

Proof. The two conditions $(A - I_n)^{n-2} \neq 0$ and $\mathrm{rank}(A - I_n) = n - 2$ imply that $(A - I_n)^{n-1} = 0$. Otherwise, $(A - I_n)^{n-1} \neq 0$ yields non-zero superdiagonal entries and $\mathrm{rank}(A - I_n) = n - 1$. Also the condition $\mathrm{rank}(A - I_n) = n - 2$ implies $d_1 = 2$, so we have two Jordan blocks. Since $d_{n-1} = n$ the first assumption $(A - I_n)^{n-2} \neq 0$ gives $d_{n-1} - d_{n-2} \neq 0$, hence there is a Jordan block of dimension $n - 1$. Thus, follows $A \sim J_{n-1,1}$. □

Next we prove that if V is an n-dimensional $\mathbf{F}H$-module of type-$(2, 1, ..., 1)$ then under a mild assumption on the dimension there is always a representing matrix equivalent to $J_{1,n-1}$.

Lemma 2.3.0.2. *Suppose V is an n-dimensional faithful $\mathbf{F}H$-module of type-$(2, 1, ..., 1)$ with $n \leq p + 1$. Then there is an ordered basis $\mathscr{B}$ consistent with the socle series such that $\rho_{\mathscr{B}}(H) = \langle J_{1,n-1}, B\rangle \leq \mathrm{UT}_n(\mathbf{F})$.*

Proof. Fix a basis $\mathscr{B}' = \{v_1, ..., v_n\}$ consistent with the socle series so that the matrices in $\rho_{\mathscr{B}'}(H)$ are upper-triangular unipotent. Suffices to prove that there is always an $A \in \rho_{\mathscr{B}'}(H)$ such that $\alpha_{i,i+1} \neq 0$, $\forall i = 1, ..., n - 2$. For such matrix follows immediately that $\mathrm{rank}(A - I_n) = n - 2$ and a routine calculation yields

$$(A - I_n)^{n-2} = \begin{bmatrix} 0 & 0 & ... & 0 & \alpha_{1,3}\alpha_{3,4}...\alpha_{n-1,n} \\ 0 & 0 & ... & 0 & \alpha_{2,3}\alpha_{3,4}....\alpha_{n-1,n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & ... & 0 & 0 \end{bmatrix} \neq O_n.$$

Therefore our claim will be an application of the previous lemma. To prove this we follow the same strategy as in type-$(1, 1, ..., 1)$ representations. If $\rho_{\mathscr{B}'}(H) = \langle M, N\rangle$, then $m_{i,i+1}, n_{i,i+1}$ cannot be zero simultaneously for any $i = 2, ..., n - 1$, since contradicts our initial claim; the action of H on $V\big/\mathrm{soc}_{i-1}(V)$ fixes a subspace of dimension at least two, hence $m_i = \dim_{\mathbf{F}}(\mathrm{soc}_i(V)\big/\mathrm{soc}_{i-1}(V)) \geq 2$. If no entry other than $(1, 2)$ is zero for either M or N then we are done. Otherwise, the superdiagonal entry of the matrices MN^k, $k < p$, contains $n - 3$ expressions of the form $m_{i,i+1} + kn_{i,i+1}$. Each of these expressions is eliminated by at most one k, hence $n \leq p + 1$ implies the existence of $k \in \mathbf{F}^*$ such that these expressions are non-zero.

Let $A \in \rho_{\mathscr{B}'}(H)$ denote a representing matrix such that $A \sim J_{1,n-1}$. The action of $(A-I_n)^k$ on the basis vector v_{n-1} for $k = 1, ..., n-2$ along with v_n yields a chain of n linearly independent vectors $\mathscr{B} := \{(A-I_n)^{n-2}v_{n-1}, ..., (A-I_n)v_{n-1}, v_{n-1}, v_n\}$ that is socle-preserving. With respect to that basis we obtain $\rho_{\mathscr{B}}(H) = \langle J_{1,n-1}, B\rangle \leq \mathrm{UT}_n(\mathbf{F})$. □

In the next lemma we give a description of the elements in the centralizer $C(J_{1,n-1})$.

Lemma 2.3.0.3. *A centralizing matrix $T \in C(J_{1,n-1})$ has the following form*

$$T = \begin{bmatrix} t_{1,1} & 0 & \cdots & 0 & t_{1,n} \\ t_{2,1} & t_{2,2} & \cdots & t_{2,n-1} & t_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & t_{2,2} & t_{2,3} \\ 0 & 0 & \cdots & 0 & t_{2,2} \end{bmatrix},$$

for various $t_{i,j} \in \mathbf{F}, t_{1,1}, t_{2,2} \in \mathbf{F}^*$.

Proof. Follows from a routine calculation similar to Lemma 2.2.0.2. □

Remark 2.3.0.4. *Notice that when $n = 3$, representations of type-$(2, 1)$ are not faithful since the representing matrices form an abelian subgroup. Thus three-dimensional representations of this type are not considered.*

Before we proceed to the next lemma, we compute that for $n = 4$ the derived subgroup of $\rho_{\mathscr{B}}(H)$ is generated by

$$[J_{1,3}, B] = \begin{bmatrix} 1 & 0 & 0 & -b_{1,3} \\ 0 & 1 & 0 & b_{3,4} - b_{2,3} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Lemma 2.3.0.5. *For $n = 4$, every matrix $T \in Z(\rho_{\mathscr{B}}(H))$ has the following form*

$$T = \begin{bmatrix} 1 & 0 & 0 & t_{1,4} \\ 0 & 1 & 0 & t_{2,4} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

for $t_{i,j} \in \mathbf{F}$.

Proof. Assume $T \in C(J_{1,3})$, $B \in \mathrm{UT}_4(\mathbf{F})$. The condition $T = [J_{1,3}, B]$, gives $t_{1,1} = t_{2,2} = 1$, and $t_{1,2} = t_{2,1} = t_{2,3} = t_{3,4} = 0$. For the resulting T, a routine computation gives $BT = TB$. Hence our claim follows. □

Substituting T from the last lemma in the equality $J_{1,3}B - TBJ_{1,3} = O_4$, gives $t_{1,3} = b_{3,4} - b_{2,3}, t_{1,4} = -b_{1,3}$. Thus, the representation is faithful if and only if $b_{1,3} \neq 0$ or $b_{3,4} - b_{2,3} \neq 0$. Since we would like to transform the second generator in a more handy form, we distinguish between the two cases.

Let $\mathscr{B} = \{e_1, e_2, e_3, e_4\}$ denote the basis of Lemma 2.3.0.2. Assume $b_{1,3} \neq 0$ and consider the new basis $\mathscr{B}_1 = \{b_{1,3}e_1 - b_{1,4}e_2, e_2, e_3, b_{2,3}e_3 + b_{1,3}e_4\}$. Then the transition matrix $T_1 := T_{\mathscr{B}_1 \leftarrow \mathscr{B}}$ is a change of basis consistent with the socle series that fixes $J_{1,n-1}$ and transforms B to

$$T_1^{-1}BT_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & b_{2,4} \\ 0 & 0 & 1 & b_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

If $b_{1,3} = 0$ (hence, $b_{2,3} - b_{3,4} \neq 0$), $b_{1,4} \neq 0$, we can transform $\mathscr{B}$ to $\mathscr{B}_2 = \{t_{2,2}e_1 + t_{2,3}e_2, t_{2,2}e_2 + t_{2,3}e_3, t_{2,2}e_3, e_4 + e_3\}$, with $t_{2,2} = \dfrac{1}{b_{1,4}}, t_{2,3} = t_{2,2} \cdot \dfrac{b_{1,4} - b_{2,4}}{b_{2,3} - b_{3,4}}$. The resulting transition matrix $T_2 := T_{\mathscr{B}_2 \leftarrow \mathscr{B}}$ transforms B to

$$T_2^{-1}BT_2 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & b_{2,4} & 0 \\ 0 & 0 & 1 & b_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

If $b_{1,4} = 0$, then $\mathscr{B}$ can be transformed to $\mathscr{B}_3 = \{e_1 + b_{3,4}e_2, e_2 + b_{2,3}e_3, e_3, e_4\}$ with the transition matrix T_3 giving

$$T_3^{-1}BT_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & b_{2,4} & 0 \\ 0 & 0 & 1 & b_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

All the above summarize to the following theorem.

Theorem 2.3.0.6. *Suppose* $\mathbf{F}$ *is a field of characteristic* $p \geq 3$ *and* V *is a faithful representation of* H *over* $\mathbf{F}$ *of type-*$(2,1,1)$*. Then there is a change of basis* $\mathscr{B}$ *consistent with the socle series such that* $\rho_{\mathscr{B}}(H) = \langle J_{1,3}, B \rangle$*. Furthermore, we have the following cases:*

(1) If $b_{1,3} \neq 0$*, then the basis can be chosen so that*

$$B = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & b_{2,4} \\ 0 & 0 & 1 & b_{2,3} \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

(2) *If* $b_{1,3} = 0$ *and* V *faithful indecomposable, then the basis can be chosen so that*

$$B = \begin{bmatrix} 1 & 0 & 0 & \zeta \\ 0 & 1 & b_{2,3} & 0 \\ 0 & 0 & 1 & b_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

while if V *is decomposable, so that*

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & b_{2,3} & 0 \\ 0 & 0 & 1 & b_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Finally for arbitrary $n \geq 5$, we obtain the next proposition.

Proposition 2.3.0.7. *Suppose* $\mathbf{F}$ *is a field of characteristic* p *and* V *is a faithful representation of* H *over* $\mathbf{F}$ *of type-*$(2, 1, ..., 1)$ *and dimension* $n \leq p + 1$. *Then there is a choice of basis* $\mathscr{B}$ *for* V*, such that* $\rho_{\mathscr{B}}(H) = \langle J_{1,n-1}, B\rangle$. *Therefore, these representations are parameterised by points* $(b_{1,3}, ..., b_{n-1,n}) \in \mathbf{F}^{\frac{n^2-n+2}{2}}$, *subject to the relations* $[J_{1,n-1}, [J_{1,n-1}, B]] = [B, [J_{1,n-1}, B]] = 0$.

2.4 Type-$(1, 1, ..., 2)$ Representations

Let V denote an n-dimensional left $\mathbf{F}H$-module and $\mathscr{B}' = \{v_1, ..., v_n\}$ a fixed basis such that the representing matrices are upper-triangular unipotent. We define a right $\mathbf{F}H$-module structure on the dual V^* by setting $(v_i^* \cdot h)(u) := v_i^*(h \cdot u)$ on the dual basis and extending linearly. Set $\rho^*_{\mathscr{B}'} : H \to \mathrm{GL}(V^*)$ for the induced linear representation of this action. If $A \in \mathrm{GL}_n(\mathbf{F})$ represents $\rho_{\mathscr{B}'}(h) : V \to V$ for some $h \in H$, then the transpose $A^\top$ represents the dual homomorphism $\rho^*_{\mathscr{B}'}(h) : V^* \to V^*$. Since A and $A^\top$ are similar, up to permutation of Jordan blocks they have the same Jordan form.

Generally V and V^* need not have the same socle type neither to obey any rule. However, if V is of type-$(1,1,...,2)$ and $\mathscr{B}'$ consistent with the socle series, then the image of $\rho_{\mathscr{B}'}(H)$ consists of matrices

$$\begin{bmatrix} 1 & c_{1,2} & c_{1,3} & ... & c_{1,n} \\ 0 & 1 & c_{2,3} & ... & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 1 & 0 \\ 0 & 0 & ... & 0 & 1 \end{bmatrix},$$

whose transpose induce a representation of type-$(2,1,...,1)$. Therefore, the dual module V^* defines a type-$(2,1,...,1)$ representation. From the previous section we know that in $\rho^*_{\mathscr{B}'}(H)$ a matrix equivalent to $J_{1,n-1}$ exists. Thus, up to permutation of Jordan blocks we can assume that among the representing matrices of a type-$(1,1,...,2)$ representation there is always one equivalent to $J_{n-1,1}$. So we conclude to the following.

Lemma 2.4.0.1. *Suppose* $\mathbf{F}$ *is a field of characteristic* p *and* V *is a faithful representation of* H *over* $\mathbf{F}$ *of type-*$(1,1,...,2)$ *and dimension* $n \leq p+1$*. Then there is a choice of basis for* V *such that* $\rho_{\mathscr{B}}(H) = \langle J_{n-1,1}, B\rangle$.

In the next lemma we give a description of the elements in the centralizer $C(J_{n-1,1})$.

Lemma 2.4.0.2. *A matrix* $T \in C(J_{n-1,1})$ *has always the following form*

$$T = \begin{bmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,n-1} & t_{1,n} \\ 0 & t_{1,1} & \cdots & t_{1,n-2} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & t_{1,1} & 0 \\ 0 & 0 & \cdots & t_{n,n-1} & t_{n,n} \end{bmatrix},$$

for various $t_{i,j} \in \mathbf{F}, t_{1,1}, t_{n,n} \in \mathbf{F}^*$.

Proof. Follows from a routine calculation similar to Lemma 2.2.0.2. □

Remark 2.4.0.3. *Notice that for $n = 3$ representations of type-$(1,2)$ are not faithful, since the representing matrices form an abelian subgroup. Thus three-dimensional representations of this type are not considered.*

Before we proceed to the next lemma, we compute the commutator of $\rho_{\mathscr{B}}(H)$ when $n = 4$,

$$[J_{3,1}, B] = \begin{bmatrix} 1 & 0 & b_{2,3} - b_{1,2} & b_{2,4} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Lemma 2.4.0.4. *For $n = 4$, every matrix $T \in Z(\rho_{\mathscr{B}}(H))$ has the following form*

$$T = \begin{bmatrix} 1 & 0 & t_{1,3} & t_{1,4} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

for $t_{i,j} \in \mathbf{F}$.

Proof. Assume $T \in C(J_{3,1})$, $B \in \mathrm{UT}_4(\mathbf{F})$. The condition $T = [J_{3,1}, B]$ gives $t_{1,1} = t_{4,4} = 1$, $t_{1,2} = t_{4,3} = 0$. Thus our assertion follows immediately. □

Substituting the resulting T in the condition $J_{3,1}B - TBJ_{3,1} = O_4$, gives $t_{1,3} = b_{2,3} - b_{1,2}, t_{1,4} = b_{2,4}$. If $b_{2,4} = 0$, then in $\rho_{\mathscr{B}}(H)$ every element has zero $(2,4)$-entry. The latter implies that $\dim_{\mathbf{F}}(\mathrm{soc}_2(V)) = 2$ which is a contradiction. Hence we can assume that $b_{2,4} \neq 0$ always.

If $\mathscr{B} = \{e_1, e_2, e_3, e_4\}$ denotes the basis of Lemma 2.4.0.6, we consider the following basis $\mathscr{B}_1 = \{e_1, -b_{2,3}e_1 + b_{2,4}e_2 + b_{1,4}e_3, b_{2,4}e_3 + b_{1,4}e_4, b_{2,4}e_4\}$. Then the transition matrix $T := T_{\mathscr{B}_1 \leftarrow \mathscr{B}}$ is a change of basis consistent with the socle series that fixes

$J_{3,1}$ and transforms B to the following matrix

$$T^{-1}BT = \begin{bmatrix} 1 & b_{1,2} & b_{1,3} + \dfrac{(b_{1,2} - b_{2,3})b_{1,4}}{b_{2,4}} & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Finally, assume that $\rho^1_{\mathscr{B}_1} = \langle J_{3,1}, B_1 \rangle, \rho^2_{\mathscr{B}_2} = \langle J_{3,1}, B_2 \rangle$ are two representations and $\mathscr{B}_1, \mathscr{B}_2$ bases as constructed above. Then $\rho^1_{\mathscr{B}_1} \sim \rho^2_{\mathscr{B}_2}$, if an invertible matrix $P \in \mathrm{GL}_4(\mathbf{F})$ that stabilises the socle series exists, such that $P \in C(J_{3,1})$ and $P^{-1}B_1P = B_2$. A routine computation shows that the two conditions imply

$$P = \begin{bmatrix} p_{1,1} & 0 & p_{1,3} & p_{1,4} \\ 0 & p_{1,1} & 0 & 0 \\ 0 & 0 & p_{1,1} & 0 \\ 0 & 0 & 0 & p_{1,1} \end{bmatrix},$$

and that different pairs $(b_{1,2}, b_{1,3}) \in \mathbf{F}^2$ define inequivalent representations of these type. All the above summarize to the following theorem.

Theorem 2.4.0.5. *Suppose* $\mathbf{F}$ *is a field of characteristic* $p \geq 3$ *and* V *a four-dimensional faithful representation of* H *over* $\mathbf{F}$ *of type-*$(1, 1, 2)$*. Then there is a choice of basis* $\mathscr{B}$ *consistent with the socle series such that* $\rho_{\mathscr{B}}(H) = \langle J_{3,1}, B \rangle$ *with*

$$B = \begin{bmatrix} 1 & b_{1,2} & b_{1,3} & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Furthermore, these representations are parameterised by points in $\mathbf{F}^2$*.*

Finally for arbitrary $n \geq 5$, we obtain the next proposition.

Proposition 2.4.0.6. *Suppose* $\mathbf{F}$ *is a field of characteristic* $p \geq 3$ *and* V *a faithful representation of* H *over* $\mathbf{F}$ *of type-*$(1, 1, ..., 2)$ *and dimension* $n \leq p + 1$*. Then there is a choice of basis* $\mathscr{B}$ *for* V*, such that* $\rho_{\mathscr{B}}(H) = \langle J_{n-1,1}, B \rangle$*. Therefore, these representations are parameterised by points* $(b_{1,2}, ..., b_{n-2,n}) \in \mathbf{F}^{\frac{n^2-n-2}{2}}$*, subject to the relations* $[J_{n-1,1}, [J_{n-1,1}, B]] = [B, [J_{n-1,1}, B]] = 0$*.*

2.5 Type-$(1, 2, 1)$ Representations

Let V denote a left four-dimensional $\mathbf{F}H$-module of type-$(1, 2, 1)$. We fix a basis $\mathscr{B}$ such that $\rho_{\mathscr{B}}(H) \leq \mathrm{UT}_4(\mathbf{F})$. Then $\rho_{\mathscr{B}}(H)$ consists of matrices with the following form

$$\begin{bmatrix} 1 & c_{1,2} & c_{1,3} & c_{1,4} \\ 0 & 1 & 0 & c_{2,4} \\ 0 & 0 & 1 & c_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad c_{i,j} \in \mathbf{F}.$$

We start off by investigating the Jordan normal form of matrices in $\rho_{\mathscr{B}}(H)$. To this end we use an idea introduced in [18], the *socle-tabloid* associated to V. Before we proceed we point out an important property of V. In [18, Theorem 2.2.2], it is proven the existence of a basis that is both socle-preserving for V and up to permutation of the dual basis elements, socle-preserving for V^*.

For the rest of this section every basis of V is assumed to have the above property.

Definition 2.5.0.1. *[18, Definition 2.2.3] Let V denote an n-dimensional left $\mathbf{F}P$-module for some p-group P and fix a basis $\mathscr{B}$. We define the socle-tabloid of V to be the tabloid $\mathtt{t}_V$, where the boxes of the tabloid are in bijective correspondence with the elements of $v \in \mathscr{B}$ filled with the following rule:*

$$v \in \mathrm{soc}_i(V) \setminus \mathrm{soc}_{i-1}(V), \;\; v^* \in \mathrm{soc}_j(V^*) \setminus \mathrm{soc}_{j-1}(V^*)$$

corresponds to $\boxed{j}$ in i-th row.

Suppose V is a left $\mathbf{F}H$-module of socle-length k. Then the quotient module $V/\mathrm{soc}_{k-i}(V)$ has socle-length i and corresponds to a submodule of the dual V^* with the same socle-length. Therefore, given an element in this submodule it cannot sit in the socle series of V^* further than $\mathrm{soc}_i(V^*)$. This idea can be translated in the following lemma.

Lemma 2.5.0.2. *[18, Lemma 2.2.7] Let V denote an $\mathbf{F}P$-module with socle-tabloid $\mathtt{t}_V$. Then the i-th row from the bottom of $\mathtt{t}_V$ contains at least one $\boxed{i}$ and no entries which exceed i.*

The last lemma implies that if V is four-dimensional $\mathbf{F}H$-module of type-$(1, 2, 1)$, then we can have only the following two socle-tabloids

$$\begin{array}{cc} \boxed{3} & \\ \boxed{2} & \boxed{2} \\ \boxed{1} & \end{array} \qquad \begin{array}{cc} \boxed{3} & \\ \boxed{2} & \boxed{1} \\ \boxed{1} & \end{array}.$$

The frequency of appearances of each number in a socle-tabloid gives the dual-type. Thus, the left tabloid corresponds to type-$(1, 2, 1)$ for V^*, whereas the right to type-$(2, 1, 1)$. For the last case we have proven that a matrix with Jordan normal form $J_{3,1}$ always exists. Therefore, representations with socle-tabloid $\begin{array}{cc} \boxed{3} & \\ \boxed{2} & \boxed{1} \\ \boxed{1} & \end{array}$ contain a matrix with Jordan normal form $J_{3,1}$. The last is not true for these with socle-tabloid $\begin{array}{cc} \boxed{3} & \\ \boxed{2} & \boxed{2} \\ \boxed{1} & \end{array}$. Finally, throughout this section we fix a basis $\mathscr{B}'$ that preserves the socle-type of V, and up to permutation, the socle-type of V^*. The proof of the existence of such a basis can be found in [18, Theorem 2.2.2].

Representations with socle-tabloid $\begin{array}{cc} \boxed{3} & \\ \boxed{2} & \boxed{1} \\ \boxed{1} & \end{array}$

Suppose V is a four-dimensional $\mathbf{F}H$-module with socle-tabloid $\begin{array}{cc} \boxed{3} & \\ \boxed{2} & \boxed{1} \\ \boxed{1} & \end{array}$. Let $\mathscr{B}'$ denote a basis such that the representing matrices are upper-triangular unipotent and is socle-preserving both for V and V^*. Then $\rho_{\mathscr{B}'}(H)$ consists of matrices of the following form

$$\begin{bmatrix} 1 & c_{1,2} & c_{1,3} & c_{1,4} \\ 0 & 1 & 0 & c_{2,3} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Recall from type-$(2, 1, ..., 1)$ representations that a matrix with Jordan normal form $J_{1,3}$ always exists. Since the dual of a representation with socle-tabloid $\begin{array}{cc} \boxed{3} & \\ \boxed{2} & \boxed{1} \\ \boxed{1} & \end{array}$ are of type-$(2, 1, 1)$, follows that up to permutation of Jordan blocks we can always find a matrix with Jordan normal form $J_{3,1}$.

Lemma 2.5.0.3. *Suppose V is a four-dimensional $\mathbf{F}H$-module with socle-tabloid*

$\begin{array}{|c|c|}\hline 3 & \\ \hline 2 & 1 \\ \hline 1 & \\ \hline\end{array}$. *Then there is a choice of basis* $\mathscr{B}$ *consistent with the socle series, such that* $\rho_{\mathscr{B}}(H)$ *is generated by*

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b_{1,2} & 1 & b_{1,4} \\ 0 & 1 & 0 & b_{2,4} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Proof. Assume that $\rho_{\mathscr{B}'}(H) = \langle M, N \rangle$ with $M \sim J_{3,1}$. Pick any element $e_1 \in V \setminus \mathrm{soc}_2(V)$. Then for $e_3 = (M - I_4)(e_1), e_4 = (M - I_4)^2(e_1)$ and a choice of $e_2 \in V^M \setminus V^H$, M transforms to the following matrix

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

From the definition of M follows that the change of basis P is consistent with the socle series, hence conjugation is well defined, i.e., $B := P^{-1}NP$ is consistent with the socle series. Furthermore, since $b_{1,3} = 0$ would imply $\mathrm{soc}(V) = 2$, we can assume $b_{1,3} \neq 0$. Thus, for the right choice of e_2 we acquire $b_{1,3} = 1$. □

We wish to describe the centraliser of A and investigate how it acts on B.

Lemma 2.5.0.4. *The centralizer* $C(A)$ *consists of matrices of the following form*

$$T = \begin{bmatrix} t_{1,1} & t_{1,2} & t_{1,3} & t_{1,4} \\ 0 & t_{1,1} & 0 & t_{1,2} \\ 0 & 0 & t_{2,2} & t_{3,4} \\ 0 & 0 & 0 & t_{1,1} \end{bmatrix}.$$

Proof. Follows from a routine computation on $TA - AT = O_4$. □

Next we investigate how elements of $C(A)$ act on B. Assume $T \in C(A)$, then the equation $TB - BT = O_4$ yields explicitly

$$\begin{bmatrix} 0 & 0 & t_{1,1} - t_{2,2} & (b_{2,4} - b_{1,2})t_{1,2} - t_{3,4} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = O_4.$$

Thus, T commutes with B if and only if $t_{1,1} = t_{2,2}$, $(b_{2,4} - b_{1,2})t_{1,2} - t_{3,4} = 0$. Furthermore, for the right choice of $T \in C(A) \cap C(B)$ we can assume that $Z(\rho_{\mathscr{B}}(H)) = \langle T \rangle$, since $Z(\rho_{\mathscr{B}}(H)) \subset C(A) \cap C(B)$. The relation $AB - TBA = O_4$ induced from the presentation of $\rho_{\mathscr{B}}(H)$

$$\begin{bmatrix} 0 & -t_{1,2} & -t_{1,3} & b_{2,4} - b_{1,2} - t_{1,2} - t_{1,4} \\ 0 & 0 & 0 & -t_{1,2} \\ 0 & 0 & 0 & -t_{1,3} \\ 0 & 0 & 0 & 0 \end{bmatrix} = O_4,$$

implies $t_{1,2} = t_{1,3} = t_{3,4} = 0, t_{1,4} \neq 0$ and $b_{2,4} - b_{1,2} = t_{1,4}$. Thus for B we must have $b_{1,2} \neq b_{2,4}$. Summarizing all the above yields the following theorem.

Theorem 2.5.0.5. *Suppose V is a faithful four-dimensional $\mathbf{F}H$-module with socle-tabloid* $\begin{array}{|c|c|}\hline 3 & \\ \hline 2 & 1 \\ \hline 1 & \\ \hline \end{array}$. *Then there is a choice of basis $\mathscr{B}$ consistent with the socle series, such that $\rho_{\mathscr{B}}(H)$ is generated by*

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b_{1,2} & 1 & b_{1,4} \\ 0 & 1 & 0 & b_{2,4} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

subject to the constraint $b_{1,2} \neq b_{2,4}$. Therefore, these representations are parameterised by the set $\{(b_{1,2}, b_{1,4}, b_{2,4}) \in \mathbf{F}^3 \mid b_{1,2} \neq b_{2,4}\}$.

Representations with socle-tabloid $\begin{array}{|c|c|}\hline 3 & \\ \hline 2 & 2 \\ \hline 1 & \\ \hline \end{array}$

This time there is no guarantee that a matrix with Jordan normal form $J_{3,1}$ exists. However, with the right choice of basis we obtain a suitable set of generators.

Lemma 2.5.0.6. *Suppose V is a four-dimensional $\mathbf{F}H$-module with socle-tabloid* $\begin{array}{|c|c|}\hline 3 \\ \hline 2 & 2 \\ \hline 1 \\ \hline\end{array}$. *Then there is a choice of basis $\mathscr{B}$ consistent with the socle series, such that $\rho_{\mathscr{B}}(H)$ is generated by the following matrices*

$$A = \begin{bmatrix} 1 & a_{1,2} & a_{1,3} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b_{1,2} & b_{1,3} & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Proof. Assume that $\rho_{\mathscr{B}'}(H) = \langle M, N \rangle$. We construct the seeking basis as follows; choose any $e_1 \in V \setminus \mathrm{soc}_2(V)$ and set $e_2 = (M - I_4)(e_1), e_3 = (N - I_4)(e_1), e_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}^T$. Then the resulting set of vectors $\mathscr{B} := \{e_1, e_2, e_3, e_4\}$ forms a basis for V. Calculating the generating matrices M and N on this new basis yields our claim. □

The commutator $C = [A, B] = ABA^{-1}B^{-1}$ in that case becomes

$$C = \begin{bmatrix} 1 & 0 & 0 & a_{1,2} - b_{1,3} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Thus the condition $C \neq I_4$ gives $a_{1,2} - b_{1,3} \neq 0$. We wish to classify equivalent classes of representations of this form. From the last lemma it is obvious that $(a_{1,2}, b_{1,2}) \neq (0,0), (a_{1,3}, b_{1,3}) \neq (0,0)$, since otherwise the fixed point space is two-dimensional. Two such representations are equivalent if an invertible matrix that stabilises the socle series exists. If P denotes such matrix, the conditions

$P^{-1}AP, P^{-1}BP$ force P to have the following form

$$P = \begin{bmatrix} p_{1,1} & 0 & 0 & p_{1,4} \\ 0 & p_{2,2} & 0 & 0 \\ 0 & 0 & p_{2,2} & 0 \\ 0 & 0 & 0 & p_{2,2} \end{bmatrix}.$$

Explicit calculations on the above two conditions imply the following theorem.

Theorem 2.5.0.7. *Suppose V is a faithful four-dimensional $\mathbf{F}H$-module with socle-tabloid $\begin{array}{|c|c} \cline{1-1} 3 & \\ \hline 2 & \multicolumn{1}{c|}{2} \\ \hline 1 & \\ \cline{1-1} \end{array}$. Then there is a choice of basis $\mathscr{B}$ consistent with the socle series, such that $\rho_{\mathscr{B}}(H)$ is generated by*

$$A = \begin{bmatrix} 1 & a_{1,2} & a_{1,3} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b_{1,2} & b_{1,3} & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Furthermore, these representations are parameterised by points in the projective space $\{[a_{1,2} : a_{1,3} : b_{1,2} : b_{1,3}] \in \mathbb{P}^3_{\mathbf{F}} \mid (a_{1,2}, b_{1,2}) \neq (0,0), (a_{1,3}, b_{1,3}) \neq (0,0), a_{1,2} \neq b_{1,3}\}$.

Chapter 3

Three-dimensional case

3.1 Introduction

Let $\mathbf{F}$ denote a field of positive characteristic $\mathrm{char}(\mathbf{F}) = p > 0$. Assume that H is the extraspecial group of order p^3 and exponent p endowed with the following presentation

$$H = \langle g_1, g_2 \mid g_1^p = g_2^p = e,\ [g_1,[g_1,g_2]] = e,\ [g_2,[g_1,g_2]] = e,\ [g_1,g_2]^p = e\rangle.$$

We wish to study three-dimensional invariants of H over $\mathbf{F}$.

Suppose V is a three-dimensional left $\mathbf{F}H$-module. From Theorem 2.2.0.5 we know the existence of a basis $\mathscr{B}'$ consistent with the socle series, such that the group of representing matrices $\rho_{\mathscr{B}'}(H)$ is generated by

$$J_3 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix},\ B = \begin{bmatrix} 1 & b_{1,2} & 0 \\ 0 & 1 & b_{2,3} \\ 0 & 0 & 1 \end{bmatrix}.$$

To make our computations easier we change the generators with something equivalent. If $\mathscr{B}' = \{e_1, e_2, e_3\}$, then $\mathscr{B} = \{2e_1, e_2 + b_{1,2}/(b_{1,2} - b_{2,3}) \cdot e_1, e_3 + b_{2,3}/2(b_{1,2} - b_{2,3}) \cdot e_2 + b_{1,2}b_{2,3}/2(b_{1,2} - b_{2,3})^2 \cdot e_1\}$ forms a basis consistent with the socle series that transforms $\{J_3, B\}$ to the following matrices

$$g_1 = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, g_2 = \begin{bmatrix} 1 & 2c_1 & 0 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix}, \ c_1, c_2 \in \mathbf{F}$$

with the commutator $h = [g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2$ given by

$$h = \begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \ c = 2(c_2 - c_1).$$

It is not difficult to see that $\{g_1, g_2\}$ forms a generating set for H. We denote the group of representing matrices with respect to the new basis by $\rho_{\mathscr{B}}(H)$. Finally since we consider faithful representations, throughout we always assume $c \neq 0$.

3.2 Generic Case

In this section we show that for any faithful generic three-dimensional $\mathbf{F}H$-module V, the ring of invariants $\mathbf{F}[V]^H$ is a complete intersection. In Lemma 3.2.0.2 we compute $\mathbf{F}(V)^H$ and we apply SAGBI/divide-by-x algorithm on the invariant field generators to construct a generating set for $\mathbf{F}[V]^H$. To this end we make use of the following result which forms the base of our technique.

Theorem 3.2.0.1. *[7, Theorem 4.3] Let V_3 denote the representation of $(\mathbf{F}, +)$ dual to the symmetric square V_2^* and $(W, +) \leq (\mathbf{F}, +)$ a finite subgroup. Then $\mathbf{F}[V_3]^W$ is the hypersurface generated by $\{x, \delta, \mathbf{N}_W(y), \mathbf{N}_W(z)\}$, where $\delta = y^2 - xz$. Furthermore, this generating set is a SAGBI basis with respect to the graded reverse lexicographic order with $z > y > x$.*

We consider the above theorem when $W \cong C_p$ to construct the invariant field generators.

Think of the composition series $\{e\} \triangleleft H_1 \triangleleft H_2 \triangleleft H$, where $H_1 = \langle g_1 \rangle, H_2 = \langle g_1, h \rangle$. We wish to describe the invariant rings for the successive quotients of the composition series and apply the identity $(\mathbf{F}[V]^N)^{G/N} = \mathbf{F}[V]^G$. However this cannot happen directly. The methods we have in our disposal are for group actions on polynomial algebras, hence whenever $\mathbf{F}[V]^N$ fails to be such an algebra the quotient group G/N is not acting nicely for our convention. To resolve this issue we pass to a localized level whereby we can apply the group action on polynomial algebras.

We first consider the case $H_1 \cong C_p$. Then Theorem 3.2.0.1 implies $\mathbf{F}[V]^{H_1} = \mathbf{F}[x, \delta, \mathbf{N}_{g_1}(y), \mathbf{N}_{g_1}(z)]$, hence the H_2/H_1-action is not on a polynomial algebra. Localizing at x yields

$$\mathbf{F}[V]^{H_1}[x^{-1}] = \mathbf{F}[x, \delta, \mathbf{N}_{g_1}(y)][x^{-1}]. \tag{3.2.1}$$

Now the right hand side algebra is polynomial and since $H_2/H_1 \cong \langle h \rangle$ we obtain

$$\mathbf{F}[V]^{H_2}[x^{-1}] = (\mathbf{F}[V]^{H_1})^{H_2/H_1}[x^{-1}] = \mathbf{F}[x, \delta, \mathbf{N}_{g_1}(y)]^{\langle h \rangle}[x^{-1}]. \tag{3.2.2}$$

The $\langle h \rangle$-action on $\mathbf{F}[x, \delta, \mathbf{N}_{g_1}(y)]$ induces an $\mathbf{F}\langle h \rangle$-module structure. Let V_1 denote the $\mathbf{F}$-vector space spanned by the algebra generators $\{x, \delta, \mathbf{N}_{g_1}(y)\}$ shifted to degree one, i.e., $V_1 = \mathrm{Span}_{\mathbf{F}}\{x, y_1 = \mathbf{N}_{g_1}(y)/x^{p-1}, y_2 = \delta/x\}$. In terms of this new basis we compute

$$y_1 \cdot h = y_1,\ y_2 \cdot h = y_2 - cx.$$

Thus $\langle h \rangle$ acts as a Nakajima group and [8, Theorem 8.0.7] implies $\mathbf{F}[V_1]^{\langle h \rangle} = \mathbf{F}[x, y_1, \mathbf{N}_h(y_2)]$. Substituting in (3.2.2) and clearing out the denominators minimally returns

$$\mathbf{F}[V]^{H_2}[x^{-1}] = \mathbf{F}[x, \mathbf{N}_{g_1}(y), \mathbf{N}_h(\delta)][x^{-1}], \tag{3.2.3}$$

where $\mathbf{N}_h(\delta) = \delta^p - c^{p-1}x^{2(p-1)}\delta$.

Now applying the $H/H_2 \cong \langle g_2 \rangle$-action on (3.2.3) gives

$$\mathbf{F}[V]^{H}[x^{-1}] = \mathbf{F}[x, \mathbf{N}_{g_1}(y), \mathbf{N}_h(\delta)]^{\langle g_2 \rangle}[x^{-1}]. \tag{3.2.4}$$

Set $z_2 := \mathbf{N}_h(\delta)$ and $\Delta_2 := g_2 - 1 \in \mathbf{F}\langle g_2 \rangle$ for the twisted derivation induced by g_2. Then z_2 generates a triangular basis of H_2-invariants

$$\{z_0 = \Delta_2^2(z_2), z_1 = \Delta_2(z_2), z_2 = \mathbf{N}_h(\delta)\}.$$

Note that as $\mathbf{F}\langle g_2\rangle$-module, the vector space spanned by this basis is isomorphic to V_3, the three dimensional indecomposable representation of $\langle g_2\rangle$. A routine computation gives

$$z_2 = \mathbf{N}_h(\delta),\ z_1 = \gamma_0^p x^p \mathbf{N}_{g_1}(y) + (c_2^{2p} - c_2^2 c^{p-1})x^{2p},\ z_0 = c^p(c_2^p - c_2)x^{2p},$$

thus $\mathbf{F}[z_0, z_1, z_2] = \mathbf{F}[x^{2p}, x^p\mathbf{N}_{g_1}(y), \mathbf{N}_h(\delta)]$ and

$$\mathbf{F}[x^{2p}, x^p\mathbf{N}_{g_1}(y), \mathbf{N}_h(\delta)][x^{-1}] = \mathbf{F}[x, \mathbf{N}_{g_1}(y), \mathbf{N}_h(\delta)][x^{-1}].$$

Therefore, from (3.2.4) follows that

$$\mathbf{F}[V]^H[x^{-1}] = \mathbf{F}[x, \mathbf{N}_{g_1}(y), \mathbf{N}_h(\delta)]^{\langle g_2\rangle}[x^{-1}] = \mathbf{F}[z_0, z_1, z_2]^{\langle g_2\rangle}[x^{-1}]. \tag{3.2.5}$$

Denote $\widehat{\delta} = z_1^2 - 2z_0z_2 - z_0z_1$. Using Theorem 3.2.0.1 gives $\mathbf{F}[z_0, z_1, z_2]^{\langle g_2\rangle} = \mathbf{F}[z_0, \widehat{\delta}, \mathbf{N}_{g_2}(z_1), \mathbf{N}_{g_2}(z_2)]$ and (3.2.5) implies

$$\mathbf{F}[V]^H[x^{-1}] = \mathbf{F}[z_0, \widehat{\delta}, \mathbf{N}_{g_2}(z_1)][x^{-1}]. \tag{3.2.6}$$

Let D denote the image of $\widehat{\delta}$ in $\mathbf{F}[V]$ and $\mathbf{N}_H(y)$ the H-norm of y

$$\mathbf{N}_H(y) = \mathbf{N}_{g_1}^p(y) - ({c_2}^p - c_2)^{p-1}x^{p(p-1)}\mathbf{N}_{g_1}(y). \tag{3.2.7}$$

Using (3.2.6) this time, gives

$$\mathbf{F}[V]^H[x^{-1}] = \mathbf{F}[x, \mathbf{N}_H(y), D][x^{-1}].$$

Expanding the definition of D yields

$$\begin{aligned} D &= \Delta_2^2(\mathbf{N}_h(\delta)) - 2\mathbf{N}_h(\delta)\Delta_2^2(\mathbf{N}_h(\delta)) - \Delta_2(\mathbf{N}_h(\delta))\Delta_2^2(\mathbf{N}_h(\delta)) \\ &= c^{2p}x^{2p}\mathbf{N}_{g_1}^2(y) + (2c^p(c_2^{2p} - c_2^2c^{p-1}) - c^{2p}({c_2}^p - c_2))x^{3p}\mathbf{N}_{g_1}(y) \\ &- 2c^p(c_2^p - c_2)x^{2p}\mathbf{N}_h(\delta) + ((c_2^{2p} - c_2^pc^{p-1})^2 - c^p(c_2^p - c_2)(c_2^{2p} - c_2^2c^{p-1}))x^{4p}. \end{aligned}$$

To make the above expression simpler, we divide through by $2c^px^{2p}$ and get rid of the last summand. Set for simpilcity $\gamma_0 = c_2 - c_1, \gamma_1 := c_1^p - c_1$ and $\gamma_2 := c_2^p - c_2$. Then the resulting polynomial

$$\mathbf{D} = \underbrace{\gamma_0^p\,\mathbf{N}_{g_1}^2(y)}_{\alpha} + (c_2^{2p} - c_2^2\gamma_0^{p-1} - \gamma_0^p\gamma_2)x^p\mathbf{N}_{g_1}(y) - \underbrace{\gamma_2\mathbf{N}_h(\delta)}_{\beta}, \tag{3.2.8}$$

is an H-invariant. The following lemma shows that is a generator of $\mathbf{F}(V)^H$ too.

Lemma 3.2.0.2. $\mathbf{F}(V)^H = \mathbf{F}(x, \mathbf{N}_H(y), \mathbf{D})$.

Proof. Note that $\mathrm{LT}(\mathbf{N}_H(y)) = y^{p^2}$. Since on the first two variables H is acting as a two elementary abelian p-group, [9, Theorem 3.7.5] implies that $\{x, \mathbf{N}_H(y)\}$ form minimum degree invariants in x and y respectively. Also, equality (3.2.2) implies $\mathbf{F}(V)^{H_2} = \mathbf{F}(x, \mathbf{N}_{g_1}(y), \mathbf{N}_H(\delta))$ and the field inclusion $\mathbf{F}(V)^H \subset \mathbf{F}(V)^{H_2}$ that the minimum z-degree H-invariant has z-degree at least p. From equation (3.2.8) follows that $\deg_z(\mathbf{D}) = p$. Hence $\mathbf{D}$ is of minimum z-degree. Now the claim is a consequence of Theorem 1.4.2.6. $\square$

For $\gamma_3 := \gamma_0 - \gamma_1 = c_2 - c_1^p$, expanding the new $\mathbf{D}$ we observe that the lead term comes from the sum of the lead terms of α and β, $\mathrm{LT}(\mathbf{D}) = \gamma_3\, y^{2p}$, while the second term from α and equals $-2\gamma_0^p x^{p-1} y^{p+1}$. So working modulo the ideal $\langle x^p \rangle \lhd \mathbf{F}[V]$ gives

$$\mathbf{D} \equiv_{\langle x^p \rangle} \gamma_3\, y^{2p} - 2\gamma_0^p x^{p-1} y^{p+1}. \tag{3.2.9}$$

For reasons that will become obvious later on we investigate and present the third and fourth term in order. Expanding and reducing modulo $\langle x^{p+1} \rangle \lhd \mathbf{F}[V]$ gives

$$\mathbf{D} \equiv_{\langle x^{p+1} \rangle} \gamma_3\, y^{2p} - 2\gamma_0^p x^{p-1} y^{p+1} + (c_2^{2p} - c_2^2 \gamma_0^{p-1} - \gamma_0^p \gamma_2) x^p y^p + \gamma_2 x^p z^p.$$

Set $\mathscr{B} = \{x, \mathbf{N}_H(y), \mathbf{D}, \mathbf{N}_H(z)\}$ where $\mathbf{N}_H(z)$ denotes the z-norm. We wish to extend $\mathscr{B}$ to a SAGBI basis by applying the SAGBI/divide-by-x algorithm. In what follows we always assume that $\gamma_i \neq 0$, for $i = 0, \ldots, 3$. Moreover for simplicity we set $\gamma_4 := \gamma_1^p + \gamma_1 - \gamma_0 = c_1^{p^2} - c_2$. Observe that in $\mathscr{B}$ there is only one non-trivial tête-à-tête: $(\mathbf{D}^p, \mathbf{N}_H^2(y))$.

Lemma 3.2.0.3. *Subducting the tête-à-tête* $(\mathbf{D}^p, \mathbf{N}_H^2(y))$*, defines an invariant with lead term:* $-2\gamma_1^p \gamma_2/\gamma_3 \cdot x^{p^2-1} y^{p^2+1}$

Proof. We work modulo the ideal in $\langle x^{p^2-1} \rangle \lhd \mathbf{F}[x, y, z]$. For $\mathbf{D}^p$ follows from (4.1.2) that in the quotient ring we have

$$\mathbf{D}^p \equiv_{\langle x^{p^2-1} \rangle} \gamma_3^p\, y^{2p^2} - 2\, \gamma_0^{p^2}\, x^{p(p-1)} y^{p(p+1)}.$$

On the other hand, expanding $\mathbf{N}_H^2(y)$ and reducing modulo x^{p^2-1} gives

$$\mathbf{N}_H^2(y) \equiv_{\langle x^{p^2-1}\rangle} y^{2p^2} - 2(1+\gamma_2^{p-1})x^{p(p-1)}y^{p(p+1)}.$$

Summing up the two parts yields

$$\mathbf{D}^p - \gamma_3^p \mathbf{N}_H^2(y) \equiv_{\langle x^{p^2-1}\rangle} -2\,\gamma_2^{p-1}\gamma_4\, x^{p(p-1)}y^{p(p+1)}.$$

We work modulo the principal ideal $\langle x^{p^2}\rangle \lhd \mathbf{F}[x,y,z]$. Set

$$\widetilde{f}_1 := \mathbf{D}^p - \gamma_3^p \mathbf{N}_H^2(y) + 2\gamma_2^{p-1}\gamma_4/\gamma_3^{\frac{p+1}{2}} \cdot \mathbf{D}^{\frac{(p+1)}{2}} x^{p(p-1)}. \tag{3.2.10}$$

We analyze each part of $\widetilde{f}_1$. The binomial theorem for $\mathbf{D} \equiv_{\langle x^p\rangle} \gamma_3 y^{2p} - 2\gamma_0^p x^{p-1}y^{p+1}$ gives

$$\begin{aligned} \mathbf{D}^{\frac{p+1}{2}} &\equiv_{\langle x^p\rangle} (\gamma_3 y^{2p} - 2\gamma_0^p x^{p-1}y^{p+1})^{\frac{p+1}{2}} \\ &\equiv_{\langle x^p\rangle} \gamma_3^{\frac{p+1}{2}} y^{p(p+1)} - \gamma_0^p\gamma_3^{\frac{p-1}{2}} y^{p(p-1)}x^{p-1}y^{p+1}. \end{aligned}$$

Thus multiplying by $x^{p(p-1)}$ both sides yields

$$\mathbf{D}^{\frac{p+1}{2}} x^{p(p-1)} \equiv_{\langle x^{p^2}\rangle} \gamma_3^{\frac{p+1}{2}} y^{p(p+1)}x^{p(p-1)} - \gamma_0^p\gamma_3^{\frac{p-1}{2}} x^{p^2-1}y^{p^2+1}.$$

Regarding the tête-à-tête difference, expanding the definition gives

$$\begin{aligned} \mathbf{D}^p - \gamma_3^p\mathbf{N}_H^2(y) &= \gamma_0^{p^2}\mathbf{N}_{g_1}^{2p}(y) + ((c_2{}^{2p^2} - c_2{}^{2p}\gamma_0^{p(p-1)}) - \gamma_2^p)x^{p^2}\mathbf{N}_{g_1}^p(y) - \gamma_2^p\mathbf{N}_h^p(\delta) \\ &- \gamma_3^p(\mathbf{N}_{g_1}^{2p}(y) - 2\gamma_2^{p-1}\mathbf{N}_{g_1}^{p+1}(y)x^{p(p-1)} + \gamma_2^{2(p-1)}x^{2p(p-1)}\mathbf{N}_{g_1}^2(y)). \end{aligned}$$

while reducing modulo x^{p^2}

$$\mathbf{D}^p - \gamma_3^p\mathbf{N}_H^2(y) \equiv_{\langle x^{p^2}\rangle} -2\gamma_2^{p-1}\gamma_4 y^{p(p+1)}x^{p(p-1)} - 2\gamma_3^p\gamma_2^{p-1}x^{(p+1)(p-1)}y^{p^2+1}.$$

Summing up the two parts now proves our claim

$$\widetilde{f}_1 \equiv_{\langle x^{p^2}\rangle} -2\gamma_1^p\gamma_2/\gamma_3 \cdot x^{p^2-1}y^{p^2+1}.$$

□

Throughout, along with the previous assumptions (i.e., $\gamma_i \neq 0, \forall i = 0, \ldots, 3$), we assume that $\gamma_4 \neq 0$ too. Notice that $\widetilde{f}_1$ cannot subduct further. Due to the SAGBI/divide-by-x algorithm we divide through by $x^{-(p^2-1)}$ and we attach this new invariant to $\mathscr{B}$. Set $f_1 := \widetilde{f}_1\, x^{-(p^2-1)}$ and $\mathscr{B}_1 := \mathscr{B} \cup \{f_1\}$. Observe that in $\mathscr{B}_1$ there is a unique non-trivial tête-à-tête: $(f_1^p, \mathbf{D}^{\frac{p^2+1}{2}})$.

Lemma 3.2.0.4. *Subducting the tête-à-tête* $(f_1^p, \mathbf{D}^{\frac{p^2+1}{2}})$*, defines an invariant with lead term:* $-\gamma_2^{p^2}\gamma_3^p \cdot x^p z^{p^3}$.

Proof. To find the lead term of that tête-à-tête difference we work modulo $\langle x^{p-1}\rangle \triangleleft \mathbf{F}[V]^H$. From previous calculation, (3.2.9), we obtain

$$\begin{aligned}
\mathbf{D}^{\frac{p^2+1}{2}} &\equiv_{\langle x^p\rangle} (\gamma_3 y^{2p} - 2\gamma_0^p x^{p-1}y^{p+1})^{\frac{p^2+1}{2}} \\
&\equiv_{\langle x^p\rangle} (\gamma_3 y^{2p} - 2\gamma_0^p x^{p-1}y^{p+1})^{\frac{p^2-1}{2}}.(\gamma_3 y^{2p} - 2\,\gamma_0^p y^{p+1}x^{p-1}) \\
&\equiv_{\langle x^p\rangle} \gamma_3^{\frac{p^2-1}{2}} y^{p^3+p} - 2\,\gamma_0^p\,\gamma_3^{\frac{p^2-1}{2}} x^{p-1}y^{p^3+1}.
\end{aligned}$$

Regarding f_1, expanding its definition we see that every term except the leading has a power of x. Therefore, f_1^p does not contribute in the quotient ring for the tête-à-tête difference.

Summing up yields

$$\gamma_3^p f_1^p - \mu\mathbf{D}^{\frac{p^2+1}{2}} \equiv_{\langle x^p\rangle} -2\,\gamma_0^p\,\gamma_3^{\frac{p^2-1}{2}}\,\mu\, x^{p-1}y^{p^3+1}.$$

Set $\mu = -2\gamma_2^{p^2}\gamma_1^{p^2}/\gamma_3^{\frac{p^2-1}{2}}$ and

$$\widetilde{f}_2 := \gamma_3^p f_1^p - \mu\mathbf{D}^{\frac{p^2+1}{2}} - \gamma_0^p\,\frac{\gamma_3^{\frac{p^2+1}{2}}}{\gamma_2^p\,\gamma_1^p}\,\mu\; x^{p-1}\mathbf{N}_H^{p-1}(y)f_1.$$

To prove our claim we work in the polynomial algebra $\mathbf{F}[x, y, z]$ modulo the ideal $J := \langle x^{p+1}, yx^p\rangle$. Using the definition of $\mathbf{N}_H(y)$, (3.2.7), and reducing modulo x^{p+1} we obtain $\mathbf{N}_H^{p-1}(y) \equiv_J y^{p^3-p^2}$. So that

$$x^{p-1}\mathbf{N}_H^{p-1}(y)f_1 \equiv_J -2\,\frac{\gamma_1^p\gamma_2}{\gamma_3}x^{p-1}y^{p^3+1}.$$

Expanding $\mathbf{D}$ in the quotient ring gives

$$\mathbf{D} \equiv_J \gamma_3 y^{2p} - 2\gamma_0^p x^{p-1}y^{p+1} + 2\gamma_2 x^p z^p,$$

hence

$$\mathbf{D}^{\frac{p^2+1}{2}} \equiv_J \gamma_3^{\frac{p^2+1}{2}} y^{p^3+p} - 2\gamma_3^{\frac{p^2-1}{2}} \gamma_0^p x^{p-1} y^{p^3+1}.$$

Furthermore, reducing f_1^p modulo J yields: $f_1^p \equiv_J -\gamma_2^{p^2} x^p z^{p^3}$. All together implies

$$\gamma_3^p f_1^p - \mu \mathbf{D}^{\frac{p^2+1}{2}} - \gamma_0^p \frac{\gamma_3^{\frac{p^2+1}{2}}}{\gamma_1^p \gamma_2} \mu\, x^{p-1} \mathbf{N}_H^{p-1} f_1$$
$$\equiv_J$$
$$-\gamma_2^{p^2} \gamma_3^p\, x^p z^{p^3}.$$

So the leading term of the subduction must be

$$\mathrm{LT}(\widetilde{f_2}) = -\gamma_2^{p^2} \gamma_3^p\, x^p z^{p^3}.$$

□

Set $f_2 := x^{-p} \widetilde{f_2}$ and $\mathscr{B}_2 := \mathscr{B}_1 \cup \{f_2\}$. Since f_2 is homogeneous of degree p^3 such that $\mathrm{LT}(f_2) = z^{p^3}$ we can replace $\mathbf{N}_H(z)$ by f_2. Now every non-trivial tête-à-tête in $\mathscr{B}_2$ subducts to zero.

Proposition 3.2.0.5. *Let V denote a three-dimensional $\mathbf{F}H$-module, satisfying $\gamma_i \neq 0, i = 0, \ldots, 4$. Then $\mathscr{B}_2 = \{x, \mathbf{N}_H(y), \mathbf{D}, f_1, f_2\}$, is a SAGBI basis hence a generating set for $\mathbf{F}[V]^H$. Furthermore, $\mathbf{F}[V]^H$ is a complete intersection with generating relations constructed during the tête-à-tête subduction of $(f_1^p, \mathbf{D}^{\frac{p^2+1}{2}})$ and $(\mathbf{D}^p, \mathbf{N}_G^2(y))$.*

Proof. We have proven already that $\mathscr{B}_2$ is a SAGBI basis. Let $A = \mathbf{F}[\mathscr{B}_2]$ denote the algebra it generates. Since $\mathrm{LM}(\mathbf{D}) = y^{2p}, \mathrm{LM}(f_2) = z^{p^3}$, from [1, Lemma 2.2.7], [7, Lemma 2.6.3] follows that $(x, \mathbf{D}, f_2)\mathbf{F}[V]^H$ is a zero-dimensional ideal and $\{x, \mathbf{D}, f_2\}$ a homogeneous system of parameters. Hence $A \subset \mathbf{F}[V]^H$ is integral. Furthermore, the invariant field $\mathbf{F}(V)^H = \mathbf{F}(x, \mathbf{N}_H(y), \mathbf{D})$ implies $\mathbf{F}[V]^H[x^{-1}] = A[x^{-1}]$. So the equality $\mathbf{F}[V]^H = A$ follows from an application of Theorem 1.4.3.10. □

Corollary 3.2.0.6. *The lead term algebra of $\mathbf{F}[V]^H$ is the $\mathbf{F}$-algebra generated by the set $\mathrm{LT}(\mathscr{B}_2) = \{x, y^{2p}, y^{p^2}, y^{p^2+1}, z^{p^3}\}$.*

In order to terminate the subduction procedure above we swapped f_2 with $\mathbf{N}_H(z)$. Since in our consideration norm elements appear more natural, it is clear that makes no difference to swap again these two elements.

Theorem 3.2.0.7. *For V a three-dimensional left $\mathbf{F}H$-module, such that $\gamma_i \neq 0, i = 0, \ldots, 4$, the set $\{x, \mathbf{D}, \mathbf{N}_H(y), f_1, \mathbf{N}_H(z)\}$, forms a SAGBI basis for $\mathbf{F}[V]^H$. Furthermore, $\mathbf{F}[V]^H$ is a complete intersection with two relations constructed during the tête-à-tête subductions of $(f_1^p, \mathbf{D}^{\frac{p^2+1}{2}})$ and $(\mathbf{D}^p, \mathbf{N}_G^2(y))$.*

A note on the assumption $\gamma_4 \neq 0$ we imposed earlier may be useful. Although assuming $\gamma_4 = 0$ affects the generating set of $\mathbf{F}[V]^H$, the structural properties remain untouched. Since none of the invariant field generators is affected under this assumption, the equality of fields $\mathbf{F}(V)^H = \mathbf{F}(x, \mathbf{N}_H(y), \mathbf{D})$ still holds. Moreover, $\gamma_4 = 0$ implies that the first tête-à-tête subduction $(\mathbf{D}^p, \mathbf{N}_H^2(y))$ in Lemma 3.2.0.3 becomes

$$\mathbf{D}^p - \gamma_3^p \mathbf{N}_H^2(y) \equiv_{\langle x^{p^2} \rangle} -2\gamma_3^p \gamma_2^{p-1} x^{p^2-1} y^{p^2+1}.$$

Against $\{x, \mathbf{D}, \mathbf{N}_H(y), \mathbf{N}_H(z)\}$, this tête-à-tête cannot subduct more (we always work for $p > 2$) and returns the same lead monomial we had before. Thus for $s_1 := (\mathbf{D}^p - \gamma_3^p \mathbf{N}_H^2(y))/(-2\gamma_3^p \gamma_2^{p-1}) x^{p^2-1}$, the second tête-à-tête subduction $(s_1^p, \mathbf{D}^{\frac{p^2+1}{2}})$ returns an invariant with lead monomial $x^p z^{p^3}$, but with different lead coefficient. Therefore we can attach to our generating set this invariant after dividing by x^p to obtain a SAGBI basis. All the above summarize to the following theorem.

Theorem 3.2.0.8. *Let V denote a three-dimensional $\mathbf{F}H$-module such that $\gamma_i \neq 0$, $i = 1, 2, 3$. Then $\mathbf{F}[V]^H$ is a complete intersection with embedding dimension five and lead term algebra* $\mathrm{LT}(\mathbf{F}[V]^H) = \mathbf{F}[x, y^{2p}, y^{p^2}, y^{p^2+1}, z^{p^3}]$.

3.3 Non-generic cases

The description of the invariant ring $\mathbf{F}[V]^H$ given above works when the coefficients $\gamma_i \neq 0, \forall i = 1, 2, 3$. However, in order to fully understand the three-dimensional invariants we need to investigate each case separately. So we distinguish between the following cases.

3.3.1 Case $c_1, c_2 \in \mathbf{F}_p$

This is the easiest case we have. The homomorphism $\rho : H \hookrightarrow \mathrm{GL}_3(\mathbf{F}_p)$, is an isomorphism onto $\mathrm{UT}_3(\mathbf{F}_p)$. Notice, that $\gamma_1 = \gamma_2 = 0$ implies $\gamma_3, \gamma_4 \neq 0$, since the representation is always assumed to be faithful (i.e. $\gamma_0 \neq 0$).

Observe that the orbit of each variable in that case is $[H : H_x] = 1$, $[H : H_y] = p$, $[H : H_z] = p^2$, hence the product of the group H coincides with the product of their norms.

Corollary 3.3.1.1. *For V a three-dimensional $\mathbf{F}H$-module such that $c_1, c_2 \in \mathbf{F}_p$*

$$\mathbf{F}[V]^H = \mathbf{F}[x, \mathbf{N}_H(y), \mathbf{N}_H(z)].$$

3.3.2 Case $c_1 \in \mathbf{F}_p$, $c_2 \in \mathbf{F}/\mathbf{F}_p$

Throughout this section we assume $c_1 \in \mathbf{F}_p$, $c_2 \in \mathbf{F}/\mathbf{F}_p$. The condition $c_1 \in \mathbf{F}_p$ implies $\gamma_1 = 0$, $\gamma_0 = \gamma_3 = -\gamma_4$. Recall from Lemma 3.2.0.3 that γ_1 occurred in the leading coefficient of the first tête-à-tête subduction, $(\mathbf{D}^p, \mathbf{N}_H^2(y))$. Hence the leading term of this subduction varies. We also recall that we set $\mathscr{B} = \{x, \mathbf{D}, \mathbf{N}_H(y), \mathbf{N}_H(z)\}$.

Lemma 3.3.2.1. *Subducting the tête-à-tête $(\mathbf{D}^p, \mathbf{N}_H^2(y))$ defines an invariant $\widetilde{f_1}$ with lead term: $\gamma_2^p x^{p^2} z^{p^2}$.*

Proof. We work modulo the principal ideal $\langle x^{p^2+1} \rangle \lhd \mathbf{F}[V]$.

Set

$$\widetilde{f_1} := \mathbf{D}^p - \gamma_3^p \mathbf{N}_H^2(y) + 2\frac{\gamma_2^{p-1}\gamma_4}{\gamma_3^{\frac{p+1}{2}}} \cdot x^{p(p-1)}\mathbf{D}.$$

Expanding and reducing modulo $\langle x^{p^2+1}\rangle$ the tête-à-tête difference yields

$$\begin{aligned}\mathbf{D}^p - \gamma_3^p\,\mathbf{N}_H^2(y) &\equiv_{\langle x^{p^2+1}\rangle} -2\,\gamma_2^{p-1}\gamma_4\,x^{p(p-1)}y^{p(p+1)} - 2\,\gamma_3^p\,\gamma_2^{p-1}x^{p^2-1}y^{p^2+1}\\ &+ (c_2^{2p} - c_2^2\gamma_0^{p-1} - \gamma_0^p\gamma_2)^p\,x^{p^2}y^{p^2} + \gamma_2^p x^{p^2}z^{p^2}.\end{aligned}$$

Regarding $x^{p(p-1)}\mathbf{D}$, earlier we calculated

$$\mathbf{D} \equiv_{\langle x^{p+1}\rangle} \gamma_3\,y^{2p} - 2\gamma_0^p x^{p-1}y^{p+1} + (c_2^{2p} - c_2^2\gamma_0^{p-1} - \gamma_0^p\gamma_2)x^p y^p + \gamma_2 x^p z^p,$$

hence multiplying by $2\gamma_2^{p-1}\gamma_4/\gamma_3^{\frac{p+1}{2}} \cdot x^{p(p-1)}$ yields

$$\begin{aligned}2\frac{\gamma_2^{p-1}\gamma_4}{\gamma_3^{\frac{p+1}{2}}}\cdot x^{p(p-1)}\mathbf{D} &\equiv_{\langle x^{p^2+1}\rangle} x^{p(p-1)}y^{p^2+p} - 2\,\frac{\gamma_0^p}{\gamma_3}x^{p^2-1}y^{p^2+1}\\ &+ (c_2^{2p} - c_2^2\gamma_0^{p-1} - \gamma_0^p\gamma_2)^p x^{p^2}y^{p^2} + 2\,\gamma_2\,x^{p^2}y^{p(p-1)}z^p.\end{aligned}$$

Merging up the two parts yields

$$\begin{aligned}\widetilde{f}_1 &\equiv_{\langle x^{p^2+1}\rangle} \gamma_2^p x^{p^2}z^{p^2} + \gamma_2^{p-1}\gamma_4\,x^{p^2}y^{p(p-1)}z^p\\ &+ (c_2^{2p} - c_2^2\gamma_0^{p-1} - \gamma_0^p\gamma_2)^p(1+\gamma_2^{p-1}\gamma_4)\,x^{p^2}y^{p^2}.\end{aligned}$$

Thus $\mathrm{LT}(\widetilde{f}_1) = \gamma_2^p x^{p^2}z^{p^2}$. □

Define $f_1 = x^{-p^2}\widetilde{f}_1$. We claim that the procedure is over. The condition $c_1 \in \mathbf{F}_p$ implies $\mathrm{LT}(\mathbf{N}_H(z)) = z^{p^2}$, hence the norm $\mathbf{N}_H(z)$ can be substituted by f_1. Now in the resulting set $\mathscr{B}_1 := \{x, \mathbf{D}, \mathbf{N}_H(y), f_1\}$ every non-trivial tête-à-tête subducts to zero. Thus $\mathscr{B}_1$ forms a SAGBI basis.

Lemma 3.3.2.2. *For V a three-dimensional left $\mathbf{F}H$-module such that $c_1 \in \mathbf{F}_p, c_2 \in \mathbf{F}/\mathbf{F}_p$, the set $\mathscr{B}_1 = \{x, \mathbf{D}, \mathbf{N}_H(y), f_1\}$ forms a SAGBI basis for $\mathbf{F}[V]^H$. Furthermore, $\mathbf{F}[V]^H$ is a complete intersection with the generating relation coming from the tête-à-tête subduction $(\mathbf{D}^p, \mathbf{N}_H^2(y))$.*

Proof. Let A denote the algebra generated by $\mathscr{B}_1$. Since $\mathrm{LM}(\mathbf{D}) = y^{2p}, \mathrm{LM}(f_1) = z^{p^2}$, from [8, Lemma 2.8.1] and [1, Lemma 2.2.7] follows that $(x, \mathbf{D}, f_1)\mathbf{F}[V]^H$ is zero-dimensional ideal and $\{x, \mathbf{D}, f_1\}$ a homogeneous system of parameters. Hence the extension $A \subset \mathbf{F}[V]^H$ is integral. Furthermore, observe that the field of fraction has not been affected throughout since the minimum degree invariants remain the same, $\mathbf{F}(V)^H = \mathbf{F}(x, \mathbf{D}, \mathbf{N}_H(y))$. Thus $\mathbf{F}[V]^H[x^{-1}] = \mathbf{F}[x, \mathbf{N}_H(y), \mathbf{D}, f_1][x^{-1}]$. So an application of Theorem 1.4.3.10 gives $\mathbf{F}[V]^H = A$. □

Corollary 3.3.2.3. *The lead term algebra of* $\mathbf{F}[V]^H$ *is the* $\mathbf{F}$*-algebra generated by the set* $\mathrm{LT}(\mathscr{B}_1) = \{x, y^{2p}, y^{p^2}, z^{p^2}\}$.

Again, since the norm elements appear more natural in our consideration, we replace f_1 with $\mathbf{N}_H(z)$ to obtain the following equivalent description.

Proposition 3.3.2.4. *Assume V is a three-dimensional left $\mathbf{F}H$-module such that $c_1 \in \mathbf{F}_p, c_2 \in \mathbf{F}/\mathbf{F}_p$. Then $\mathbf{F}[V]^H = \mathbf{F}[x, \mathbf{D}, \mathbf{N}_H(y), \mathbf{N}_H(z)]$ is a hypersurface with lead term algebra $\mathrm{LT}(\mathbf{F}[V]^H) = \mathbf{F}[x, y^{2p}, y^{p^2}, z^{p^2}]$.*

3.3.3 Case $c_1 \in \mathbf{F}/\mathbf{F}_p$, $c_2 \in \mathbf{F}_p$

In that case $\gamma_2 = 0$. However, $\gamma_3, \gamma_4 \neq 0$, since otherwise $\gamma_0 = 0$. This assumption changes the whole setup. For example $\mathbf{D}$ is no longer the same as

$$\mathbf{D} = c^p \mathbf{N}_{g_1}^2(y) + ({c_2}^{2p} - {c_2}^2 \gamma_0^{p-1}) x^p \mathbf{N}_{g_1}(y),$$

while the H_1-norm of y becomes an H-invariant, $\mathbf{N}_H(y) = y^p - x^{p-1}y$. Recall from equation (3.2.4) the equality $\mathbf{F}[V]^H[x^{-1}] = \mathbf{F}[x, \mathbf{N}_{g_1}(y), \mathbf{N}_h(\delta)]^{\langle g_2 \rangle}[x^{-1}]$. By shifting the right-hand side generators to degree one $y_1 = \mathbf{N}_{g_1}(y)/x^{p-1}, y_2 = \mathbf{N}_h(\delta)/x^{2p-1}$, we obtain a new three-dimensional representation of H and an equality $\mathbf{F}[V]^H[x^{-1}] = \mathbf{F}[x, y_1, y_2]^{\langle g_2 \rangle}[x^{-1}]$. On this new basis $\{x, y_1, y_2\}$ we compute

$$x \cdot g_2 = x,\ y_1 \cdot g_2 = y_1,\ y_2 \cdot g_2 = y_2 + 2\gamma_0^p y_1 + (c_2^{2p} - c_2^2 \gamma_0^{p-1})x.$$

So the new representation of $\langle g_2 \rangle$ has the following form

$$\widehat{\rho} : \langle g_2 \rangle \rightarrow,\ g_2 \mapsto \begin{bmatrix} 1 & 2\gamma_0^p & c_2^{2p} - c_2^2\gamma_0^{p-1} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

and the action is Nakajima. Therefore

$$\mathbf{F}[x, y_1, y_2]^{\langle g_2 \rangle} = \mathbf{F}[x, y_1, \mathbf{N}_{g_2}(y_2)],$$

with $\mathbf{N}_{g_2}(y_2) = \frac{1}{2\gamma_0^{p^2}}(y_2^p - y_2\Delta_2(y_2)^{p-1})$. Set for simplicity $\widehat{\mathbf{N}}_{g_2}(y_2) := 2\gamma_0^{p^2}\mathbf{N}_{g_2}(y_2)$ and notice that the equality $\mathbf{F}[x, y_1, y_2]^{\langle g_2 \rangle} = \mathbf{F}[x, y_1, \widehat{\mathbf{N}}_{g_2}(y_2)]$ yields after clearing out the denominators minimally

$$\mathbf{F}[V]^H[x^{-1}] = \mathbf{F}[x, \mathbf{N}_H(y), \mathbf{N}_H(\delta) = \mathbf{N}_h^p(\delta) - \mathbf{N}_h(\delta)\Delta_2(\mathbf{N}_h(\delta))^{p-1}][x^{-1}]. \quad (3.3.1)$$

Notice that by construction $\{x, \mathbf{N}_H(y), \mathbf{N}_H(\delta)\}$ is a set of minimum degree H-invariants. Concerning the new minimum z-degree invariant $\mathbf{N}_H(\delta)$, expanding the definition shows that $\deg_z(\mathbf{N}_H(\delta)) = p^2$, $\mathrm{LT}(\mathbf{N}_H(\delta)) = y^{2p^2}$ and the second term in order is $-\gamma_3^{p-1}x^{p^2-p}y^{p^2+p}$. Also a routine computation returns

$$\Delta_2(\mathbf{N}_H(\delta)) = 2\gamma_3 x^p y^p - 2c_2\gamma_0^{p-1}x^{2p-1}y + 2c_1\gamma_0^{p-1}x^{2(p-1)}yz + c_2^2(1-\gamma_0^{p-1})x^{2p}.$$

Finally, we attach the norm $\mathbf{N}_H(z)$ and denote $\mathscr{B} := \{x, \mathbf{N}_H(y), \mathbf{N}_H(\delta), \mathbf{N}_H(z)\}$. In $\mathscr{B}$ there is a unique non-trivial tête-à-tête: $(\mathbf{N}_H(\delta), \mathbf{N}_H^{2p}(y))$.

Lemma 3.3.3.1. *Subducting the tête-à-tête* $(\mathbf{N}_H(\delta), \mathbf{N}_H^{2p}(y))$ *defines an invariant with lead term:* $2y^{p^2+1}x^{p^2-1}$.

Proof. We work modulo the ideal $\langle x^{p^2-p+1}\rangle \triangleleft \mathbf{F}[V]$.

Follows easily that $\mathbf{N}_H^{2p}(y) \equiv_{\langle x^{p^2-p+1}\rangle} y^{2p^2} - 2x^{p^2-p}y^{p^2+p}$. Moreover, reducing $\mathbf{N}_H(\delta)$ modulo $\langle x^{p^2-p+1}\rangle$ gives: $\mathbf{N}_H(\delta) \equiv_{\langle x^{p^2-p+1}\rangle} y^{2p^2} - \gamma_3^{p-1}x^{p^2-p}y^{p^2+p}$. Summing up the two parts yields

$$\mathbf{N}_H(\delta) - \mathbf{N}_H^{2p}(y) \equiv_{\langle x^{p^2-p+1}\rangle} (2-\gamma_3^{p-1})x^{p^2-p}y^{p^2+1}.$$

Set

$$\widetilde{h}_1 := \mathbf{N}_H(\delta) - \mathbf{N}_H^{2p}(y) - (2-\gamma_3^{p-1})\mathbf{N}_H^{p+1}(y)x^{p^2-p}.$$

We work modulo the ideal in $\mathbf{F}[V]$ generated by x^{p^2+1} and yx^{p^2}. We investigate each part separately.

Expanding the definition of $\mathbf{N}_H(\delta)$ and $\mathbf{N}_H^{2p}(y)$, gives after reducing modulo $\langle x^{p^2+1}, yx^{p^2}\rangle$,

$$\begin{aligned}\mathbf{N}_H(\delta) &\equiv_{\langle x^{p^2+1},yx^{p^2}\rangle} \; y^{2p^2} - \gamma_3^{p-1}x^{p^2-p}y^{p^2+p} + c_2\gamma_0^{p-1}\gamma_3^{p-2}x^{p^2-1}y^{p^2+1} - x^{p^2}z^{p^2}\\ \mathbf{N}_H^{2p}(y) &\equiv_{\langle x^{p^2+1},yx^{p^2}\rangle} \; y^{2p^2} - 2x^{p(p-1)}y^{p^2+p}.\end{aligned}$$

Concerning $\mathbf{N}_H^{p+1}(y)x^{p^2-p}$, after expanding the definition and reducing modulo $\langle x^{p^2+1}, yx^{p^2}\rangle$:

$$\mathbf{N}_H^{p+1}(y)x^{p^2-p} \equiv_{\langle x^{p^2+1},yx^{p^2}\rangle} x^{p^2-p}y^{p^2+p} - x^{p^2-1}y^{p^2+1}.$$

Merging up the two parts yields

$$\widetilde{h}_1 \equiv_{\langle x^{p^2+1},yx^{p^2}\rangle} (c_2\gamma_0^{p-1}\gamma_3^{p-2} - \gamma_3^{p-1} + 2)y^{p^2+1}x^{p^2-1} - x^{p^2}z^{p^2}.$$

□

Set $h_1 := 1/(c_2\gamma_0^{p-1}\gamma_3^{p-2} - \gamma_3^{p-1} + 2) \cdot x^{-(p^2-1)}\widetilde{h}_1$ and $\mathscr{B}_1 := \mathscr{B} \cup \{h_1\}$. In $\mathscr{B}_1$ there is a unique non-trivial tête-à-tête : $(h_1^p, \mathbf{N}_H^{p^2+1}(y))$.

Lemma 3.3.3.2. *Subducting the tête-à-tête $(h_1^p, \mathbf{N}_H^{p^2+1}(y))$, defines an invariant with lead monomial: $x^p z^{p^3}$*

Proof. First off we find the lead term of the tête-à-tête difference. We work modulo $\langle x^p\rangle \triangleleft \mathbf{F}[V]$. For $\mathbf{N}_H^{p^2+1}(y)$ expanding and reducing modulo $\langle x^p\rangle$ gives

$$\mathbf{N}_H^{p^2+1}(y) \equiv_{\langle x^p\rangle} y^{p^3+p} - x^{p-1}y^{p^3+1}.$$

Regarding h_1^p, from the previous lemma $\mathrm{LT}(\widetilde{h}_1) = (c_2\gamma_0^{p-1}\gamma_3^{p-2} - \gamma_3^{p-1} + 2)\cdot x^{p^2-1}y^{p^2+1}$ and we divided through by x^{p^2-1} to obtain h_1. So in h_1 every term but the leading contain an x-power. Thus $h_1^p \equiv_{\langle x^p\rangle} y^{p^3+p}$ and all together gives

$$h_1^p - \mathbf{N}_H^{p^2+1}(y) \equiv_{\langle x^p\rangle} x^{p-1}y^{p^3+1}.$$

Set for the next step of the subduction

$$\widetilde{h}_2 := h_1^p - \mathbf{N}_H^{p^2+1}(y) - x^{p-1}\, h_1\, \mathbf{N}_H^{p^2-p}(y).$$

Now we work modulo $\langle x^{p+1}\rangle \lhd \mathbf{F}[V]$. For h_1^p, expanding and reducing modulo $\langle x^{p+1}\rangle$ gives: $h_1^p \equiv_{\langle x^{p+1}\rangle} y^{p^3+p} - 1/(c_2^p\gamma_0^{p(p-1)}\gamma_3^{p(p-2)} - \gamma_3^{p(p-1)} + 2)\cdot x^p z^{p^3}$. Also follows easily that $\mathbf{N}_H(y) \equiv_{\langle x^{p+1}\rangle} y^{p^3+p} - x^{p-1}y^{p^3+1}$.

For $x^{p-1}\, h_1\, \mathbf{N}_H^{p(p-1)}(y)$, we know that in h_1 every term but the leading contain an x-power. In the product $x^{p-1}\mathbf{N}_H^{p(p-1)}(y)$ it is not difficult to see that no other term except the leading remains in the quotient ring. Thus all together

$$x^{p-1}h_1\mathbf{N}_H^{p(p-1)}(y) \equiv_{\langle x^{p+1}\rangle} x^{p-1}y^{p^3+1}.$$

Adding up every the two parts gives

$$\widetilde{h}_2 \equiv_{\langle x^{p+1}\rangle} x^p z^{p^3}/(c_2^p\gamma_0^{p(p-1)}\gamma_3^{p(p-2)} - \gamma_3^{p(p-1)} + 2).$$

□

Denote $h_2 := x^{-p}\widetilde{h}_2$ and $\mathscr{B}_2 := \mathscr{B}_1 \cup \{h_2\}$. Since the resulting subduction has the same lead term with $\mathbf{N}_H(z)$, as previously suffices to swap $\mathbf{N}_H(z)$ with h_2. Now in the resulting set every non-trivial tête-à-tête subducts to zero.

Lemma 3.3.3.3. *Let V denote a three-dimensional $\mathbf{F}H$-module such that $c_1 \in \mathbf{F}/\mathbf{F}_p, c_2 \in \mathbf{F}_p$. Then the set $\{x, \mathbf{N}_H(y), h_1, h_2\}$ forms a SAGBI basis for $\mathbf{F}[V]^H$. Furthermore, $\mathbf{F}[V]^H$ is a hypersurface with the unique relation coming from the subduction of $(h_1^p, \mathbf{N}_H^{p+1}(y))$.*

Proof. We have proven already that $\mathscr{B}_2$ is a SAGBI basis. Let A denote the algebra it generates. Since $\mathrm{LM}(\mathbf{N}_H(y))$ and $\mathrm{LM}(h_2) = z^{p^3}$, follows that $(x, \mathbf{N}_H(y), h_2)\mathbf{F}[V]^H$ is a zero-dimensional ideal and $\{x, \mathbf{N}_H(y), h_2\}$ a homogeneous system of parameters. Hence $A \subset \mathbf{F}[V]^H$ is integral. The invariant field $\mathbf{F}(V)^H = \mathbf{F}(x, \mathbf{N}_H(y), h_1)$ implies $\mathbf{F}[V]^H[x^{-1}] = A[x^{-1}]$. So the equality $\mathbf{F}[V]^H = A$ follows from an application of Theorem 1.4.3.10. □

Corollary 3.3.3.4. *The lead term algebra of $\mathbf{F}[V]^H$ is the $\mathbf{F}$-algebra generated by the set $\mathrm{LT}(\mathscr{B}_2) = \{x, y^p, y^{p^2+1}, z^{p^3}\}$.*

As previously we swap again f_2 and $\mathbf{N}_H(z)$.

Proposition 3.3.3.5. *Assume V is a three-dimensional $\mathbf{F}H$-module such that $c_1 \in \mathbf{F}/\mathbf{F}_p, c_2 \in \mathbf{F}_p$. Then $\mathbf{F}[V]^H = \mathbf{F}[x, \mathbf{N}_H(y), h_1, \mathbf{N}_H(z)]$ is a hypersurface with lead term algebra $\mathrm{LT}(\mathbf{F}[V]^H) = \mathbf{F}[x, y^p, y^{p^2+1}, z^{p^3}]$.*

3.3.4 Case $c_1 \in \mathbf{F}/\mathbf{F}_p$, $c_2 \in \mathbf{F}/\mathbf{F}_p$

In this case $\gamma_1, \gamma_2 \neq 0$. Also γ_3 and γ_4 cannot be zero simultaneously since implies $c_1 \in \mathbf{F}_p$. Furthermore, we have seen that the assumption $\gamma_4 = 0$ is not essential and yields invariant ring similar to the generic case. So we have to examine only the case $\gamma_3 = 0$.

We check how much this assumption affects our setup. Observe that the lead term of $\mathbf{D}$ changes. Expanding this time gives: $\mathrm{LT}(\mathbf{D}) = -2\gamma_0^p x^{p-1} y^{p+1}$. Denote $\widehat{\mathbf{D}} := x^{-(p-1)}\mathbf{D}$ for this invariant after we divided by the superfluous x-power.

Remark 3.3.4.1. *Since on the first two variables the action is Nakajima, $\{x, \mathbf{N}_H(y)\}$ is a set of minimum degree invariants. The constraint $\gamma_3 = 0$ does not affect the invariant field $\mathbf{F}(V)^{H_2} = \mathbf{F}(x, \mathbf{N}_{g_1}(y), \mathbf{N}_h(\delta))$, hence the inclusion $\mathbf{F}(V)^H \subset \mathbf{F}(V)^{H_2}$ implies that the minimum z-degree invariant of $\mathbf{F}[V]^H$ has z-degree at least p. Since $\deg_z(\widehat{\mathbf{D}}) = p$, follows that $\mathbf{F}(V)^H = \mathbf{F}(x, \widehat{\mathbf{D}}, \mathbf{N}_H(y))$.*

Define $\mathscr{B} := \{x, \widehat{\mathbf{D}}, \mathbf{N}_H(y), \mathbf{N}_H(z)\}$. Then there is a unique non-trivial tête-à-tête: $(\widehat{\mathbf{D}}^{p^2}, \mathbf{N}_H^{p+1}(y))$. Before we proceed we make a note that will be used below. Expanding the definition of $\mathbf{N}_H^{p+1}(y)$ and reducing modulo x^{p^2} gives

$$\begin{aligned}\mathbf{N}_H^{p+1}(y) &= \mathbf{N}_{g_1}^{p^2+p}(y) - \gamma_2^{p-1} x^{p(p-1)} \mathbf{N}_{g_1}^{p^2+1}(y) - \gamma_2^{p(p-1)} x^{p^2(p-1)} \mathbf{N}_{g_1}^{2p}(y) + \gamma_2^{p^2-1} x^{(p^2+p)(p-1)} \mathbf{N}_{g_1}^{p+1}(y) \\ &\equiv_{\langle x^{p^2}\rangle} -2(\gamma_0^{p^3} + \gamma_0^{p^3+p^2-p}) x^{p(p-1)} y^{p^3+p} + \gamma_2^{p-1} x^{p^2-1} y^{p^3+1}.\end{aligned}$$

We shall use this computation in the following lemma.

Lemma 3.3.4.2. *Subducting the tête-à-tête $(\widehat{\mathbf{D}}^{p^2}, \mathbf{N}_H^{p+1}(y))$, defines an invariant with lead monomial: $\gamma_0^{p^3} x^{p^2} z^{p^3}$.*

Proof. We work modulo $\langle x^{p^2-1}\rangle \lhd \mathbf{F}[V]$. Clearly $\widehat{\mathbf{D}}^{p^2} \equiv_{\langle x^{p^2-1}\rangle} -2\,\gamma_0^{p^3} y^{p^2(p+1)}$, since every term but the leading in $\widehat{\mathbf{D}}$ contains a positive x-power.

Concerning $\mathbf{N}_H^{p+1}(y)$, expanding and reducing modulo x^{p^2-1} gives

$$\mathbf{N}_H^{p+1}(y) \equiv_{\langle x^{p^2}-1\rangle} y^{p^2(p+1)} - (1+\gamma_2^{p-1})x^{p(p-1)}y^{p^3+p}. \tag{3.3.2}$$

Adding up the two parts yields

$$\widehat{\mathbf{D}}^{p^2} + 2\,\gamma_0^{p^3}\,\mathbf{N}_H^{p+1}(y) \equiv_{\langle x^{p^2-1}\rangle} -2(\gamma_0^{p^3} + \gamma_0^{p^3+p^2-p})x^{p(p-1)}y^{p^3+p}.$$

Set

$$\widetilde{t}_1 := \widehat{\mathbf{D}}^{p^2} + 2\,\gamma_0^{p^3}\,\mathbf{N}_H^{p+1}(y) - \frac{(\gamma_0^{p^3} + \gamma_0^{p^3+p^2-p})}{\gamma_0^{p^2}}\,x^{p(p-1)}\,\widehat{\mathbf{D}}^p\,\mathbf{N}_H^{p-1}(y).$$

We work modulo $\langle x^{p^2}\rangle \lhd \mathbf{F}[V]$. Expanding $\widehat{\mathbf{D}}^p$ and reducing modulo $\langle x^{p^2}\rangle$ yields

$$\begin{aligned}\widehat{\mathbf{D}}^p \;&\equiv_{\langle x^{p^2}\rangle}\; -2\,\gamma_0^{p^2}y^{p(p+1)} + \gamma_0^{p^2}x^{p(p-1)}y^{2p} + ((c_2{}^{2p} - c_2{}^2\gamma_0^{p-1})^p - \gamma_0^{2p^2})^p x^p y^{p^2}\\ &- \quad \gamma_0^{p^2}x^p z^{p^2} - \gamma_0^{2p^2-p}x^{p(p-1)}y^{2p}\,.\end{aligned}$$

For $x^{p(p-1)}\,\mathbf{N}_H^{p-1}(y)$, the binomial theorem acquires

$$\begin{aligned}x^{p(p-1)}\mathbf{N}_H^{p-1}(y) \;&=\; x^{p(p-1)}\sum_{i=0}^{p-1}\binom{p-1}{i}(\mathbf{N}_{g_1}^p(y))^{p-1-i}(-\gamma_2^{p-1}x^{p(p-1)})^i\mathbf{N}_{g_1}^i(y)\\ &=\; \sum_{i=0}^{p-1}(-1)^i\binom{p-1}{i}\gamma_2^{i(p-1)}\mathbf{N}_{g_1}(y)^{(p-1)(p-i)}x^{p(p-1)(i+1)}.\end{aligned}$$

Thus, $x^{p(p-1)}\,\mathbf{N}_H^{p-1}(y) \equiv_{\langle x^{p^2}\rangle} x^{p(p-1)}y^{p^2(p-1)}$. For the tête-à-tête $(\widehat{\mathbf{D}}^{p^2}, \mathbf{N}_H^{p+1}(y))$, the comments above give

$$\widehat{\mathbf{D}}^{p^2} + 2\gamma_0^{p^3}\mathbf{N}_H^{p+1}(y) \equiv_{\langle x^{p^2}\rangle} -2(\gamma_0^{p^3} + \gamma_0^{p^3+p^2-p})x^{p(p-1)}y^{p^3+p} + 2\gamma_0^{p^3}\gamma_2^{p-1}x^{p^2-1}y^{p^3+1}.$$

All together gives

$$\widetilde{t}_1 \equiv_{\langle x^{p^2}\rangle} 2\gamma_0^{p^3}\gamma_2^{p-1}x^{p^2-1}y^{p^3+1}.$$

However we are not finished yet. Notice that $\widetilde{t}_1$ can be subducted further against $\mathscr{B}$. Set

$$t_1 := \widetilde{t}_1 + \gamma_0^{p^3-p}\gamma_2^{p-1}\,x^{p^2-1}\widehat{\mathbf{D}}^{p^2-p+1}.$$

This time we work modulo $\langle x^{p^2+1}\rangle \lhd \mathbf{F}[V]$. In $\mathbf{D}^{p^2-p+1}$ every term but the leading contains an x-power strictly greater than two, so

$$x^{p^2-1}\mathbf{D}^{p^2-p+1} \equiv_{\langle x^{p^2+1}\rangle} -2\gamma_2^{p-1}x^{p^2-1}y^{p^3+1}.$$

From the above analysis after expanding $\widetilde{t}_1$ and reducing modulo x^{p^2+1} yields

$$\widetilde{t}_1 \equiv_{\langle x^{p^2+1}\rangle} 2\gamma_0^{p^3}\gamma_2^{p-1}x^{p^2-1}y^{p^3+1} + \gamma_0^{p^3}x^{p^2}z^{p^3} + (c_2^{2p} - c_2^2\gamma_0^{p-1} - \gamma_0^{2p})^{p^2}x^{p^2}y^{p^3}.$$

Furthermore, $x^{p(p-1)}\,\widehat{\mathbf{D}}^p\,\mathbf{N}_H^{p-1}(y) \equiv_{\langle x^{p^2+1}\rangle} -2\,\gamma_0^{p^2}\,x^{p(p-1)}y^{p^3+p}$ and

$$\widehat{\mathbf{D}}^{p^2}+2\,\gamma_0^{p^3}\,\mathbf{N}_H^{p+1}(y) \equiv_{\langle x^{p^2+1}\rangle} -2(\gamma_0^{p^3}+\gamma_0^{p^3+p^2-p})x^{p(p-1)}y^{p^3+p}+\gamma_0^{p^3}x^{p^2}z^{p^3}+(c_2^{2p}-c_2^2\gamma_0^{p-1}-\gamma_0^{2p})^{p^2}x^{p^2}y^{p^3}.$$

All together gives

$$t_1 := \widehat{\mathbf{D}}^{p^2} + 2\,\gamma_0^{p^3}\,\mathbf{N}_H^{p+1}(y) - \frac{(\gamma_0^{p^3} + \gamma_0^{p^3+p^2-p})}{\gamma_0^{p^2}}\,x^{p(p-1)}\,\widehat{\mathbf{D}}^p\,\mathbf{N}_H^{p-1}(y) + \gamma_0^{p^3-p}\gamma_2^{p-1}x^{p^2-1}\widehat{\mathbf{D}}^{p^2-p+1}$$

$$\equiv_{\langle x^{p^2+1}\rangle}$$

$$\gamma_0^{p^3}x^{p^2}z^{p^3} + (c_2^{2p} - c_2^2\gamma_0^{p-1} - \gamma_0^{2p})^{p^2}x^{p^2}y^{p^3},$$

so we have $\mathrm{LT}(t_1) = \gamma_0^{p^3}x^{p^2}z^{p^3}$ as asserted. □

Denote $w_1 := x^{-p^2}t_1$, $\mathscr{B}_1 := \mathscr{B} \cup \{w_1\}$. Now in $\mathscr{B}_1$ every non-trivial tête-à-tête subducts to zero.

Lemma 3.3.4.3. *For V a three-dimensional $\mathbf{F}H$-module such that $c_1, c_2 \in \mathbf{F}/\mathbf{F}_p$, $\gamma_3 = 0$, $\mathscr{B}_1$ forms a SAGBI basis for $\mathbf{F}[V]^H$. Furthermore, there is a single relation constructed during the tête-à-tête subduction of $(\widehat{\mathbf{D}}^{p^2}, \mathbf{N}_H^{p+1}(y))$.*

Proof. Let A denote the algebra generated by $\mathscr{B}_1$. We have already proven that $\mathscr{B}_1$ forms a SAGBI basis for A. Furthermore, from [8, Lemma 2.6.3] and [1, Lemma 2.2.7] follows that $(x, \widehat{\mathbf{D}}, w_1)\mathbf{F}[V]^H$ is zero-dimensional and $\{x, \widehat{\mathbf{D}}, w_1\}$ a homogeneous system of parameters. Hence the extension $A \subset \mathbf{F}[V]^H$ is integral. Remark 3.3.4.1 implies that the field of fraction has not been affected, thus $\mathbf{F}[V]^H[x^{-1}] = A[x^{-1}]$. Therefore, the equality $A = \mathbf{F}[V]^H$ follows from an application of Theorem 1.4.3.10. □

Corollary 3.3.4.4. *The lead term algebra of $\mathbf{F}[V]^H$ is the $\mathbf{F}$-algebra generated by the set $\mathrm{LT}(\mathscr{B}_2) = \{x, y^{p+1}, y^{p^2}, z^{p^3}\}$.*

As always we prefer the norm elements to generate our invariant ring when this is feasible.

Proposition 3.3.4.5. *Assume V is a three-dimensional $\mathbf{F}H$-module such that $c_1, c_2 \in \mathbf{F}/\mathbf{F}_p$, $\gamma_3 = 0$. Then $\mathbf{F}[V]^H = \mathbf{F}[x, \widehat{\mathbf{D}}, \mathbf{N}_H(y), \mathbf{N}_H(z)]$ is a hypersurface with lead term algebra* $\mathrm{LT}(\mathbf{F}[V]^H) = \mathbf{F}[x, y^{p+1}, y^{p^2}, z^{p^3}]$.

Chapter 4

Four-dimensional case

4.1 Invariants of type-(1,1,1,1) representations.

4.1.1 Setup

Let V denote a four-dimensional left $\mathbf{F}H$-module of socle type-$(1,1,1,1)$. In what follows we investigate the structure of the invariant ring $\mathbf{F}[V]^H$ and compute the invariant field $\mathbf{F}(V)^H$. We prove that $\mathbf{F}[V]^H$ is not Cohen-Macaulay and for $p=5$ the existence of a partial hsop which fails to be regular sequence.

Recall from Theorem 2.2.0.5 the existence of a basis $\mathscr{B}$ consistent with the socle series, such that the group of representing matrices is generated by

$$g_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \; g_2 = \begin{bmatrix} 1 & c_{1,2} & c_{1,3} & 0 \\ 0 & 1 & c_{1,2} & c_{2,4} \\ 0 & 0 & 1 & c_{1,2} \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

subject to the constraint $c_{2,4} - c_{1,3} \neq 0$, with commutator

$$c = [g_1, g_2] = \begin{bmatrix} 1 & 0 & 0 & c_{2,4} - c_{1,3} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

We denote this group by $\rho_{\mathscr{B}}(H)$.

Lemma 4.1.1.1. *The group $\rho_{\mathscr{B}}(H)$ is not a bireflection group.*

Proof. The superdiagonal entries of a matrix $g_1^m g_2^n$ coincide and they are all equal to $mc_{1,2} + n$. Pick $M = g_1^{m_1} g_2^{n_1} ... g_1^{m_k} g_2^{n_k} \in \rho_{\mathscr{B}}(H)$ an arbitrary element. Then the superdiagonal entries of M coincide too, and equal the sum of the superdiagonal entries of each pair $g_1^{m_j} g_2^{n_j}$. So it follows that if another generating set for $\rho_{\mathscr{B}}(H)$ consisting of bireflections was chosen, then the generators must all have zero superdiagonal entries. The last is a contradiction since the fixed point space is two-dimensional and we drop into a different representation type. □

From [12] we know that when an invariant ring is Cohen-Macaulay, then the group of representing matrices is a generated by bireflections. Therefore, as a consequence of the lemma we see that $\mathbf{F}[V]^H$ fails to be Cohen-Macaulay.

Remark 4.1.1.2. *In what follows we always work with $p > 3$. Observe, that if $p = 3$ then $J_4^p \neq I_4$ and J_4 has order nine.*

Before we investigate the structure of $\mathbf{F}[V]^H$ we compute the invariant field $\mathbf{F}(V)^H$.

4.1.2 The invariant field $\mathbf{F}(V)^H$

Think of the following series

$$\{e\} \lhd H_1 \lhd H_2 \lhd H,$$

where $H_1 = \langle g_1 \rangle \cong C_p$, $H_2 = \langle g_1, c \rangle \cong C_p \times C_p$. From Theorem 1.4.2.6 we know that in order to compute $\mathbf{F}(V)^H$ we need to find the invariants of minimum degree at each variable.

We start by computing $\mathbf{F}(V)^{H_1}$. Let V_4 denote the four-dimensional indecomposable representation of H_1. Since g_1 acts as the maximal four-dimensional Jordan normal form, as $\mathbf{F}H_1$-module $V = V_4$. Therefore, $\mathbf{F}(V)^{H_1} = \mathbf{F}(V_4)^{C_p}$. Using [22, Theorem 4.1] gives a SAGBI basis for $\mathbf{F}[V_4]^{C_p}$ and the minimum degree x_i-invariants of that basis is a generating set for $\mathbf{F}(V)^{H_1}$. To describe these invariants, first we need to recall a notion defined in [22].

Definition 4.1.2.1. *Let $\beta \in \mathbf{F}[x_1, ..., x_k]$ denote an arbitrary monomial. We call β **admissible** if it is the lead monomial of a C_p-invariant in some polynomial algebra $\mathbf{F}[x_1, ..., x_n]$. We denote the corresponding C_p-invariant by* $\mathrm{inv}(\beta)$.

For convenience we set always $\mathrm{inv}(x_1^i) = x_1^i$. The following theorem implies that every monomial can be used to construct an admissible monomial for sufficiently large n.

Theorem 4.1.2.2. *Assume that β is a monomial in $\mathbf{F}[x_1, ..., x_{m-1}]$. Then for a positive integer $i \geq 2$, the monomial $\beta x_m^i \in \mathbf{F}[x_1, ..., x_{m-1}][x_m]$ is the lead monomial of a C_p-invariant in some polynomial algebra $\mathbf{F}[x_1, ..., x_n]$ for sufficiently large n.*

Proof. For a proof, see, [22, Theorem 2.3]. □

We use this theorem to present two examples of invariants arising from admissible monomials that we will need in this section. We follow the same notation.

Example 4.1.2.3. *Assume that $\beta = 1$, $i = 2, m = 2$ and $C_p = \langle g \rangle$. Then from the previous theorem we know that for sufficiently large $n > 0$ the monomial x_2^2 is the lead term of a C_p-invariant. Think of the polynomial $f_1 = x_2^2 - 2x_1x_3$. Applying the twisted derivation $\Delta = g - 1 \in \mathbf{F}C_p$ on f_1 yields $\Delta(f_1) = x_1^2$. Since $g(x_2x_1) = x_1^2$, define $f_2 = f_1 - x_1 x_2 = x_2^2 - 2x_1x_3 - x_1x_2$. Applying Δ this time returns zero,*

$\Delta(f_2) = 0$. *Therefore* f_2 *is a* C_p*-invariant and* $\operatorname{inv}(x_2^2) = f_2$. *Notice that this is the integral invariant from the three-dimensional case.*

Example 4.1.2.4. *Similarly someone can think the case* $\beta = 1$, $i = 3, m = 2$ *and construct* $\operatorname{inv}(x_2^3)$. *Following the same idea yields the* C_p*-invariant* $\operatorname{inv}(x_2^3) = x_2^3 + x_1^2(3x_4 - x_2) - 3x_1x_2x_3$.

Now we are able to describe the generating set of the invariant field $\mathbf{F}(V)^{H_1}$.

Proposition 4.1.2.5. *Let* V_4 *denote the four-dimensional indecomposable representation of* $C_p = \langle g_1 \rangle$. *Then* $\mathbf{F}(V_4)^{C_p} = \mathbf{F}(x_1, \mathbf{N}_{g_1}(x_2), \operatorname{inv}(x_2^2), \operatorname{inv}(x_2^3))$. *Furthermore, we obtain an equality of localized rings*

$$\mathbf{F}[V_4]^{C_p}[x_1^{-1}] = \mathbf{F}[x_1, \mathbf{N}_{g_1}(x_2), \operatorname{inv}(x_2^2), \operatorname{inv}(x_2^3)][x_1^{-1}].$$

Proof. Let $\{x_1, \mathbf{N}_{g_1}(x_2), \operatorname{inv}(x_2^2), \operatorname{inv}(x_2^3)\}$ be a subset of the SAGBI basis elements of $\mathbf{F}[V_4]^{C_p}$ as described in [22, Theorem 4.1]. From the previous examples we have

$$\operatorname{inv}(x_2^2) = x_2^2 - 2x_1x_3 - x_1x_2, \operatorname{inv}(x_2^3) = x_2^3 + x_1^2(3x_4 - x_2) - 3x_1x_2x_3,$$

so they are of degree one in x_3 and x_4 respectively. Also x_1 and $\mathbf{N}_{g_1}(x_2)$ are of minimum degree, since C_p acts on the first two variables as Nakajima group. Therefore, $\mathbf{F}(V_4)^{C_p} = \mathbf{F}(x_1, \mathbf{N}_{g_1}(x_2), \operatorname{inv}(x_2^2), \operatorname{inv}(x_2^3))$. Finally, since $\operatorname{LC}_{x_4}(\operatorname{inv}(x_2^3)) = x_1^2$ the equality of localized rings follows from Theorem 1.4.2.6. □

Using the equality $\mathbf{F}[V]^{H_1}[x_1^{-1}] = \mathbf{F}[x_1, \mathbf{N}_{g_1}(x_2), \operatorname{inv}(x_2^2), \operatorname{inv}(x_2^3)][x_1^{-1}]$ and applying the $H_2/H_1 \cong \langle c \rangle$-action yields

$$\mathbf{F}[V]^{H_2}[x_1^{-1}] = \mathbf{F}[x_1, \mathbf{N}_{g_1}(x_2), \operatorname{inv}(x_2^2), \operatorname{inv}(x_2^3)]^{\langle c \rangle}[x_1^{-1}].$$

Thus we need to describe $\mathbf{F}[x_1, \mathbf{N}_{g_1}(x_2), \operatorname{inv}(x_2^2), \operatorname{inv}(x_2^3)]^{\langle c \rangle}$. To this end, we shift the generators of the last algebra to degree one:

$$\begin{aligned}
\mathbf{F}[V]^{H_2}[x_1^{-1}] &= \mathbf{F}[x_1, \mathbf{N}_{g_1}(x_2), \operatorname{inv}(x_2^2), \operatorname{inv}(x_2^3)]^{\langle c \rangle}[x_1^{-1}] \\
&= \mathbf{F}[x_1, \frac{\mathbf{N}_{g_1}(x_2)}{x_1^{p-1}}, \frac{\operatorname{inv}(x_2^2)}{x_1}, \frac{\operatorname{inv}(x_2^3)}{x_1^2}]^{\langle c \rangle}[x_1^{-1}] \\
&= \mathbf{F}[x_1, y_1, y_2, y_3]^{\langle c \rangle}[x_1^{-1}],
\end{aligned}$$

where $y_1 := \mathbf{N}_{g_1}(x_2)/x_1^{p-1}, y_2 := \mathrm{inv}(x_2^2)/x_1$ and $y_3 := \mathrm{inv}(x_2^3)/x_1^2$.

Since we changed the basis, we have created a new representation for $\langle c\rangle$. Denote this representation by ρ_c. Then ρ_c is fully determined by the action of c on this new basis $\{x_1, y_1, y_2, y_3\}$. Follows easily that

$$\begin{aligned} x_1 \cdot c = x_1, &\quad y_1 \cdot c = y_1, \\ y_2 \cdot c = y_2, &\quad y_3 \cdot c = y_3 + 3(c_{2,4} - c_{1,3})x_1, \end{aligned}$$

therefore,

$$c \mapsto \rho_c(c) = \begin{bmatrix} 1 & 0 & 0 & 3(c_{2,4} - c_{1,3}) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The last implies that $\langle c\rangle$ acts on the new basis as Nakajima group, hence the invariant ring $\mathbf{F}[x_1, y_1, y_2, y_3]^{\langle c\rangle}$ has a well-known description

$$\mathbf{F}[x_1, y_1, y_2, y_3]^{\langle c\rangle} = \mathbf{F}[x_1, y_1, y_2, \mathbf{N}_c(y_3)],$$

with $\mathbf{N}_c(y_3) = y_3^p - (c_{2,4} - c_{1,3})^{p-1} x_1^{p-1} y_3$. After clearing the denominators minimally we obtain

$$\mathbf{F}[V]^{H_2}[x_1^{-1}] = \mathbf{F}[x_1, \mathbf{N}_{g_1}(x_2), \mathrm{inv}(x_2^2), \mathbf{N}_c(\mathrm{inv}(x_2^3))][x_1^{-1}], \tag{4.1.1}$$

where $\mathbf{N}_c(\mathrm{inv}(x_2^3)) = \mathrm{inv}(x_2^3)^p - (c_{2,4} - c_{1,3})^{p-1}\, x_1^{3(p-1)}\, \mathrm{inv}(x_2^3)$, is of minimum x_4-degree.

Now applying $H/H_2 \cong \langle g_2\rangle$ on (4.1.1) gives

$$\mathbf{F}[V]^H[x_1^{-1}] = (\mathbf{F}[V]^{H_2}[x_1^{-1}])^{H/H_2} = \mathbf{F}[x_1, \mathbf{N}_{g_1}(x_2), \mathrm{inv}(x_2^2), \mathbf{N}_c(\mathrm{inv}(x_2^3))]^{\langle g_2\rangle}[x_1^{-1}],$$

so this time we need to describe $\mathbf{F}[x_1, \mathbf{N}_{g_1}(x_2), \mathrm{inv}(x_2^2), \mathbf{N}_c(\mathrm{inv}(x_2^3))]^{\langle g_2\rangle}$. Shifting the generators to degree one again yields the following basis: $\{x_1, z_1 := \mathbf{N}_{g_1}(x_2)/x_1^{p-1}, z_2 := \mathrm{inv}(x_2^2)/x_1, z_3 := \mathbf{N}_c(\mathrm{inv}(x_2^3))/x_1^{3p-1}\}$. Thus

$$\mathbf{F}[V]^H[x_1^{-1}] = \mathbf{F}[x_1, z_1, z_2, z_3]^{\langle g_2\rangle}[x_1^{-1}].$$

This time we have to understand how g_2 acts on the basis elements. After explicit computations we find

$$x_1 \cdot g_2 = x_1,\ z_1 \cdot g_2 = z_1 + (c_{1,2}^p - c_{1,2})x_1,$$
$$z_2 \cdot g_2 = z_2 + (c_{1,2}(c_{1,2} - 1) - 2c_{2,4})x_1,$$
$$z_3 \cdot g_2 = z_3 + 3(c_{1,3} - c_{2,4})^p z_1 + (\kappa^p - \kappa(c_{2,4} - c_{1,3})^{p-1})x_1,$$

where $\kappa = c_{1,2}^3 - c_{1,2} + 3\,c_{1,4} - 3\,c_{1,2}c_{1,4}$. Therefore, the induced representation this time is

$$g_2 \mapsto \rho_{g_2}(g_2) = \begin{bmatrix} 1 & c_{1,2}^p - c_{1,2} & c_{1,2}(c_{1,2}-1) - c_{2,4} & \kappa^p - \kappa(c_{1,3} - c_{2,4})^{p-1} \\ 0 & 1 & 0 & 3(c_{1,3} - c_{2,4})^p \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Previously the action of c on the new basis was Nakajima, so we were able to apply basic techniques to compute the ring of invariants. Here this is not the case and $\mathbf{F}[x_1, z_1, z_2, z_3]^{\langle g_2 \rangle}$ is not directly computable, so we follow a different approach.

The quotient group $H/Z(H)$ acts on the first three-variables $\{x_1, x_2, x_3\}$. Since $\dim_{\mathbf{F}}(V^H) = 1$, the quotient V/V^H defines a three-dimensional $\mathbf{F}H/Z(H)$-module and the canonical projection $\pi : V \to V/V^H$ induces an inclusion of algebras $\mathbf{F}[V/V^H]^{H/Z(H)} \hookrightarrow \mathbf{F}[V]^H$. Since $H/Z(H)$ is a two elementary abelian p-group, using [7] gives a description of $\mathbf{F}[V/V^H]^{H/Z(H)}$. The generating set of the last invariant ring contains the minimum degree invariants of $\mathbf{F}[V]^H$ in the first three variables and the following theorem describes their lead monomials.

Theorem 4.1.2.6. ([2, Theorem 6.2]) *Assume that $G \cong C_p \times C_p = \langle e_1, e_2 \rangle$ is an elementary abelian group of rank two and that*

$$\rho : G \to \mathrm{GL}_3(\mathbf{k}),$$

is a generic rank two representation over $\mathbf{k} := \mathbf{F}(x_{11}, x_{1,2}, x_{21}, x_{22})$. Then there is a SAGBI basis of $\mathbf{F}[V_3]^G$, $\mathscr{B} := \{x_1, f_1, f_2, \mathbf{N}_G(x_3)\}$, consisting of homogeneous polynomials with lead monomials

$$x_1, \mathrm{LM}(f_1) = x_2^p, \mathrm{LM}(f_2) = x_2^{p+2}, \mathrm{LM}(\mathbf{N}_G(x_3)) = x_3^{p^2}.$$

We want to construct H-invariants with lead monomials as given in the last theorem. Regarding x_1 there is nothing to say. The stabilizer of x_3 in $\mathbf{F}[V]^H$ has cardinality p, thus the lead term of the orbit product $\mathbf{N}_H(x_3)$ is $\mathrm{LT}(\mathbf{N}_H(x_3)) = x_3^{p^2}$. So we need to construct f_1, f_2.

Lemma 4.1.2.7. *Assume $c_{1,2}^2 - c_{1,2} - 2c_{2,4} \neq 0$. There exists an invariant $f_1 \in \mathbf{F}[V]^H$ in the first three variables such that $\mathrm{LT}(f_1) = x_2^p$, given by the formula*

$$f_1 = \mathbf{N}_{g_1}(x_2) - \alpha\, x_1^{p-2}\mathrm{inv}(x_2^2),$$

where $\alpha = \frac{c_{1,2}^p - c_{1,2}}{c_{1,2}^2 - c_{1,2} - 2c_{2,4}} \in \mathbf{F}$.

Proof. The commutator c leaves fixed the first three variables, so $\mathbf{N}_{g_1}(x_2)$ and $\mathrm{inv}(x_2^2)$ are H_2-invariant. To verify that $f_1 \in \mathbf{F}[V]^H$ we have only to check that $g_2(f_1) = f_1$. A routine computation proves our claim. □

Because the denominator of α will occur in our analysis frequently, we set $\gamma := c_{1,2}^2 - c_{1,2} - 2\,c_{2,4}$ and we assume $\gamma \neq 0$ from now on. Finding f_2 is expected to be a bit more difficult since one additional variable is required. However, we would like to think f_2 for convenience as an extension of f_1. Setting $\tilde{f} := \mathrm{inv}(x_2^2)^p - f_1^2$ gives: $\mathrm{inv}(x_2^2) \cdot g_2 = \mathrm{inv}(x_2^2) + \gamma x_1^2, \mathbf{N}_{g_1}(x_2) \cdot g_2 = \mathbf{N}_{g_1}(x_2) + (c_{1,2}^p - c_{1,2})\, x_1^p$, thus $\tilde{f} \cdot g_2 = \tilde{f} + \gamma x_1^{2p}$. Although $\tilde{f}$ is not an H-invariant, can be turned into one by adding some extra terms.

Lemma 4.1.2.8. *Assume $c_{1,2} \notin \mathbf{F}_p$ and define*

$$f_2 = (\mathrm{inv}(x_2^2)^p - f_1^2 - \,\kappa\, x_1^p\, \mathbf{N}_{g_1}(x_2))/(2\alpha x_1^{p-2}),$$

where $\kappa := \frac{\gamma^p}{c_{1,2}^p - c_{1,2}}$. Then $f_2 \in \mathbf{F}[V]^H$ and $\mathrm{LT}(f_2) = x_2^{p+2}$.

Proof. We observe that the second term in order in f_1^2 is $-2\alpha x_2^{p+2} x_1^{p-2}$. Since $\mathrm{LT}(\mathrm{inv}(x_2^2)^p) = \mathrm{LT}(f_1^2)$ and every term in $x_1^p \mathbf{N}_{g_1}(x_2)$ has at least a power of x_1^p, the lead term must be $2\alpha x_2^{p+2} x_1^{p-2}$. Thus in f_2 we obtain $\mathrm{LT}(f_2) = x_2^{p+2}$. Regarding the first assertion, from the comments in the paragraph right before the lemma we see that g_2 fixes $\mathrm{inv}(x_2^2)^p - \,\kappa\, x_1^p\, \mathbf{N}_{g_1}(x_2)$ and since f_1 is an H-invariant, follows that $f_2 \in \mathbf{F}[V]^H$. □

Now the only thing left to compute $\mathbf{F}(V)^H$ is to construct the minimum x_4-degree invariant. Equation (4.1.1) gives $\mathbf{F}(V)^{H_2} = \mathbf{F}(x_1, \mathbf{N}_{g_1}(x_2), \mathrm{inv}(x_2^2), \mathbf{N}_c(\mathrm{inv}(x_2^3)))$, with $\mathbf{N}_c(\mathrm{inv}(x_2^3))$ of minimum x_4-degree, $\deg_{x_4}(\mathbf{N}_c(\mathrm{inv}(x_2^3))) = p$. Due to the inclusion of fields $\mathbf{F}(V)^H \subset \mathbf{F}(V)^{H_2}$ we know that the minimum x_4-degree H-invariant must have degree at least p too. So if we were able to construct an H-invariant with exactly that x_4-degree, then it would be automatically a generator of $\mathbf{F}(V)^H$.

Lemma 4.1.2.9. *The polynomial defined by the formula*

$$f_3 := \mathbf{N}_c(\mathrm{inv}(x_2^3)) - b_1 x_1^p\, \mathbf{N}_{g_1}^2(x_2) - b_2\, x_1^{2p}\, \mathbf{N}_{g_1}(x_2) \in \mathbf{F}[V]^H,$$

where

$$b_1 := \frac{3(c_{1,3} - c_{2,4})^p}{2(c_{1,2}^p - c_{1,2})}\,,\ b_2 := \frac{w}{(c_{1,2}^p - c_{1,2})} - \frac{3(c_{1,3} - c_{2,4})^p}{2} \in \mathbf{F}$$

$w = c_{1,2}^{3p} + 2c_{1,2}^p c_{2,4}^p - c_{1,2}^p - (c_{2,4} - c_{1,3})^{p-1}(c_{1,2}^3 + 2c_{1,2}c_{2,4} - c_{1,2})$ *and* $c_{1,2} \notin \mathbf{F}_p$, *forms an H-invariant of minimum x_4-degree. Moreover* $\mathrm{LT}(f_3) = x_2^{3p}$.

Proof. As a reminder, we have $\mathrm{inv}(x_2^3) = x_2^3 + x_1^2(3x_4 - x_2) - 3x_1x_2x_3$. From the description of the orbit product $\mathbf{N}_c(y_3) = y_3^p - (c_{2,4} - c_{1,3})^{p-1}x_1^{p-1}y_3$, where $y_3 = \mathrm{inv}(x_3^2)/x_1^2$, we obtain

$$\frac{\mathbf{N}_c(\mathrm{inv}(x_2^3))}{x_1^{2p}} = \frac{\mathrm{inv}(x_2^3)}{x_1^{2p}} - (c_{2,4} - c_{1,3})^{p-1}\, x_1^{p-1} \frac{\mathrm{inv}(x_2^3)}{x_1^2},$$

hence

$$\mathbf{N}_c(\mathrm{inv}(x_2^3)) = \mathrm{inv}(x_2^3)^p - (c_{2,4} - c_{1,3})^{p-1}\, x_1^{3(p-1)} \mathrm{inv}(x_2^3)$$

follows that is has x_4-degree p from the definition of $\mathrm{inv}(x_2^3)$. A routine computation gives

$$\mathbf{N}_c(\mathrm{inv}(x_2^3)) \cdot g_2 := \mathbf{N}_c(\mathrm{inv}(x_2^3)) + 3\,(c_{1,3} - c_{2,4})^p\, x_1^{2p}\, \mathbf{N}_{g_1}(x_2) + w\, x_1^{3p},$$

for $w = c_{1,2}^{3p} + 2c_{1,2}^p c_{2,4}^p - c_{1,2}^p - (c_{2,4} - c_{1,3})^{p-1}(c_{1,2}^3 + 2c_{1,2}c_{2,4} - c_{1,2}) \in \mathbf{F}$. Thus for

$$b_1 := \frac{3(c_{1,3} - c_{2,4})^p}{2(c_{1,2}^p - c_{1,2})}\,,\ b_2 := \frac{w}{(c_{1,2}^p - c_{1,2})} - \frac{3(c_{1,3} - c_{2,4})^p}{2} \in \mathbf{F},$$

the resulting polynomial becomes an invariant, $f_3 \in \mathbf{F}[V]^H$. □

Lemma 4.1.2.10. $\mathbf{F}(V)^H = \mathbf{F}(x_1, f_1, f_2, f_3)$. *In particular, localizing at x_1 yields*

$$\mathbf{F}[V]^H[x_1^{-1}] = \mathbf{F}[x_1, f_1, f_2, f_3][x_1^{-1}].$$

Proof. From the above discussion it is obvious that $\mathbf{F}(V/V^H)^H = \mathbf{F}(x_1, f_1, f_2) \subset \mathbf{F}(V)^H$. Thus attaching the minimum x_4-degree invariant on $\mathbf{F}(V/V^H)^H$ yields the seeking equality $\mathbf{F}(V)^H = \mathbf{F}(x_1, f_1, f_2, f_3)$. The equality of localized rings now follows from Theorem 1.4.2.6 since $\mathrm{LC}_{x_4}(f_3) = x_1^{2p}$. □

4.1.3 The invariant ring $\mathbf{F}[V]^H$

Set $\mathscr{B}' := \{x_1, f_1, f_2, f_3, \mathbf{N}_H(x_3), \mathbf{N}_H(x_4)\}$. We wish to apply SAGBI/divide-by-x algorithm on $\mathscr{B}'$. In $\mathscr{B}'$ there are two non-trivial tête-à-têtes : (f_1^{p+2}, f_2^p), (f_1^3, f_3).

Lemma 4.1.3.1. *Subducting the tête-à-tête (f_1^3, f_3) defines an invariant with lead term: $-2\alpha^2 x_1^{2(p-2)} x_2^{p+4}$.*

Proof. Let $\langle x_1^{p-1}\rangle \lhd \mathbf{F}[V]$ denote the ideal generated by x_1^{p-1}. For f_1^3, expanding and reducing modulo $\langle x_1^{p-1}\rangle$ yields

$$f_1^3 \equiv_{\langle x_1^{p-1}\rangle} x_2^{3p} - 3\alpha x_1^{p-2} x_2^{2(p+1)}.$$

Concerning f_3 things are straightforward, since all the other terms but the leading contain a power of x_1^{p-1}. Thus

$$f_3 \equiv_{\langle x_1^{p-1}\rangle} x_2^{3p}.$$

All together gives

$$f_1^3 - f_3 \equiv_{\langle x_1^{p-1}\rangle} -3\alpha x_1^{p-2} x_2^{2(p+1)}.$$

So the tête-à-tête (f_1^3, f_3) has lead term: $-3\alpha x_1^{p-2} x_2^{2(p+1)}$. Define now

$$\tilde{h}_1 := f_1^3 - f_3 + 3\,\alpha\, x_1^{p-2} f_1 f_2.$$

We work modulo the ideal $\langle x_1^{p+1}\rangle \lhd \mathbf{F}[V]$ and analyze each part of the last expression. Every term in f_1 has x_1-degree less than $(p+1)$. So expanding and reducing modulo x_1^{p+1} gives

$$f_1^3 \equiv_{\langle x_1^{p+1}\rangle} \mathbf{N}_{g_1}^3(x_2) - 3\,\alpha\, x_1^{p-2} x_2^{2p}\,\mathrm{inv}(x_2^2) \equiv_{\langle x_1^{p+1}\rangle} x_2^{3p} - 3\, x_1^{p-1} x_2^{2p+1} - 3\,\alpha\, x_1^{p-2} x_2^{2p}\mathrm{inv}(x_2^2).$$

For f_3 we find

$$f_3 \equiv_{\langle x_1^{p+1}\rangle} \mathrm{inv}(x_2^3)^p - b_1\, x_1^p x_2^{2p}.$$

The expression of f_2 modulo $\langle x_1^3\rangle$ is equivalent to reducing $x_1^{p-2} f_2$ modulo $\langle x_1^{p+1}\rangle$. Thus

$$f_2 \quad \equiv_{\langle x_1^3\rangle} \quad x_2^{p+2} - 2x_3 x_2^p x_1 - (\alpha+1)/\alpha \cdot x_2^{p+1} x_1 - 1/\alpha \cdot x_3^p x_1^2 - \kappa/2\alpha \cdot x_2^p x_1^2,$$

implies

$$x_1^{p-2} f_2 \equiv_{\langle x_1^{p+1}\rangle} x_1^{p-2} x_2^{p+2} - 2x_3 x_2^p x_1^{p-1} - (\alpha+1)/\alpha \cdot x_2^{p+1} x_1^{p-1} - 1/\alpha \cdot x_3^p x_1^p - \kappa/2\alpha \cdot x_2^p x_1^p. \tag{4.1.2}$$

Summarizing all the above yields

$$\mathrm{LT}(\tilde{h}_1) = (b_1 - \frac{3}{2}(1+\kappa)) x_1^p x_2^{2p} = \frac{3}{2} \frac{c_{1,3}^p + c_{2,4}^p - c_{1,2}^{2p} + c_{1,2}}{c_{1,2}^p - c_{1,2}} x_1^p x_2^{2p}.$$

Set

$$h_1 = \tilde{h}_1 - \frac{3}{2} \frac{c_{1,3}^p + c_{2,4}^p - c_{1,2}^{2p} + c_{1,2}}{c_{1,2}^p - c_{1,2}} x_1^p f_1^2.$$

This time we work modulo $\langle x_1^{2p-3}\rangle$. For $x_1^p f_1^2$ follows easily that: $x_1^p f_1^2 \equiv_{\langle x_1^{2p-3}\rangle} x_1^p x_2^{2p}$. Thus no term of $x_1^p f_1^2$ exists in the quotient ring.

Expanding f_1^3 and reducing modulo $\langle x_1^{2p-3}\rangle$ gives

$$f_1^3 \equiv_{\langle x_1^{2p-3}\rangle} \alpha^2\, x_1^{2(p-2)}\, x_2^{p+4}.$$

Similarly for f_3 we obtain

$$f_3 \equiv_{\langle x_1^{2p-3}\rangle} x_2^{3p} - 3\, x_1^p x_2^p x_3^p.$$

However, these two terms of f_3 both vanish in the quotient ring. The lead term of f_1^3 cancels x_2^{3p}, while the forth term of (4.1.2) multiplied by $3\alpha f_1$ in $\widetilde{h_1}$ cancels $-3x_1^p x_2^p x_3^p$.

Furthermore, in $3\alpha x_1^{p-2} f_1 f_2$ the lead term of $x_1^{p-2} f_2$ multiplied with the corresponding of $x^{p-2}\text{inv}(x_2^2)$ in f_1 yields: $-3\alpha^2 x_1^{2(p-2)} x_2^{p+4}$. Thus, with the corresponding in f_1^3 gives a copy of $-2\alpha^2 x_1^{2(p-2)} x_2^{p+4}$ in h_1 modulo $\langle x_1^{2p-3}\rangle$. From all the above discussion we conclude that this can be the only term. Thus

$$\text{LT}(h_1) = -2\alpha^2 x_1^{2(p-2)} x_2^{p+4}.$$

□

Lemma 4.1.3.2. *The tête-à-tête (f_1^{p+2}, f_2^p) subducts to zero.*

Proof. Remember from previous remark that H acts on the first three variables as an elementary abelian p-group. Therefore, from [7, Theorem 6.2] we know that $\{x_1, f_1, f_2, \mathbf{N}_H(x_3)\}$ forms a SAGBI basis for $\mathbf{F}[x_1, x_2, x_3]^H \subset \mathbf{F}[V]$. Thus (f_1^{p+2}, f_2^p) subducts to zero necessarily. □

We set $s_1 = x_1^{-2(p-2)} h_1$ and $\mathscr{B} := \{x_1, f_1, f_2, s_1, \mathbf{N}_H(x_3)\}$ with $\text{LT}(\mathscr{B}) = \{x_1, x_2^p, x_2^{p+2}, x_2^{p+4}, x_3^{p^2}\}$. Note that when s_1 is attached, f_3 is not needed anymore. Following Lemma 4.1.2.10 now we obtain the following theorem.

Theorem 4.1.3.3. $\mathbf{F}[V]^H[x_1^{-1}] = \mathbf{F}[x_1, f_1, f_2, s_1][x_1^{-1}]$. *The corresponding lead terms are:* $\text{LT}(f_1) = x_2^p, \text{LT}(f_2) = x_2^{p+2}, \text{LT}(s_1) = x_2^{p+4}$.

In $\mathscr{B}$ we obtain three non-trivial tête-à-têtes : (f_1^{p+4}, s_1^p), (f_2^{p+4}, s_1^{p+2}), $(f_2^2, f_1 s_1)$. Computations made on MAGMA for primes $p = 5, 7$ and 11 suggest that the above tête-à-tête subductions lead to invariants with lead term some power of x_2. At the second stage the number of subductions increases significantly making the computation of $\mathbf{F}[V]^H$ infeasible. From our experience this phenomenon is explained from the fact that $\rho_{\mathscr{B}}(H)$ is not a bireflection group, hence $\mathbf{F}[V]^H$ not Cohen-Macaulay.

4.1.4 Non Cohen-Macaulyness of $\mathbf{F}[V]^H$

In this section we construct for $p = 5$ an hsop which is not a regular sequence. In the introduction we proved that $\rho_{\mathscr{B}}(H)$ is not bireflection group, hence $\mathbf{F}[V]^H$ not

Cohen-Macaulay. From Chapter 1 also we know that the ring of invariants $\mathbf{F}[V]^H$ is always a graded finitely generated connected $\mathbf{F}$-algebra. Thus we can exploit the following theorem for this prime to prove that $\mathbf{F}[V]^H$ is not Cohen-Macaulay by presenting an intrinsic argument.

Theorem 4.1.4.1. *[8, Theorem, 2.8.1] Let R be a finitely generated connected graded $\mathbf{F}$-algebra which is Cohen-Macaulay. Then every homogeneous system of parameters for R is a regular sequence for R.*

The last theorem implies that if we were able to construct an hsop for $\mathbf{F}[V]^H$ which is not a regular sequence, then we have proven our claim. We pick a partial hsop that works for any prime number $\{x_1, \mathbf{N}_H(x_2), \mathbf{N}_H(x_3)\}$ and claim that when $p = 5$ cannot extend to a regular sequence. To prove this claim we need two things:

(1) there exist invariants $f, h \in \mathbf{F}[V]^H$, such that

$$f\,\mathbf{N}_H(x_3) + h\,\mathbf{N}_H(x_2) \in (x_1)\mathbf{F}[V]^H,$$

(2) $f \notin (x_1, \mathbf{N}_H(x_2))\mathbf{F}[V]^H$.

The computations that follow have been made on MAGMA over the finite field $\mathtt{F}\langle t\rangle$:=$\mathtt{GF}(p^r)$ for $r := 4$, with $c_{i,j} :=$ $\mathtt{Random}(F)$ random over the Galois field $\mathtt{GF}(p^4)$.

The main idea of the following technique comes from [24, Corollary, 11.5]. First we recall a construction from commutative algebra that will be used for the rest of this section, **toric ideals**. Assume that we have a vector configuration, $\mathscr{A} = \{\mathbf{a}_1, ..., \mathbf{a}_n\} \subset \mathbb{Z}^d - \{0\}$, i.e., the induced matrix has rank d. Then we can define a map between commutative monoids as follows

$$\pi : \mathbb{N}^n \to \mathbb{Z}^d,$$
$$\mathbf{u} = (u_1, ..., u_n) \mapsto A\mathbf{u},$$

where $A = [\mathbf{a}_1 \cdots \mathbf{a}_n] \in \mathbb{Z}^{d\times n}$. This induces an $\mathbf{F}$-algebra homomorphism

$$\hat{\pi} : \mathbf{F}[x_1, ..., x_n] \to \mathbf{F}[t_1^{\pm 1}, ..., t_d^{\pm 1}],$$
$$x_j \mapsto \mathbf{t}^{\mathbf{a}_j} := t_1^{a_{1j}} \cdots t_d^{a_{dj}}.$$

Definition 4.1.4.2. *The toric ideal associated to $\mathscr{A}$, $I_{\mathscr{A}} \subset \mathbf{F}[x_1, ..., x_n]$, is the kernel of the map $\hat{\pi}$.*

With respect any term order we can use generators of the toric ideal induced from vectors of lead terms of a subset $\mathscr{B} \subset \mathbf{F}[V]^H$, to subduct tête-à-têtes . Think of a polynomial algebra in n variables $\mathbf{F}[X_1, ..., X_n]$ and the diagram

$$\begin{array}{ccc} & & \mathbf{F}[\mathscr{B}] \\ & \overset{\phi}{\nearrow} & \\ \mathbf{F}[X_1, ..., X_n] & & \\ & \underset{\psi}{\searrow} & \\ & & \mathbf{LT}_{\prec}(\mathbf{F}[\mathscr{B}]), \end{array}$$

under the identifications $X_i \mapsto f_i$ for ϕ and $X_i \mapsto \mathrm{LT}_{\prec}(f_i)$ for ψ. In principle this iterated process of subductions and attachments creates a chain of sets $\mathscr{B} \subset \mathscr{B}_1 \subset ... \subset \mathscr{B}_k$ and we obtain a SAGBI basis for $\mathbf{F}[V]^H$ precisely when $\mathbf{LT}_{\prec}(\mathbf{F}[\mathscr{B}_k]) = \mathbf{LT}_{\prec}(\mathbf{F}[V]^H)$. Below we use lexicographic order with $X_1 < ... < X_n$ for $\mathbf{F}[X_1, ..., X_n]$.

Also we use the notation $\textsc{subd}(t, \mathbf{A})$ to denote the subduction of a tête-à-tête t against a list of invariants $\mathbf{A}$, after is has been divided by the superfluous x_1-power and the leading coefficient. According to that notation for instance

$$s_1 = \textsc{subd}\left(f_1^3 - f_3, [x_1, f_1, f_2, f_3, \mathbf{N}_A(x_3)_H(x_3)]\right).$$

Below follows a series of subductions and Gröbner basis calculations which construct the invariants that prove our claim. We also remind you that $\mathscr{B} = \{x_1, f_1, f_2, s_1, \mathbf{N}_H(x_3)\}$.

Step 1: The Gröbner basis of the toric ideal $I_{\mathscr{B}}$ for any p, is the set of binomials $\{X_4X_2 - X_3^2, X_4^2X_3 - X_2^5, X_4^3 - X_3X_2^4, X_4X_3^3 - X_2^6, X_3^5 - X_2^7\}$. Furthermore, the binomial $X_4X_2 - X_3^2$ forms a generic choice and Subducting $t_2 := f_2^2 - s_1 f_1$ gives an invariant $s_2 := \text{SUBD}(t_2, \mathscr{B})$ with

$$\text{LT}(s_2) = x_2^{2p+1}.$$

For $p = 5$, the other invariants obtained by the subdcutions $s_3 := \text{SUBD}(s_1 f_2^3 - f_1^6, \mathscr{B})$, $s_4 := \text{SUBD}(f_1^5 - s_1^2 f_2, \mathscr{B})$, $s_5 := \text{SUBD}(s_1^3 - f_2 f_1^4, \mathscr{B})$, have lead terms

$$\text{LT}(s_3) = x_3^{10} x_2^{16},\ \text{LT}(s_4) = x_3^{10} x_2^{11},\ \text{LT}(s_5) = x_3^{10} x_2^{13}.$$

The last tête-à-tête subduction $\text{SUBD}(f_1^7 - f_2^5, \mathscr{B})$, subducts to a polynomial with lead term x_3^{25}.

Let $\mathscr{B}_1 := \mathscr{B} \cup \{s_2, s_3, s_4, s_5\}$ denote the new list after the above elements have been attached.

Step 2: Among Gröbner basis elements of $I_{\mathscr{B}_1}$ there is a binomial $X_3X_5 - X_2X_6$. Define $s_6 := \text{SUBD}(f_2 s_1 - f_1 s_2, \mathscr{B}_1)$, then

$$\text{LT}(s_6) := x_3^{10} x_2^5.$$

Step 3: There exists an invariant $s_7 := \text{SUBD}(s_1^2 - s_2 f_2, \mathscr{B}_1) \in \mathbf{F}[V]^H$, with

$$\text{LT}(s_7) = x_3^{10} x_2^7,$$

obtained by Subducting the reduced Gröbner basis element of $I_{\mathscr{B}_1}$, $X_5^2 - X_6X_3$. Furthermore, for $\mathscr{B}_2 := \mathscr{B}_1 \cup \{s_6, s_7\}$, the Gröbner basis element $X_2^4 - X_5X_6$ of $I_{\mathscr{B}_2}$ subducts to an invariant $s_8 := \text{SUBD}(f_1^4 - s_1 s_2, \mathscr{B}_2)$, with $\text{LT}(s_8) = x_3^{10} x_2^9$.

Step 4: For $\mathscr{B}_3 := \mathscr{B}_2 \cup \{s_8\}$, we have a tête-à-tête subduction $s_9 := \text{SUBD}(s_2^2 - f_1^3 f_2, \mathscr{B}_3)$, obtained by the binomial generator $X_7 - X_2X_8$, of $I_{\mathscr{B}_3}$, with $\text{LT}(s_9) = x_3^{20}$. Additionally there are three more invariats, obtained from the subduction of the Gröbner basis elements of $I_{\mathscr{B}_3}$, $X_6^2 - X_2^3X_3, X_7 - X_5X_4, X_7 - X_1^2X_3$. Denote

$$s_{10} := \text{SUBD}(s_3 - f_1 s_4, \mathscr{B}_3),$$
$$s_{11} := \text{SUBD}(s_3 - s_1 s_7, \mathscr{B}_3),$$
$$s_{1,2} := \text{SUBD}(s_3 - f_2 s_8, \mathscr{B}_3).$$

the corresponding subductions. These invariants have lead term: $x_3^{20}x_2^2$. We can confirm that including them in $\mathscr{B}_3$ along with s_9, gives all the SAGBI elements up to degree 27. Set $\mathscr{B}_4 := \mathscr{B}_3 \cup \{s_9, s_{10}, s_{11}, s_{1,2}\}$.

Step 5: The Gröbner basis of $I_{\mathscr{B}_4}$, contains a binomial $X_3X_{16} - X_5X_{1,3}$ such that the corresponding tête-à-tête subducts to $s_{1,3} := \textsc{subd}(s_1s_9 - f_2s_{1,2}, \mathscr{B}_4)$, with lead term

$$\mathrm{LT}(s_{1,3}) = x_3^{25}x_2^2.$$

Furthermore, if the invariant $\textsc{subd}(s_1s_9 - f_2s_{1,2}, \mathscr{B}_4)$ is included, then we have all the SAGBI basis elements up to degree 29.

A synopsis of the above tête-à-tête subductions is given in the following table where in the first row we have the subductions and in the second their corresponding lead terms as depicted above:

s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}
x_2^9	x_2^{11}	$x_3^{10}x_2^{16}$	$x_3^{10}x_2^{11}$	$x_3^{10}x_2^{13}$	$x_3^{10}x_2^5$	$x_3^{10}x_2^7$	$x_3^{10}x_2^9$	x_3^{20}	$x_3^{20}x_2^2$	$x_3^{20}x_2^2$	$x_3^{20}x_2^2$	$x_3^{25}x_2^2$

Table 4.1: Table of lead terms for $p = 5$.

Now we return to our initial assertion.

Proposition 4.1.4.3. *For $p = 5$, the partial hsop $\{x_1, \mathbf{N}_H(x_2), \mathbf{N}_H(x_3)\}$ is not a regular sequence.*

Proof. Firstly, we notice that the set $\{x_1, \mathbf{N}_H(x_2)\}$ is a regular sequence for $\mathbf{F}[V]^H$. So to prove our assertion, we need only to prove the following two arguments

(1) there exist invariants $f, h \in \mathbf{F}[V]^H$, such that

$$f\,\mathbf{N}_H(x_3) + h\,\mathbf{N}_H(x_2) \in (x_1)\mathbf{F}[V]^H,$$

(2) $f \notin (x_1, \mathbf{N}_H(x_2))\mathbf{F}[V]^H$.

Then we have proven that $\mathbf{N}_H(x_3)$ is a zero divisor in $\mathbf{F}[V]^H/(x_1, \mathbf{N}_H(x_2))\mathbf{F}[V]^H$, hence $\{x_1, \mathbf{N}_H(x_2), \mathbf{N}_H(x_3)\}$ is not a regular sequence. We shall denote by $\mathrm{LC}_i \in \mathbf{F}$ the coefficients during the MAGMA computations.

Set $f := f_1^4 f_2$. Can be easily verified that $\mathrm{LT}(f\,\mathbf{N}_H(x_3)) = x_3^{25}x_2^{27}$. From **Step 5** we know that $(f_1^4 f_2 \mathbf{N}_H(x_3), s_{1,3}\mathbf{N}_H(x_2))$ is a tête-à-tête with lead term $\mathrm{LT}(f_1^4 f_2 \mathbf{N}_H(x_3) - s_{1,3}\mathbf{N}_H(x_2)) = \mathrm{LC}_1\, x_3^{20}x_2^{32}$, while by **Step 4** we observe that the polynomial $s_9\, f_1\, \mathbf{N}_H(x_2)$ has the same lead term, hence $(f_1^4 f_2 \mathbf{N}_H(x_3) - s_{1,3}\mathbf{N}_H(x_2), \mathrm{LC}_1\, s_9 f_1 \mathbf{N}_H(x_2))$ is a tête-à-tête too. The lead term of the last tête-à-tête according to MAGMA is: $\mathrm{LT}(f_1^4 f_2 \mathbf{N}_H(x_3) - s_{1,3}\mathbf{N}_H(x_2) - \mathrm{LC}_1\, s_9 f_1 \mathbf{N}_H(x_2)) = \mathrm{LC}_2\, x_3^{10}x_2^{42}$, for some $\mathrm{LC}_2 \in \mathbf{F}$.

Due to **Step 3** we know that an invariant with lead term $x_3^{10}x_2^{7}$ exists. Thus along with f_1^2 gives $\mathrm{LT}(s_7 f_1^2 \mathbf{N}_H(x_2)) = x_3^{10}x_2^{42}$. So the tête-à-tête difference $(f_1^4 f_2 \mathbf{N}_H(x_3) - s_{13}\mathbf{N}_H(x_2) - \mathrm{LC}_1\, s_9 f_1 \mathbf{N}_H(x_2), \mathrm{LC}_2\, s_7 f_1^2 \mathbf{N}_H(x_2))$, yields a new invariant, with

$$\mathrm{LT}(f\,\mathbf{N}_H(x_3) - s_{1,3}\mathbf{N}_H(x_2) - \mathrm{LC}_1\, s_9 f_1 \mathbf{N}_H(x_2) - \mathrm{LC}_2\, s_7 f_1^2 \mathbf{N}_H(x_2)) = \mathrm{LC}_3\, x_2^{52}.$$

The last monomial though is the lead term of $s_1^3\mathbf{N}_H(x_2)$. Their difference on MAGMA returns an invariant with lead term of the form $\mathrm{LC}_4 x_3^{20}x_2^{31}x_1$. Therefore

$$f\,\mathbf{N}_H(x_3) - s_{13}\mathbf{N}_H(x_2) - \mathrm{LC}_1\, s_9 f_1 \mathbf{N}_H(x_2) - \mathrm{LC}_2\, s_7 f_1^2 \mathbf{N}_H(x_2) - \mathrm{LC}_3\, s_1^3 \mathbf{N}_H(x_2) \in (x_1)\mathbf{F}[V]^H.$$

So we can set $h = s_{13} + \mathrm{LC}_1\, s_9 f_1 + \mathrm{LC}_2\, s_7 f_1^2 + \mathrm{LC}_3\, s_1^3$ to obtain the first requirement. For the second one, that is $f \notin (x_1, \mathbf{N}_H(x_2))\mathbf{F}[V]^H$, assume the contrary. Then $f = g_1 x_1 + g_2 \mathbf{N}_H(x_2)$, for $g_1, g_2 \in \mathbf{F}[V]^H$. However, $\mathrm{LT}(f) = x_2^{27}$, so the lead term necessarily comes from the multiplication of $g_2 \mathbf{N}_H(x_2)$. This implies though, that g_2 has lead monomial x_2^2 which is a contradiction since we have proved earlier that the invariants in $\mathbf{F}[V]^H$ with the minimum x_2-degree have degree at least five. So such an invariant can't exist. □

4.2 Invariants of type-(1,1,2) representations.

4.2.1 The invariant field $\mathbf{F}(V)^H$

Let V denote a four-dimensional left $\mathbf{F}H$-module of type-$(1,1,2)$. Then the group of representing matrices consists of

$$\begin{bmatrix} 1 & c_{1,2} & c_{1,3} & c_{1,4} \\ 0 & 1 & c_{2,3} & c_{2,4} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \ c_{i,j} \in \mathbf{F}.$$

We recall from Theorem 2.4.0.5 the existence of a basis $\mathscr{B}'$ consistent with the socle series, such that $\{J_{3,1}, \widetilde{B}\}$ forms a generating set for $\rho_{\mathscr{B}'}(H)$ with

$$\widetilde{B} := \begin{bmatrix} 1 & \widetilde{b_{1,2}} & \widetilde{b_{1,3}} & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \ \widetilde{b_{1,2}}, \widetilde{b_{1,3}} \in \mathbf{F}.$$

For computational reasons we change the generating set of H with something equivalent. Instead of $J_{3,1}$ we choose to work with

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

Notice that $A \sim J_{3,1}$, i.e., $\exists P \in \mathrm{GL}_4(\mathbf{F})$ such that $P^{-1}AP = J_{3,1}$. A routine computation gives

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

and conjugating the second generator

$$P^{-1}\widetilde{B}P = \begin{bmatrix} 1 & b_{1,2} & 0 & b_{1,4} \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Denote $B := P^{-1}\widetilde{B}P$ and $\mathscr{B}$ for the resulting basis. Then $\rho_{\mathscr{B}}(H) = \langle A, B\rangle$. Before we start the invariant field $\mathbf{F}(V)^H$ computation we observe the following.

Lemma 4.2.1.1. *The group $\rho_{\mathscr{B}}(H)$ is a bireflection group.*

Proof. To prove our assertion suffices to show that the fixed point space of each generator is at least two-dimensional. For A follows immediately that $V^A = \mathrm{Span}_{\mathbf{F}}\{e_1, e_3\}$, while for B it is not difficult to see that $V^B = \mathrm{Span}_{\mathbf{F}}\{e_1, b_{1,4}e_2 - b_{1,2}e_4\}$. Now our claim follows.

□

Consider the composition series $\langle A\rangle \triangleleft \langle A, C\rangle \triangleleft \langle A, B\rangle = H$, where $C := [A, B]$ denotes the commutator element

$$C = ABA^{-1}B^{-1} = \begin{bmatrix} 1 & 0 & 1 & -b_{1,2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The first step is to compute $\mathbf{F}[V]^{\langle A\rangle}$. Since $\langle A\rangle \cong C_p$ we can apply [6, Theorem 3.2]. Notice that $\langle A\rangle$ acts on the first three-variables as Nakajima group, hence

$\{x_1, x_2, \mathbf{N}_A(x_3)\}$ is a set of minimum x_i-degree $\langle A\rangle$-invariants, $i = 1, 2, 3$. Furthermore, follows easily that $f_1 = x_3^2 - 2x_4x_1 - x_1x_3 \in \mathbf{F}[V]^{\langle A\rangle}$ is of minimum x_4-degree. So the following lemma is a consequence of Theorem 1.4.2.6.

Lemma 4.2.1.2. $\mathbf{F}(V)^{\langle A\rangle} = \mathbf{F}(x_1, x_2, \mathbf{N}_A(x_3), f_1)$. *Furthermore, we have an equality of localized rings:* $\mathbf{F}[V]^{\langle A\rangle}[x_1^{-1}] = \mathbf{F}[\mathscr{B}][x_1^{-1}]$.

Define $\mathscr{B} := \{x_1, x_2, f_1, \mathbf{N}_A(x_3)\}$. In $\mathscr{B}$ there is a unique non-trivial tête-à-tête: $(f_1^p, \mathbf{N}_A^2(x_3))$.

Lemma 4.2.1.3. *Subducting the tête-à-tête* $(f_1^p, \mathbf{N}_A^2(x_3))$, *yields an invariant with lead term:* $-2x_4^px_1^p$.

Proof. Expanding the definition of the tête-à-tête difference yields: $\mathrm{LT}(f_1^p - \mathbf{N}_A^2(x_3)) = -x_3^{p+1}x_1^{p-1}$.

Set $h_2 := f_1^p - \mathbf{N}_A^2(x_3) - 2x_1^{p-1}f_1^{\frac{p+1}{2}}$. We work modulo $\langle x_1^{p+1}\rangle \lhd \mathbf{F}[V]$ to prove our claim. Expanding $f_1^p - \mathbf{N}_A^2(x_3)$ and reducing modulo $\langle x_1^{p+1}\rangle$ yields

$$f_1^p - \mathbf{N}_A^2(x_3) \equiv_{\langle x_1^{p+1}\rangle} 2x_3^{p+1}x_2^{p-1} - 2x_4^px_1^p - x_3^px_1^p.$$

Regarding $x_1^{p-1}f_1^{\frac{p+1}{2}}$, reducing modulo $\langle x_1^2\rangle$ the invariant $f_1^{\frac{p+1}{2}}$, is equivalent to reducing $x_1^{p-1}f_1^{\frac{p+1}{2}}$ modulo $\langle x_1^{p+1}\rangle$. Thus, since

$$f_1^{\frac{p+1}{2}} \equiv_{\langle x_1^2\rangle} x_3^{p+1} + x_4x_3^{p-1}x_1 + x_3^px_1,$$

we obtain

$$-2x_1^{p-1}f_1^{\frac{p+1}{2}} \equiv_{\langle x_1^{p+1}\rangle} -2x_3^{p+1}x_1^{p-1} - 2x_4x_3^{p-1}x_1^p - 2x_3^px_1^p.$$

Adding up the two parts proves our claim: $\mathrm{LT}(h_2) = -2x_4^px_1^p$. □

Set $f_2 := h_2 \cdot (-x_1^{-p}/2)$ and $\mathscr{B}' := \mathscr{B} \cup \{f_2\}$. Then $\mathscr{B}'$ is a SAGBI basis for the algebra it generates since every tête-à-tête subducts to zero. Furthermore, since $\mathrm{LT}(f_2) = \mathrm{LT}(\mathbf{N}_A(x_4))$ we can replace f_2 with $\mathbf{N}_A(x_4)$ to obtain the following result.

Lemma 4.2.1.4. $\mathbf{F}[V]^{\langle A\rangle} = \mathbf{F}[x_1, x_2, f_1, \mathbf{N}_A(x_3), \mathbf{N}_A(x_4)]$.

Proof. From Lemma 4.2.1.2, follows that $\mathbf{F}[V]^{\langle A\rangle}[x_1^{-1}] = \mathbf{F}[\mathscr{B}'][x_1^{-1}]$ since we just added a new invariant. Also [8, Lemma 2.6.3] implies that the extension $\mathbf{F}[\mathscr{B}'] \subset \mathbf{F}[V]^{\langle A\rangle}$ is integral. Since $\mathscr{B}'$ is a SAGBI basis the result is an application of Theorem 1.4.3.10. □

Applying the $\langle A, C\rangle/\langle C\rangle \cong \langle C\rangle$-action on the equality of localized rings in Lemma 4.2.1.2 gives

$$\mathbf{F}[V]^{\langle A,C\rangle}[x_1^{-1}] = (\mathbf{F}[V]^{\langle A\rangle})^{\langle A,C\rangle/\langle A\rangle}[x_1^{-1}] = \mathbf{F}[\mathscr{B}]^{\langle C\rangle}[x_1^{-1}].$$

To understand $\mathbf{F}[\mathscr{B}]^{\langle C\rangle}[x_1^{-1}]$ we shift the generators of $\mathbf{F}[\mathscr{B}]$ to degree one $y_1 := x_1, y_2 := x_2, y_3 := \mathbf{N}_A(x_3)/x_1^{p-1}, y_4 := f_1/x_1$ and set $W = \mathrm{Span}_{\mathbf{F}}\{y_1, y_2, y_3, y_4\}$ for the vector space they span. Then W is a right $\mathbf{F}\langle C\rangle$-module with C acting

$$y_1 \cdot C = y_1,\ \ y_2 \cdot C = y_2,\ \ y_3 \cdot C = y_3,\ \ y_4 \cdot C = y_4 + y_2 - b_{1,2}y_1.$$

Now the $\langle C\rangle$-action on W is Nakajima, hence the next lemma is a consequence of [8, Theorem 8.0.7].

Lemma 4.2.1.5. $\mathbf{F}[W]^{\langle C\rangle} = \mathbf{F}[y_1, y_2, y_3, \mathbf{N}_C(y_4)]$.

As a result of the last lemma we obtain $\mathbf{F}[V]^{\langle A,C\rangle}[x_1^{-1}] = \mathbf{F}[y_1, y_2, y_3, \mathbf{N}_C(y_4)][x_1^{-1}]$. Substituting and clearing out the denominators minimally gives

$$\mathbf{F}[V]^{\langle A,C\rangle}[x_1^{-1}] = \mathbf{F}[x_1, x_2, \mathbf{N}_A(x_3)/x_1^{p-1}, \mathbf{N}_C(f_1/x_1)][x_1^{-1}] = \mathbf{F}[x_1, x_2, \mathbf{N}_A(x_3), \mathbf{N}_C(f_1)][x_1^{-1}].$$

Furthermore, the generators of the right hand side algebra in the last equality are of minimum x_i-degree for $i = 1, 2, 3, 4$. Regarding the only unknown invariant

$$\mathbf{N}_C(f_1) = f_1.(f_1 + x_2x_1 - b_{1,2}x_1^2)...(f_1 + (p-1)x_2x_1 - (p-1)b_{1,2}x_1^2)$$

we note that forms an invariant of degree $2p$ and x_4-degree p.

Remark 4.2.1.6. *It is worth mentioning that although $\mathbf{N}_C(f_1)$ consists a natural choice of an $\langle A, C\rangle$-invariant of minimum x_4-degree, it is not the invariant of minimum degree with respect to that property.*

We would like to fix that since it is more convenient for our computations to work with invariants of minimum degree with respect a given property. Since $\mathrm{LT}(\mathbf{N}_C(f_1)) = x_3^{2p}$, $\mathrm{LT}(\mathbf{N}_A(x_3)) = x_3^p$, there is a non-trivial tête-à-tête $(\mathbf{N}_C(f_1), \mathbf{N}_A^2(x_3))$. Subducting this tête-à-tête gives the seeking invariant.

Lemma 4.2.1.7. *Subducting* $(\mathbf{N}_C(f_1), \mathbf{N}_A^2(x_3))$ *gives an invariant with lead term* $2x_3^{p+1}x_1^{p-1}$. *Furthermore, it is of minimum* x_4*-degree and after dividing by the superfluous* x_1 *power the resulting invariant is the minimum degree invariant with respect to that property.*

Proof. Set $\widetilde{g_1} := \mathbf{N}_C(f_1) - \mathbf{N}_A^2(x_3)$ and assume that there is another invariant f of minimum degree. Then necessarily $\mathrm{LT}(f) = cx_4^p$, for some $c \in \mathbf{F}$. Let $\mathscr{C} = \{x_1, x_2, \mathbf{N}_A(x_3), f\}$ and think of the inclusion $\mathbf{F}[\mathscr{C}] \subset \mathbf{F}[V]^{\langle A,C\rangle} \subset \mathbf{F}[V]^{\langle A\rangle}$. Since $\mathbf{N}_A(x_4)$ and f have the same lead term we have $\mathbf{F}[V]^{\langle A\rangle} = \mathbf{F}[x_1, x_2, \mathbf{N}_A(x_3), f_1, f]$. The latter implies $\mathbf{F}[\mathscr{C}][f_1] = \mathbf{F}[V]^{\langle A\rangle}$, thus $\mathbf{F}[V]^{\langle A,C\rangle}[f_1] = \mathbf{F}[V]^{\langle A\rangle}$. However from Galois theory we know $[\mathbf{F}(V)^{\langle A\rangle} : \mathrm{Quot}(\mathbf{F}[\mathscr{C}])] = |\langle A, C\rangle|/|\langle A\rangle| = p$ and this is a contradiction. A basis for the field $\mathbf{F}(V)^{\langle A\rangle}$ as a $\mathrm{Quot}(\mathbf{F}[\mathscr{C}])$-vector space is given by the set of secondary invariants, which in our case is just the singleton $\{f_1\}$. So such an invariant f cannot exist.

To prove the first part of our claim, we work modulo $\langle x_1^p\rangle \triangleleft \mathbf{F}[V]$. Follows immediately that $\mathbf{N}_A(x_3)^2 \equiv_{\langle x_1^p\rangle} x_3^{2p} - 2x_3^{p+1}x_1^{p-1}$. Regarding $\mathbf{N}_C(f_1)$, observe that every term but the leading contain a copy of x_1^{p-1}. Among them there is a unique with x_1^{p-1} in its expression, namely $x_3^2x_2^{p-1}x_1^{p-1}$. Thus $\mathbf{N}_C(f_1) \equiv_{\langle x_1^p\rangle} x_3^{2p} + x_3^2x_2^{p-1}x_1^{p-1}$. So our claim follows: $\mathrm{LT}(\widetilde{g_1}) = 2x_1^{p-1}x_3^{p+1}$. □

Set $g_1 := \widetilde{g_1}/2x_1^{p-1}$. We shall use g_1 to construct the minimum x_4-degree H-invariant.

From [8, Corollary 3.1.6] follows that the $\langle C\rangle$-action on $\mathbf{F}[V]$ yields: $\mathbf{F}[V]^{\langle C\rangle} = \mathbf{F}[x_1, x_2, x_3, \mathbf{N}_C(x_4)]$. Using the inclusion $\mathbf{F}[V]^H \subset \mathbf{F}[V]^{\langle C\rangle}$, shows that the minimum x_4-degree H-invariant has x_4-degree p. Therefore, an H-invariant with x_4-degree exactly p is a generator of $\mathbf{F}(V)^H$.

Lemma 4.2.1.8. *The polynomial*

$$\begin{aligned}\overline{f} &:= ((p-1)/2\cdot b_{1,2}^p x_1 + (p+1)/2\cdot x_2)\mathbf{N}_A^2(x_3) - (x_2^p - x_1^{p-1}x_2)g_1\\ &+ (((p+1)/2\cdot b_{1,2}^p + (p-1)/2\cdot b_{1,2})x_1x_2^p + (b_{1,2}^{p-1}b_{1,4} - b_{14}^p)x_1^{p+1})\mathbf{N}_A(x_3)\\ &+ \left\{\sum_{j=0}^{p-2}((p-1)/2\cdot b_{1,2}^{p-j} + (p+1)/2\cdot b_{1,2}^{p-1-j} + b_{1,2}^{p-2-j}b_{1,4})x_1^{p-j}x_2^{j+1}\right\}\mathbf{N}_A(x_3),\end{aligned}$$

forms an H-invariant of minimum x_4-degree with lead term $\mathrm{LT}(\overline{f}) := (p+1)/2\cdot x_3^{2p}x_2$.

Proof. Reducing g_1 modulo $\langle x_1\rangle \lhd \mathbf{F}[V]^H$ gives: $g_1 \equiv_{\langle x_1\rangle} x_3^{p+1} + (p-1)/2\cdot x_3^2x_2^{p-1}$. Now it is easy to see that

$$\overline{f} \equiv_{\langle x_1\rangle} x_2\mathbf{N}_A^2(x_3) - x_2^p g_1 \equiv_{\langle x_1\rangle} (p+1)/2\cdot x_3^{2p}x_2 - x_3^{p+1}x_2^p - (p-1)/2\cdot x_3^2x_2^{2p-1},$$

and our claim follows, $\mathrm{LT}(\overline{f}) = (p+1)/2\cdot x_3^{2p}x_2$.

Clearly $\overline{f}$ is an A-invariant. Applying the twisted derivation $\Delta_B = B - 1 \in \mathbf{F}H$ gives $\Delta_B(\mathbf{N}_A(x_3)) = \mathbf{N}_A(x_3) + x_2^p - x_1^{p-1}x_2$ and

$$\begin{aligned}\Delta_B(g_1) &= (b_{1,2}^{p-1}b_{1,4} - b_{14}^p)x_1^{p+1} + ((p+1)/2\cdot b_{1,2}^{p-1} + b_{1,2}^{p-2}b_{1,4})x_1^px_2 + (p-1)/2\cdot x_1^{p-1}x_2^2\\ &+ (p-1)/2\cdot b_{1,2}x_1x_2^p + (p+1)/2\cdot x_2^{p+1} - b_{1,2}^p x_1\mathbf{N}_A(x_3) + x_2\mathbf{N}_A(x_3)\\ &+ \sum_{j=1}^{p-2}((p-1)/2\cdot b_{1,2}^{p-j} + (p+1)/2\cdot b_{1,2}^{p-1-j} + b_{1,2}^{p-2-j}b_{1,4})x_1^{p-j}x_2^{j+1}.\end{aligned}$$

Plugging into $\Delta_B(\overline{f})$ these expressions returns zero. Thus $\overline{f} \in \mathbf{F}[V]^H$. □

Set $f := 2\overline{f}$. It is not difficult to see that for $f \in \mathbf{F}[x_1, x_2, x_3][x_4]$, the leading coefficient is: $\mathrm{LC}(f) = 2(x_1x_2^p - x_1^px_2)$. Furthermore, since the H-action on the first three variables is Nakajima, $\{x_1, x_2, \mathbf{N}_H(x_3)\}$ forms a set of minimum degree invariants in the first three variables. Now we obtain the following theorem.

Theorem 4.2.1.9. $\mathbf{F}(V)^H = \mathbf{F}(x_1, x_2, \mathbf{N}_H(x_3), f)$. *Furthermore, we have an equality of rings* $\mathbf{F}[V]^H[l^{-1}] = \mathbf{F}[x_1, x_2, \mathbf{N}_H(x_3), f][l^{-1}]$, *where* $l = x_2^px_1 - x_2x_1^p$ *and* $\mathrm{LT}(\mathbf{N}_H(x_3)) = x_3^{p^2}, \mathrm{LT}(f) = x_3^{2p}x_2$.

Proof. Both equalities follow as an application of Theorem 1.4.2.6. □

Remark 4.2.1.10. *The invariant l showing up above is a rather interesting and well-known example of invariant. We have $\mathbf{F}_p[x_1, x_2]^{\mathrm{SL}_2(\mathbf{F}_p)} = \mathbf{F}_p[l, d_{1,2}]$, where $d_{1,2} = \frac{x_1 x_2^{p^2} - x_1^{p^2} x_2}{x_1 x_2^p - x_1^p x_2}$, denotes the Dickson invariant.*

4.2.2 Non Cohen-Macaulyness of $\mathbf{F}[V]^H$

Our next step is to investigate the structure of $\mathbf{F}[V]^H$. Using MAGMA for small primes reveals high computational complexity with the number of tête-à-tête subductions increasing significantly at each step. From our experience this implies that $\mathbf{F}[V]^H$ is not Cohen-Macaulay. In this section we present computational evidence that for $p = 3, 5$ and 7 this claim is true.

In particular, when $p = 3$ we are able to compute explicitly a generating set of $\mathbf{F}[V]^H$ and with a simple counting argument prove that is not Cohen-Macaulay. For $p = 5, 7$, although MAGMA does not return a generating set we prove the existence of a partial hsop which fails to be a regular sequence.

More analytically, set $\mathscr{H} := \{x_1, x_2, \mathbf{N}_B(g_1)\}$ where the last element denotes the B-norm of g_1. Since $\mathrm{LT}(\mathbf{N}_B(g_1)) = x_3^{p(p+1)}$, from [8, Lemma 2.6.3] follows that $\mathscr{H}$ is a partial hsop. We shall prove that exist invariants $u_1, u_2 \in \mathbf{F}[V]^H$, such that

$$u_1\, \mathbf{N}_B(g_1) + u_2\, x_2 \in (x_1)\mathbf{F}[V]^H \tag{4.2.1}$$

for every prime p and that for $p = 5, 7$ we have $u_1 \notin (x_1, x_2)\mathbf{F}[V]^H$. This will show that $\mathscr{H}$ does not act regularly on $\mathbf{F}[V]^H$ for these primes.

Observe that there is a tête-à-tête: $(\mathbf{N}_B(g_1) f^{p-1/2}, \mathbf{N}_H^2(x_3) x_2^{p-1/2})$. We claim that subducting this tête-à-tête constructs (4.2.1).

Lemma 4.2.2.1. *Subducting $(\mathbf{N}_B(g_1) f^{p-1/2}, \mathbf{N}_H^2(x_3) x_2^{p-1/2})$ yields invariants $u_1, u_2 \in \mathbf{F}[V]^H$ such that $u_1\, \mathbf{N}_B(g_1) + u_2\, x_2 \in (x_1)\mathbf{F}[V]^H$.*

Proof. Set $s := \mathbf{N}_B(g_1) f^{p-1/2} - x_2^{p-1/2} \mathbf{N}_H^2(x_3)$. To find out the lead term of s we work modulo $\langle x_1 \rangle \lhd \mathbf{F}[V]$.

Follows easily that: $\mathbf{N}^2_H(x_3)x_2^{p-1/2} \equiv_{\langle x_1\rangle} x_3^{2p^2}x_2^{p-1/2} - 2x_3^{p^2+p}x_2^{(2p^2-p-1)/2} + x_3^{2p}x_2^{(4p^2-3p-1)/2}$. Recall from Lemma 4.2.1.8, $g_1 \equiv_{\langle x_1\rangle} x_3^{p+1} + (p-1)/2 \cdot x_3^2x_2^{p-1}$, and from the explicit description of $\Delta_B(g_1)$ that we have: $g_1 \cdot B \equiv_{\langle x_1\rangle} x_3^{p+1} + x_3^p x_2 + (p-1)/2 \cdot x_3^2x_2^{p-1} + (p+1)/2 \cdot x_2^{p+1}$. More generally, we compute that: $g_1 \cdot B^i \equiv_{\langle x_1\rangle} x_3^{p+1} + ix_3^px_2 + (p-1)/2 \cdot x_3^2x_2^{p-1} + c_ix_2^{p+1}$, where $c_0 := (p-1)/2, c_1 = (p+1)/2$, $c_i = c_{i-1} + i + (p-1)/2, i \geq 2$, or alternatively $c_i = \sum_{j=1}^{i} j + i \cdot c_0, i \geq 1$. We claim that $\prod_{i=1}^{p-1} c_i = 1$. Since each c_i can be written as a multiple of c_0, $c_i = -i^2c_0$, $\forall i \geq 1$, follows that $\prod_{i=1}^{p-1} -i^2c_0 = \left(\prod_{i=1}^{p-1} i^2\right)c_0^{p-1} = 1$.

Using this observation we obtain a description of the norm

$$\begin{aligned} \mathbf{N}_B(g_1) \;\equiv_{\langle x_1\rangle}\;& x_3^{p(p+1)} - x_3^{p^2+1}x_2^{p-1} + \lambda_1 \cdot x_3^{2p}x_2^{p(p-1)} + \lambda_2 \cdot x_3^{p+1}x_2^{p^2-1} \\ +\;& (p-1)/2 \cdot x_3^2x_2^{(p+2)(p-1)}, \end{aligned}$$

where

$$\begin{aligned} \lambda_1 \;&:=\; \frac{p-1}{2} + \sum_{1\leq i_1<\ldots<i_{(p-1)/2}\leq p-1} \left(\frac{p-1}{2}\right)^{(p-1)/2} c_{i_1}c_{i_2}\ldots c_{i_{(p-1)/2}} \\ &+\; \sum_{j=1}^{p-1}\left\{\sum_{S_j}\left(\frac{p-1}{2}\right)^{(p-1)/2} c_{i_1}c_{i_2}\ldots c_{i_{(p-1)/2}}\right\}, \\ \lambda_2 \;&:=\; 1 + \sum_{1\leq i_1<\ldots<i_{(p-1)/2}\leq p-1} \left(\frac{p-1}{2}\right)^{(p+1)/2} c_{i_1}c_{i_2}\ldots c_{i_{(p-1)/2}}, \end{aligned}$$

with $S_j = \{1 \leq i_1 < \ldots < i_{(p-1)/2} \leq p-1 \,|\, i_1, \ldots, i_{(p-1)/2} \neq j\}$. We claim that λ_1, λ_2 can be simplified significantly. First off, $|S_j| := |S|/2$ where $|S| = \binom{p-1}{\frac{p-1}{2}}$. Thus $(p-1) \cdot |S| = (p-1)/2 \cdot |S|$. In fact, in the second sum of λ_1, each summand appears precisely $(p-1)/2$ times. Therefore,

$$\sum_{j=1}^{p-1}\left\{\sum_{S_j} c_0^{(p-1)/2} c_{i_1}c_{i_2}\ldots c_{i_{(p-1)/2}}\right\} = \frac{p-1}{2} \cdot \sum_{1\leq i_1<\ldots<i_{(p-1)/2}\leq p-1} c_0^{(p-1)/2} c_{i_1}c_{i_2}\ldots c_{i_{(p-1)/2}}.$$

That is,

$$\begin{aligned} \lambda_1 \;&:=\; \frac{p-1}{2} + \frac{p+1}{2} \cdot \sum_{1\leq i_1<\ldots<i_{(p-1)/2}\leq p-1} c_0^{(p-1)/2} c_{i_1}c_{i_2}\ldots c_{i_{(p-1)/2}}, \\ \lambda_2 \;&:=\; 1 + \frac{p-1}{2} \cdot \sum_{1\leq i_1<\ldots<i_{(p-1)/2}\leq p-1} c_0^{(p-1)/2} c_{i_1}c_{i_2}\ldots c_{i_{(p-1)/2}}. \end{aligned}$$

Our goal is to determine λ_1, λ_2. Let Δ_B denote the twisted derivation corresponding to B. Then we calculate $\Delta_B^3(g_1) = 0$. Therefore, for $X = \Delta_B^2(g_1), Y = \Delta_B(g_1), Z = g_1$, the set $\{X, Y, Z\}$ defines a basis for a three-dimensional left $\mathbf{FZ}/p$-module. From [20][Lemma 6.1], we know that in such case an explicit description of $\mathbf{N}_B(g_1) = A_0 + A_1X + ... + A_{p-2}X^{p-2}$, with $A_i \in \mathbf{F}[Y, Z]$ can be given. Furthermore, we know that each A_i has the following combinatorial description

$$A_i = \begin{cases} \sum_{k=1}^{i+1} \xi_{i,k} Z^k Y^{p-i-k}, \ \textit{for } 1 \le i \le (p-1)/2 \\ \sum_{k=1}^{p-i} \xi_{i,k} Z^k Y^{p-i-k}, \ \textit{for } (p+1)/2 \le i \le p-2, \end{cases}$$

where

$$A_0 = Z^p - ZY^{p-1}, \xi_{i,k} = \frac{(-1)^i}{2^i(p-k)} \binom{p-2k+1}{i-k+1} \binom{p-k}{k-1}.$$

We shall exploit the above description and the coefficients $\xi_{i,k}$ to compute λ_1. First off, we compute that modulo $\langle x_1 \rangle$ we have: $Y \equiv_{\langle x_1 \rangle} x_3^p x_2 + (p+1)/2 \cdot x_2^{p+1}, X \equiv_{\langle x_1 \rangle} x_2^{p+1}$, whereas earlier we computed also: $Z \equiv_{\langle x_1 \rangle} x_3^{p+1} + (p-1)/2 \cdot x_3^2 x_2^{p-1}$. We claim that for $i > 0$ there is only one term in the expansion of $\mathbf{N}_B(g_1)$ above, which contains $x_3^{2p} x_2^{p(p-1)}$. Pick an arbitrary summand: $Z^k Y^{p-i-k} X^i$. To track down where $x_3^{2p} x_2^{p(p-1)}$ lies, suffices to understand what k, i construct such term. Explicitly we have

$$\begin{aligned} Z^k \quad &\equiv_{\langle x_1 \rangle} \quad \sum_{j=0}^{k} \binom{k}{j} \left(\frac{p-1}{2}\right)^j \cdot x_3^{(p+1)(k-j)} x_2^{(p-1)j}, \\ Y^{p-i-k} \quad &\equiv_{\langle x_1 \rangle} \quad \sum_{\omega=0}^{p-i-k} \binom{p-i-k}{\omega} \left(\frac{p+1}{2}\right)^\omega \cdot x_3^{p(p-i-k-\omega)} x_2^{(p+1)\omega+(p-i-k)-\omega}. \end{aligned}$$

To obtain $x_3^{2p} x_2^{p(p-1)}$, we must have $p^2 - (\omega + j + i)p + (k + j) = 2p$ $(*)$, for suitable choices of $\omega, j \in \mathbb{Z}^+, k \ge 1$. Observe that always $\omega + j + i \le p - i - k + j + i \le p$, therefore $\omega + j + i = p - \lambda$, for $0 \le \lambda \le p - 1$. Let $1 \le i \le (p-1)/2$; since $k \le i + 1 = (p+1)/2$, follows that $k + j \le p + 1$ and if $(*)$ holds, we must have $\omega + j + i = p - 1, k + j = p$. The last equality implies: $k = (p+1)/2, j = (p-1)/2$. The latter along with the initial assumption $1 \le i \le (p-1)/2$, gives $i = (p-1)/2$. So the only summand which contains the above term is $\xi_{(p-1)/2,(p+1)/2} Z^{(p+1)/2} X^{(p-1)/2}$. Let now $(p+1)/2 \le i \le p-2$; then $k \le (p-1)/2$, hence $k + j \le p - 1$. From the last now, it is straightforward that for such i, $(*)$ can never hold. Finally, for $i = 0$ we observe that in A_0, Z^p contains $x_3^{2p} x_2^{p(p-1)}$ as well. Thus to determine λ_1 suffices to sum up the coefficients of the corresponding terms. We compute $\xi_{(p-1)/2,(p+1)/2} = (-1)^{(p+1)/2}/2^{(p-3)/2}$, while for $k = (p+1)/2, j = (p-1)/2$, the coefficient of $x_3^{2p} x_2^{p(p-1)}$ in $Z^{(p+1)/2} X^{(p-1)/2}$ is $((p-1)/2)^{(p-1)/2}(p+1)/2$. Therefore,

$$\lambda_1 = \xi_{(p-1)/2,(p+1)/2} \cdot \left(\frac{p-1}{2}\right)^{(p-1)/2} \cdot \frac{p+1}{2} + \frac{p-1}{2}.$$

All together yields $\lambda_1 = (p-3)/2$.

The last implies

$$\sum_{1 \leq i_1 < \ldots < i_{(p-1)/2} \leq p-1} c_0^{(p-1)/2} c_{i_1} c_{i_2} \ldots c_{i_{(p-1)/2}} = -2.$$

Therefore, substituting that to λ_2 yields: $\lambda_2 = 2$.

Now we return back to our initial claim. From the previous lemma again follows that: $f \equiv_{\langle x_1 \rangle} x_3^{2p} x_2 - 2x_3^{p+1} x_2^p + x_3^2 x_2^{2p-1}$. Expanding $f^{p-1/2}$, we obtain modulo $\langle x_1 \rangle$:

$$f^{p-1/2} \equiv_{\langle x_1 \rangle} \sum_{j=0}^{p-1} x_3^{p(p-1)-j(p-1)} x_2^{p-1/2+j(p-1)}.$$

Working out the terms of the product $\mathbf{N}_B(g_1) f^{p-1/2}$ we observe that

$$\begin{aligned} \mathbf{N}_B(g_1) f^{p-1/2} \quad \equiv_{\langle x_1 \rangle} \quad & x_3^{2p^2} x_2^{p-1/2} + (\lambda_1 - 1) \cdot x_3^{p(p+1)} x_2^{2p^2-p-1/2} \\ + \quad & (\lambda_1 + \lambda_2) \cdot x_3^{p^2+1} x_2^{2p^2+p-3/2} + (\lambda_2 + (p-1)/2) \cdot x_3^{2p} x_2^{4p^2-3p-1} \\ + \quad & (p-1)/2 \cdot x_3^{p+1} x_2^{4p^2-p-3/2}. \end{aligned}$$

Summarizing all the above gives: $\mathrm{LT}(s) = (\lambda_1 + 1) \cdot x_3^{p^2+p} x_2^{(p-1)(2p+1)/2}$.

Set $s_1 := s - (\lambda_1 + 1) \cdot x_2^{(p-1)(2p+1)/2} \mathbf{N}_B(g_1)$. As previously we work modulo $\langle x_1 \rangle \lhd \mathbf{F}[V]$. Observe that the third term of $\mathbf{N}_B(g_1) f^{p-1/2}$ vanishes with the second of $\mathbf{N}_B(g_1) x_2^{(p-1)(2p+1)/2}$ since $2\lambda_1 + \lambda_2 + 1 = 0$. Therefore $\mathrm{LT}(s_1) = ((p-1)/2 - \lambda_1(\lambda_1 + 1) + 1) \cdot x_3^{2p} x_2^{4p^2-3p-1/2} = (2 - (p-3)^2/4) \cdot x_3^{2p} x_2^{4p^2-3p-1/2}$.

Finally, we set $s_2 := s_1 - (2 - (p-3)^2/4) \cdot x_2^{(4p^2-3p-3)/2} f$. We claim that every term in s_2 contains an x_1-power. From previous steps we know that the only remaining terms modulo $\langle x_1 \rangle$ must be $x_3^{p+1}x_2^{4p^2-p-3/2}$ and $x_3^2 x_2^{(p+2)(p-1)}$. For the last monomial, observe that in s_2 the coefficient is $(\lambda_1 + 1/2 - (2-(p-3)^2/4)$ and equals zero. Regarding the former, adding up all the corresponding terms in s_2 yields: $(p - 1/2 - (\lambda_1+1)\lambda_2 + 2(2-(p-3)^2/4))$. Working out this coefficient gives zero too. Therefore $s_2 \equiv_{\langle x_1 \rangle} 0$. Now our claim follows. $\square$

Define $u_1 := f^{p-1/2}, u_2 := -x_2^{p-3/2}\mathbf{N}_H^2(x_3) + 1/2 \cdot x_2^{\frac{2p^2-p-3}{2}}\mathbf{N}_B^2(g_1) + 1/4 \cdot x_2^{\frac{4p^2-3p-5}{2}} f$ to be the invariants of equation (4.2.1).

In the beginning of the section we said that for $p = 3$ on MAGMA we can make explicit computations. Using `FundamentalInvariants`() command and randomly assigned variables we can compute a generating set for $\mathbf{F}[V]^H$. Therefore with this setup we will see that $\mathbf{F}[V]^H$ is not Cohen-Macaulay by a simple counting argument. Regarding the claim $u_1 \notin (x_1, x_2)\mathbf{F}[V]^H$ when $p = 5, 7$, we exploit the linear algebra method on MAGMA (see, [9, 3.1.1]) which computes an $\mathbf{F}$-vector space basis of $\mathbf{F}[V]_d^H$, $\forall d > 0$. To prove that $u_1 \notin (x_1, x_2)\mathbf{F}[V]^H$ for these primes our strategy is the following. Assuming the contrary implies that $u_1 = x_1h_1 + x_2h_2$, for $h_1, h_2 \in \mathbf{F}[V]^H$ with h_2 homogeneous of degree $\deg(h_2) = (2p^2 - p - 3)/2$ and $\mathrm{LT}(h_2) = x_3^{p(p-1)}x_2^{p-3/2}$. Thus, to prove our assertion suffices for these primes to show that $h_2 \notin \mathbf{F}[V]_d^H$ for $d := (2p^2 - p - 3)/2$.

For the computations below we worked over the field `F<t>:=GF`(p^r), for $r :=$ 2 with $c_{1,2}, c_{2,4}$:= `Random(F)` being random over `F` and the polynomial ring `S<x4,x3,x2,x1>:=PolynomialRing(F,4,"grevlex")`. Furthermore, we use the command `InvariantsOfDegree()` to compute an $\mathbf{F}$-basis of $\mathbf{F}[V]_d^H$.

Case $p = 5$: Here we have $d = 21$, $\mathrm{LT}(h_2) = x_3^{20}x_2$. `InvariantsOfDegree()` returns a list of 33 basis element for $\mathbf{F}[V]_{21}^H$ with the following lead terms:

$$\{x_3^{10}x_2^{11-i}x_1^i \mid i = 0, \dots, 10\}, \{x_2^{21-i}x_1^i \mid i = 0, \dots, 21\}.$$

Since any homogeneous invariant in $\mathbf{F}[V]_{21}^H$ is a linear combination of these basis elements, assuming $h_2 \in \mathbf{F}[V]_{21}^H$ implies that among them there is one with the same lead term. However, $x_3^{20}x_2$ is not in the above sets. Therefore, $u_1 \notin (x_1, x_2)\mathbf{F}[V]^H$.

Case $p = 7$: This time $d = 44$, $\mathrm{LT}(h_2) = x_3^{42}x_2^2$ and `InvariantsOfDegree()` returns a list of 90 generators for $\mathbf{F}[V]_{44}^H$ with lead terms:

$$\{x_3^{28}x_2^{16-i}x_1^i \mid i = 0, \ldots, 14\}, \{x_3^{14}x_2^{30-i}x_1^i \mid i = 0, \ldots, 29\}, \{x_2^{44-i}x_1^i \mid i = 0, \ldots, 44\}.$$

Likewise, assuming $h_2 \in \mathbf{F}[V]_{44}^H$ implies that a basis element with lead term $x_3^{42}x_2^2$ exists. However this is clearly a contradiction again, therefore $u_1 \notin (x_1, x_2)\mathbf{F}[V]^H$.

So for $p = 5$ and 7 there is evidence that $\{x_1, x_2, \mathbf{N}_B(g_1)\}$ is an hsop which is not a regular sequence, hence [8, Theorem 2.8.1] implies that $\mathbf{F}[V]^H$ is not Cohen-Macaulay with this setup.

Finally we examine the case $p = 3$. Using the same MAGMA setup, the command `FundamentalInvariants()` returns a set of eleven invariants $\{t_1, t_2, ..., t_{11}\}$ with lead terms

$$\begin{array}{llll} \mathrm{LT}(t_1) = x_1, & \mathrm{LT}(t_2) = x_2, & \mathrm{LT}(t_3) = x_3^6x_2, & \mathrm{LT}(t_4) = x_3^9, \\ \mathrm{LT}(t_5) = x_3^{10}x_2, & \mathrm{LT}(t_6) = x_3^{12}, & \mathrm{LT}(t_7) = x_3^{16}, & \mathrm{LT}(t_8) = x_3^{20}, \\ \mathrm{LT}(t_9) = x_3^{22}, & \mathrm{LT}(t_{10}) = x_3^{26}, & \mathrm{LT}(t_{11}) = x_4^{27}, & \end{array}$$

such that $\mathbf{F}[V]^H = \mathbf{F}[t_1, ..., t_{11}]$. Since $\{x_1, x_2, \mathbf{N}_H(x_3), \mathbf{N}_H(x_4)\}$ is always an hsop we compute the secondary invariants over $\mathbf{F}[x_1, x_2, \mathbf{N}_H(x_3), \mathbf{N}_H(x_4)]$. Using the command `SecondaryInvariants()` gives back again eleven-invariants with lead terms

$$\begin{array}{llll} \mathrm{LT}(g_1) = 1, & \mathrm{LT}(g_2) = x_3^6x_2, & \mathrm{LT}(g_3) = x_3^{10}x_2, & \mathrm{LT}(g_4) = x_3^{12}, \\ \mathrm{LT}(g_5) = x_3^{16}, & \mathrm{LT}(g_6) = x_3^{20}, & \mathrm{LT}(g_7) = x_3^{22}, & \mathrm{LT}(g_8) = x_3^{24}, \\ \mathrm{LT}(g_9) = x_3^{26}, & \mathrm{LT}(g_{10}) = x_3^{28}, & \mathrm{LT}(g_{11}) = x_3^{32}. & \end{array}$$

such that

$$\mathbf{F}[V]^H = \sum_{i=1}^{11} \mathbf{F}[x_1, x_2, \mathbf{N}(\mathrm{x}_3), \mathbf{N}(\mathrm{x}_4)]g_{\mathrm{i}}.$$

The fact that $\mathbf{F}[V]^H$ is not Cohen-Macaulay has been reflected already. Being Cohen-Macaulay over a finitely generated algebra $R = \mathbf{F}[h_1, ..., h_n]$, where

$\deg(h_i) = d_i$, is equivalent to

$$|\{\textit{minimal generating set of } \mathbf{F}[V]^H \textit{ as R-module}\}| = \prod_{i=1}^{n} d_i \Big/ |H|.$$

In our case the left-hand side is eleven, while the right-hand side $9 \cdot 27/27 = 9$. So follows by a simple counting argument that $\mathbf{F}[V]^H$ is not Cohen-Macaulay.

Summarizing all the above we conjecture the following.

Conjecture 4.2.2.2. *Let p be an odd prime. Then the ring of invariants $\mathbf{F}[V]^H$ is not Cohen-Macaulay with the partial homogeneous system of parameters $\{x_1, x_2, \mathbf{N}_B(g_1)\}$ acting non-regularly for $p > 3$.*

4.3 Invariants of type-(1,2,1) representations.

4.3.1 Introduction

In this section we investigate invariants of type-$(1, 2, 1)$ representations. We remind that for this type we can only have representations with one of the following socle-tabloids.

$$\begin{array}{l} \boxed{3} \\ \boxed{2}\boxed{1} \\ \boxed{1} \end{array} \qquad \begin{array}{l} \boxed{3} \\ \boxed{2}\boxed{2} \\ \boxed{1} \end{array}$$

For simplicity we will refer to the left tabloid by $(3, 21, 1)$ and the right by $(3, 22, 1)$.

In each case we show that the group of representing matrices is generated by bireflections and we compute the invariant field $\mathbf{F}(V)^H$. Furthermore, for representations with socle-tabloid $(3, 21, 1)$ we present computational evidence that the invariants are not Cohen-Macaulay, while for those with socle-tabloid $(3, 22, 1)$ evidence that $\mathbf{F}[V]^H$ is a complete intersection.

4.3.2 Invariants of type-$(1,2,1)$ with socle-tabloid: $(3,21,1)$

Suppose V is a four-dimensional $\mathbf{F}H$-module of type-$(1,2,1)$ with socle-tabloid $(3,21,1)$. From Theorem 2.5.0.5 there is a choice of basis $\mathscr{B}$, such that the group of representing matrices $\rho_{\mathscr{B}}(H)$ is generated by the following matrices

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b_{1,2} & 1 & b_{1,4} \\ 0 & 1 & 0 & b_{2,4} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

subject to the condition $b_{1,2} - b_{2,4} \neq 0$, with commutator

$$C = [A,B] = ABA^{-1}B^{-1} = \begin{bmatrix} 1 & 0 & 0 & b_{2,4} - b_{1,2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Before we proceed to explicit computations we observe the following.

Lemma 4.3.2.1. *The group $\rho_{\mathscr{B}}(H)$ is a bireflection group.*

Proof. Suppose $\mathscr{B} := \{e_1, e_2, e_3, e_4\}$. To prove our assertion suffices to show that the null space of the nilpotent part of each generator is at least two-dimensional. For A follows immediately that $\dim_{\mathbf{F}}(\ker(A - I)) = \mathrm{Span}_{\mathbf{F}}\{e_1, e_3\}$, while for B it is not difficult to see that $\dim_{\mathbf{F}}(\ker(B - I)) = \mathrm{Span}_{\mathbf{F}}\{e_1, e_2 - b_{1,2}e_3\}$. Hence our assertion follows. □

Now we investigate the structure of $\mathbf{F}[V]^H$. In Lemma 4.3.2.3 we describe the invariant field $\mathbf{F}(V)^H$ and we use the invariant field generators to present evidence that $\mathbf{F}[V]^H$ is not Cohen-Macaulay.

Recall from type-$(1,1,2)$ case that $\mathbf{F}[V]^{\langle A \rangle} = \mathbf{F}[x_1, x_2, \mathbf{N}_A(x_3), f_1, f_2]$, where

$$f_1 = x_3^2 - 2x_4x_1 - x_1x_3, \quad f_2 = \textsc{subd}(f_1^p - \mathbf{N}_A(x_3), [x_1, x_2, f_1, \mathbf{N}_A(x_3)]).$$

Localizing at x_1 gives $\mathbf{F}[V]^{\langle A\rangle}[x_1^{-1}] = \mathbf{F}[x_1, x_2, \mathbf{N}_A(x_3), f_1][x_1^{-1}]$. Hence shifting the generators to degree one $y_1 = \mathbf{N}_A(x_3)/x_1^{p-1}$, $y_2 = f_1/x_1$ and applying the quotient group $\langle A, C\rangle/\langle A\rangle \cong \langle C\rangle$ yields

$$\mathbf{F}[V]^{\langle A,C\rangle}[x_1^{-1}] = \mathbf{F}[x_1, x_2, y_1, y_2]^{\langle C\rangle}[x_1^{-1}]. \tag{4.3.1}$$

The action of C now is on a polynomial algebra and on this new basis we have

$$x_1.C = x_1, \quad x_2.C = x_2,$$
$$y_1.C = y_1, \quad y_2.C = y_2 - 2(b_{2,4} - b_{1,2})x_1.$$

Using [8, Corollary 3.1.6] we obtain $\mathbf{F}[x_1, x_2, y_1, y_2]^{\langle C\rangle} = \mathbf{F}[x_1, x_2, y_1, \mathbf{N}_C(y_2) = y_2^p - (b_{2,4} - b_{1,2})^{p-1}x_1^{p-1}y_2]$. Substituting in equation (4.3.1) and clearing the denominators minimally gives

$$\mathbf{F}[V]^{\langle A,C\rangle}[x_1^{-1}] = \mathbf{F}[x_1, x_2, \mathbf{N}_A(x_3), w_1 := f_1^p - (b_{2,4} - b_{1,2})^{p-1}x_1^{2(p-1)}f_1][x_1^{-1}].$$

In the resulting set of invariants $\{x_1, x_2, \mathbf{N}_A(x_3), w_1\}$, there is only one non-trivial tête-à-tête : $(\mathbf{N}_A^2(x_3), w_1)$.

Lemma 4.3.2.2. *Subducting the tête-à-tête* $(w_1, \mathbf{N}_A^2(x_3))$ *gives an invariant with lead term:* $2x_3^{p+1}x_1^{p-1}$.

Proof. The lead term of the tête-à-tête difference is $\mathrm{LT}(w_1 - \mathbf{N}_A^2(x_3)) = 2x_3^{p+1}x_1^{p-1}$. Since it cannot subduct more against $\{x_1, x_2, \mathbf{N}_A(x_3), w_1\}$ our claim follows. □

Define $u_1 := (w_1 - \mathbf{N}_A^2(x_3))/2x_1^{p-1}$. Expanding the definition of u_1 gives

$$\begin{aligned} u_1 &= x_3^{p+1} - x_4^p x_1 + (p-1)/2 \cdot x_3^p x_1 + ((b_{2,4} - b_{1,2})^{p-1} + 1)(p-1)/2 \cdot x_1^{p-1}x_3^2 \\ &+ (b_{2,4} - b_{1,2})^{p-1}x_4 x_1^p + (b_{2,4} - b_{1,2})^{p-1}(p+1)/2 \cdot x_3 x_1^p. \end{aligned}$$

We shall use u_1 to describe the minimum x_4-degree H-invariant. From [8, Corollary 3.1.6] again, the $\langle C\rangle$-action on $\mathbf{F}[V]$ gives $\mathbf{F}[V]^{\langle C\rangle} = \mathbf{F}[x_1, x_2, x_3, \mathbf{N}_C(x_4) = x_4^p - (b_{1,2} - b_{2,4}) \cdot x_1^{p-1}x_4]$. So the inclusion $\mathbf{F}[V]^H \subset \mathbf{F}[V]^{\langle C\rangle}$ implies that the minimum x_4-degree H-invariant has degree at least p. Thus suffices to construct an H-invariant with x_4-degree exactly p. For the remaining generators of $\mathbf{F}(V)^H$ observe that H acts on the first three variables as a Nakajima group, hence $\{x_1, x_2, \mathbf{N}_H(x_3)\}$ form minimum degree invariants on the first three variables.

Theorem 4.3.2.3. *Assume $b_{2,4} \in \mathbf{F} \setminus \mathbf{F}_p$. Then the H-invariant*

$$h_1 = \gamma_1 \cdot x_1^p \mathbf{N}_A(x_3) + \gamma_2 \cdot x_1^{p-1} x_2 \mathbf{N}_A(x_3) + \gamma_3 \cdot x_2^p \mathbf{N}_A(x_3) + \gamma_4 \cdot \mathbf{N}_A^2(x_3) - x_1^{p-1} u_1$$

with

$$\begin{aligned}
\gamma_1 &= \left\{ \sum_{i=0}^{p-2} (-b_{1,2}^{p-1-i} b_{1,4} b_{2,4}^i + 1/2 \cdot b_{1,2}^{p-1-i} b_{2,4}^{2+i} - 1/2 \cdot b_{1,2}^{p-1-i} b_{2,4}^{i+1}) \right\} + b_{1,4}^p - b_{1,4} b_{2,4}^{p-1} \\
&- 1/2 \cdot b_{1,2}^p (b_{2,4}^p - b_{2,4})/(b_{2,4}^p - b_{2,4}), \\
\gamma_2 &= (b_{1,2} - b_{2,4})^{p-1}/(b_{2,4}^p - b_{2,4}), \gamma_3 = -1/(b_{2,4}^p - b_{2,4}), \gamma_4 = (b_{1,2}^p - b_{2,4})/2(b_{2,4}^p - b_{2,4}),
\end{aligned}$$

is of minimum x_4-degree with $\mathrm{LC}_{x_4}(h_1) = x_1^p$. Therefore, $\mathbf{F}(V)^H = \mathbf{F}(x_1, x_2, \mathbf{N}_H(x_3), h_1)$ and we have an equality of rings: $\mathbf{F}[V]^H[x_1^{-1}] = \mathbf{F}[x_1, x_2, \mathbf{N}_H(x_3), h_1][x_1^{-1}]$.

Proof. Obviously $h_1 \in \mathbf{F}[V]^{\langle A \rangle}$. Applying the twisted B-derivation yields $\Delta_B(h_1) = 0$, hence $h_1 \in \mathbf{F}[V]^H$. The equality of fields $\mathbf{F}(V)^H = \mathbf{F}(x_1, x_2, \mathbf{N}_H(x_3), h_1)$ now follows from Theorem 1.4.2.6 since $\deg_{x_4}(h_1) = p$. Finally, notice that the lead term of h_1 as a polynomial in x_4 is x_1^p, thus $\mathbf{F}[V]^H[x_1^{-1}] = \mathbf{F}[x_1, x_2, \mathbf{N}_H(x_3), h_1][x_1^{-1}]$ as an application of Theorem 1.4.2.6 too. □

Expanding the definition of h_1 gives $\mathrm{LT}(h_1) = -(b_{1,2}^p - b_{2,4})/2(b_{2,4}^p - b_{2,4}) \cdot x_3^{2p}$. Set $\mathscr{B} := \{x_1, x_2, \mathbf{N}_H(x_3), h_1\}$. In $\mathscr{B}$ there is a unique non-trivial tête-à-tête : $(h_1^p, \mathbf{N}_H^2(x_3))$. Explicit computations for $p = 3, 5$ and 7 on MAGMA, imply that subducts to an invariant with lead monomial $x_3^p x_2^{p^2}$. However, the number of tête-à-têtes for each of these primes increases significantly at each step. Due to the high computational complexity explicit calculations are infeasible. However, from our experience the latter implies that $\mathbf{F}[V]^H$ is not Cohen-Macaulay. Below we collect evidence for the existence of a partial hsop which does not act regularly for the above primes.

Lemma 4.3.2.4. *Subducting the tête-à-tête $(h_1^p, \mathbf{N}_H^2(x_3))$, yields an invariant with lead term: $-2(b_{2,4}^{p^2} - b_{2,4}^p)/(b_{1,2}^{2p^2} - 2b_{1,2}^{p^2} b_{2,4}^p + b_{2,4}^{2p}) \cdot x_3^p x_2^{p^2} x_1^{p^2-p}$.*

Proof. Expanding the tête-à-tête difference gives $\mathrm{LT}(h_1^p - \mathbf{N}_H^2(x_3)) = 1/2(b_{1,2}^{p^2} - b_{2,4}^p) \cdot x_3^{p^2} x_2^{p^2}$. Suppose $\widetilde{u_1} := h_1^p - \mathbf{N}_H^2(x_3) - 1/2(b_{1,2}^{p^2} - b_{2,4}^p) \cdot x_2^{p^2}\mathbf{N}_H(x_3)$. Set $c_0 := \sum_{i=0}^p b_{2,4}^{p^2-p-i(p-1)}$ for the coefficient of the second term of $\mathbf{N}_H^2(x_3)$ and $c_1 := (b_{1,2}^{p^2} - b_{2,4}^{p^2})/2(b_{1,2}^{p^2} - b_{2,4}^p)$ for the third of h_1^p. Define $c := c_1 - c_0$. Expanding u_1 gives $\mathrm{LT}(u_1) = c \cdot x_3^{p(p+1)} x_2^{p(p-1)}$. Thus for the next step of the subduction we subtract off $c \cdot x_1^{p^2-p} h_1^{\frac{p+1}{2}}$. This time $\mathrm{LT}(u_1 - c \cdot x_1^{p^2-p} h_1^{\frac{p+1}{2}}) = c' \cdot x_3^{p^2} x_2^p x_1^{p^2-p}$, where c' is the difference between the coefficients of the second terms of u_1 and $x_1^{p^2-p} h_1^{\frac{p+1}{2}}$. Carry on that procedure yields the following invariant

$$\widetilde{s_1} := u_1 - c \cdot x_1^{p^2-p} h_1^{\frac{p+1}{2}} + c' \cdot x_1^{p^2-p} x_2^p \mathbf{N}_H(x_3) + \sum_{i=0}^{(p-1)/2} c_i x_1^{p^2-p} x_2^{2(i+1)p} h_1^{\frac{p-1}{2}-i},$$

where c_i is defined similarly to c' for all $i \in \{0, ..., (p-1)/2\}$. Using the definition of each invariant and reducing modulo the ideal $\langle x_1^{p^2-p+1} \rangle \lhd \mathbf{F}[V]$ gives

$$\widetilde{s_1} \equiv_{\langle x_1^{p^2-p+1} \rangle} -2(b_{2,4}^{p^2} - b_{2,4}^p)/(b_{1,2}^{2p^2} - 2b_{1,2}^{p^2} b_{2,4}^p + b_{2,4}^{2p}) \cdot x_3^p x_2^{p^2} x_1^{p^2-p}.$$

Now our assertion follows. □

Define $s_1 := -(b_{1,2}^{2p^2} - 2b_{1,2}^{p^2} b_{2,4}^p + b_{2,4}^{2p})/2(b_{2,4}^{p^2} - b_{2,4}^p) \cdot \widetilde{s_1}$ and $\mathscr{B}' := \{x_1, x_2, \mathbf{N}_H(x_3)\}$. Then $\mathscr{B}'$ is a partial hsop from [8, Lemma 2.6.3]. We are going to use s_1 to provide evidence that for certain primes $\mathscr{B}'$ is not a regular sequence, hence $\mathbf{F}[V]^H$ not Cohen-Macaulay.

Proposition 4.3.2.5. *There exist invariants $g_1, g_2 \in \mathbf{F}[V]^H$ such that $g_1\mathbf{N}_H(x_3) + g_2 x_2 \in (x_1)\mathbf{F}[V]^H$.*

Proof. Assume $b_{1,2}^p - b_{2,4} \neq 0$. We assert that for $c_i := 1/(2(b_{1,2}^{2p} - 2b_{1,2}^p b_{2,4} + b_{2,4}^2)^{i+1})$,

$$\begin{aligned} s_1\mathbf{N}_H(x_3) &- x_2^{p^2} h_1^{\frac{p+1}{2}} + 1/(b_{1,2}^p - b_{2,4}) \cdot x_2^{p(p+1)} \mathbf{N}_H(x_3) \\ &- \sum_{i=0}^{(p-3)/2} c_i \cdot x_2^{p(p+2)+2ip} h_1^{\frac{p-1}{2}-i} + 1/(b_{1,2}^{p^2} - b_{2,4}^p) \cdot x_2^{p^2} s_1 \in (x_1)\mathbf{F}[V]^H. \end{aligned}$$

Set $v_1 := s_1\mathbf{N}_H(x_3) - x_2^{p^2} h_1^{\frac{p+1}{2}} + 1/(b_{1,2}^p - b_{2,4}) \cdot x_2^{p(p+1)} \mathbf{N}_H(x_3)$. Expanding the definition of v_1 gives $\mathrm{LT}(v_1) = c_0 \cdot x_3^{p^2-p} x_2^{p^2+p}$. So we subtract off $c_0 \cdot x_2^{p^2+2p} h_1^{p-1/2}$

which is the first summand. Inductively we find

$$\mathrm{LT}(v_1-\sum_{i=0}^{j} c_i\cdot x_2^{p(p+2)+2ip}h_1^{\frac{p-1}{2}-i}) = c_{j+1}x_3^{\frac{p(p+1)}{2}-p(j+1)}x_2^{p(p+2)+2(j+1)p}, \quad \forall j\in\{0,...,(p-5)/2\}.$$

Finally for $j=(p-3)/2$ we compute

$$\mathrm{LT}(v_1-\sum_{i=0}^{\frac{(p-3)}{2}} c_i\cdot x_2^{p(p+2)+2ip}h_1^{\frac{p-1}{2}-i}) = -1/(b_{1,2}^{p^2}-b_{2,4}^p)\cdot x_3^p x_2^{2p^2}.$$

For the final step we subtract $1/(b_{1,2}^{p^2}-b_{2,4}^p)\cdot x_2^{2p^2}s_1$ and we work modulo $\langle x_1^p\rangle \lhd \mathbf{F}[V]$. Expanding and reducing h_1 modulo $\langle x_1^p\rangle$ gives

$$h_1 \equiv_{\langle x_1^p\rangle} x_3^{2p} + 2/(b_{1,2}^p - b_{2,4})\cdot x_3^p x_2^p - 2(b_{1,2}^p-b_{2,4}^p)/(b_{1,2}^p-b_{2,4})\cdot x_3^{p+1}x_1^{p-1}.$$

Analyzing the terms involved in v_1 yields

$$\begin{aligned} s_1\mathbf{N}_H(x_3) &\equiv_{\langle x_1^p\rangle} x_3^{p(p+1)}x_2^{p^2} + \left(\sum_{i=0}^{p-1}(b_{1,2}^{2p^2-(i+1)p}-b_{1,2}^{p^2-ip})b_{2,4}^i\right)\cdot x_3^{2p^2+1}x_1^{p-1}, \\ x_2^{p^2}h_1^{\frac{p+1}{2}} &\equiv_{\langle x_1^p\rangle} x_3^{p(p+1)}x_2^{p^2} + 1/(b_{1,2}^p-b_{2,4})\cdot x_3^{p^2}x_2^{p^2+p} + \sum_{i=0}^{(p-3)/2} c_i\cdot x_3^{p(p-1)-ip}x_2^{p(p+2)+ip}. \\ x_2^{p(p+1)}\mathbf{N}_H(x_3) &\equiv_{\langle x_1^p\rangle} x_3^{p^2}x_2^{p(p+1)}. \end{aligned}$$

Therefore all together implies

$$v_1 \equiv_{\langle x_1^p\rangle} \sum_{i=0}^{(p-3)/2} c_i x_3^{p(p-1)-ip}x_2^{p(p+2)+ip} + \left(\sum_{i=0}^{p-1}(b_{1,2}^{2p^2-(i+1)p}-b_{1,2}^{p^2-ip})b_{2,4}^i\right)\cdot x_3^{2p^2+1}x_1^{p-1}.$$

For the second part of the expression expanding the definition and reducing gives

$$-\sum_{i=0}^{(p-3)/2} c_i\cdot x_2^{p(p+2)+2ip}h_1^{\frac{p-1}{2}-i} + 1/(b_{1,2}^{p^2}-b_{2,4}^p)\cdot x_2^{p^2}s_1 \equiv_{\langle x_1^p\rangle} -\sum_{i=0}^{(p-3)/2} c_i x_3^{p(p-1)-ip}x_2^{p(p+2)+ip}.$$

Adding up the two parts returns

$$\begin{aligned} v_1 - \sum_{i=0}^{(p-3)/2} c_i\cdot x_2^{p(p+2)+2ip}h_1^{\frac{p-1}{2}-i} &+ 1/(b_{1,2}^{p^2}-b_{2,4}^p)\cdot x_2^{p^2}s_1 \\ &\equiv_{\langle x_1^p\rangle} \left(\sum_{i=0}^{p-1}(b_{1,2}^{2p^2-(i+1)p}-b_{1,2}^{p^2-ip})b_{2,4}^i\right)\cdot x_3^{2p^2+1}x_1^{p-1} \in (x_1)\mathbf{F}[V]^H. \end{aligned}$$

Finally, if we define $g_1 = s_1$ and

$$\begin{aligned} g_2 &= x_2^{p^2-1} h_1^{\frac{p+1}{2}} + 1/(b_{1,2}^p - b_{2,4}) \cdot x_2^{p(p+1)-1} \mathbf{N}_H(x_3) \\ &- \sum_{i=0}^{(p-3)/2} c_i \cdot x_2^{p(p+2)+2ip-1} h_1^{\frac{p-1}{2}-i} + 1/(b_{1,2}^{p^2} - b_{2,4}^p) \cdot x_2^{p^2-1} s_1, \end{aligned}$$

gives $g_1 \mathbf{N}_H(x_3) + g_2 x_2 \in (x_1)\mathbf{F}[V]^H$. Thus our assertion follows. $\square$

As a consequence of the proposition, if we were able to prove that $s_1 \notin (x_1, x_2)\mathbf{F}[V]^H$ then $\mathscr{B}'$ would be a partial hsop which is not a regular sequence, hence [8, Theorem 2.8.1] would imply that $\mathbf{F}[V]^H$ is not Cohen-Macaulay. Albeit proving this assertion for any prime p is a very difficult question in general, we are able to make explicit computation for certain primes.

We use the MAGMA command `InvariantsOfDegree` over the field `F`$\langle t \rangle$:=`GF`(p^r) for $r := 3$ with $b_{i,j}$:= `Random`(F) random and polynomial ring `S<x4,x3,x2,x1>` := `PolynomialRing(F,4,"grevlex")`. Assuming the contrary, $s_1 \in (x_1, x_2)\mathbf{F}[V]^H$ implies $s_1 = v_1 x_1 + v_2 x_2$ for suitable $v_1, v_2 \in \mathbf{F}[V]^H$. In particular, we must have $\mathrm{LT}(v_2) = x_3^p x_2^{p^2-1}$ and $v_2 \in \mathbf{F}[V]^H_{p^2+p-1}$. So in order to have $s_1 \notin (x_1, x_2)\mathbf{F}[V]^H$ it is enough to show that in `InvariantsOfDegree(H,S,`p^2+p-1`)` no basis element has lead monomial equal $\mathrm{LM}(v_2)$. Below we present the lead monomials of basis elements in `InvariantsOfDegree(H,S,`p^2+p-1`)` for $p = 3, 5$ and 7:

(1) $p = 3$

$$\{x_1^{11-i} x_2^i \mid i = 0, ..., 11\}, \{x_3^9 x_1^{2-i} x_2^i \mid i = 0, 1, 2\}, \{x_3^6 x_1^{5-i} x_2^i \mid i = 0, ..., 5\}$$

(2) $p = 5$

$$\{x_1^{29-i} x_2^i \mid i = 0, ..., 29\}, \{x_3^{25} x_1^{4-i} x_2^i \mid i = 0, ..., 4\}, \{x_3^{10} x_1^{19-i} x_2^i \mid i = 0, ..., 19\},$$
$$\{x_3^{20} x_1^{9-i} x_2^i \mid i = 0, ..., 9\}$$

(3) $p = 7$

$$\{x_1^{55-i} x_2^i \mid i = 0, ..., 55\}, \{x_3^{49} x_1^{6-i} x_2^i \mid i = 0, ..., 6\}, \{x_3^{14} x_1^{41-i} x_2^i \mid i = 0, ..., 41\},$$
$$\{x_3^{28} x_1^{27-i} x_2^i \mid i = 0, ..., 27\}, \{x_3^{42} x_1^{13-i} x_2^i \mid i = 0, ..., 13\}.$$

Observe now that for $p = 3, 5$ and 7 there is no monomial $x_3^3 x_2^8$, $x_3^5 x_2^{24}$ or $x_3^7 x_2^{48}$ correspondingly. Thus, $s_1 \notin \mathbf{F}[V]^H_{p^2+p-1}$ with this setup. Hence for these primes we have evidence that $\mathbf{F}[V]^H$ is not Cohen-Macaulay.

Conjecture 4.3.2.6. *Assume V is a four-dimensional $\mathbf{F}H$-module of type-$(1,2,1)$ with socle-tabloid* $\begin{array}{|c|c}\hline 3 & \\ \hline 2 & \multicolumn{1}{|c|}{1} \\ \hline 1 & \\ \hline \end{array}$. *Then $\mathbf{F}[V]^H$ is not Cohen-Macaulay for any prime $p > 2$.*

4.3.3 Invariants of type-$(1, 2, 1)$ with socle-tabloid: $(3, 22, 1)$

Suppose V is a four-dimensional $\mathbf{F}H$-module of type-$(1, 2, 1)$ with socle-tabloid $(3, 22, 1)$. From Theorem 2.5.0.7 there is a choice of basis $\mathscr{B}$ such that the group of representing matrices $\rho_{\mathscr{B}}(H)$ is generated by the following matrices

$$A = \begin{bmatrix} 1 & a_{1,2} & a_{1,3} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b_{1,2} & b_{1,3} & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

with commutator

$$C = [A, B] = ABA^{-1}B^{-1} = \begin{bmatrix} 1 & 0 & 0 & a_{1,2} - b_{1,3} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

We first compute $\mathbf{F}(V)^H$. It is clear that $x_1, \mathbf{N}_H(x_2) = x_2^p - x_1^{p-1}x_2, \mathbf{N}_H(x_3) = x_3^p - x_1^{p-1}x_3$ are minimum degree invariants since the action on the first three variables is Nakajima. For the last one we find a lower bound. Since the $\langle C \rangle$-action on $\mathbf{F}[V]$ is Nakajima $\mathbf{F}[V]^{\langle C \rangle} = \mathbf{F}[x_1, x_2, x_3, \mathbf{N}_C(x_4) = x_4^p - (a_{1,2} - b_{1,3}) \cdot x_1^{p-1}x_4]$. Hence the inclusion $\mathbf{F}[V]^H \subset \mathbf{F}[V]^{\langle C \rangle}$ implies that the minimum x_4-degree H-invariant has x_4-degree at least p as well.

Theorem 4.3.3.1. *The H-invariant*

$$\begin{aligned}\widetilde{g_1} &= b_{1,2}^p x_3^{p+1} + a_{1,2}^p x_3^p x_2 + b_{1,3}^p x_3 x_2^p + a_{1,3}^p x_2^{p+1} - x_4^p x_1 - (\sum_{i=0}^{p-1} a_{1,2}^{p-1-i} b_{1,2} b_{1,3}^i + b_{1,2}^p)/2 \cdot x_3^2 x_1^{p-1} \\ &- \sum_{i=0}^{p} a_{1,2}^{p-i} b_{1,3}^i \cdot x_3 x_2 x_1^{p-1} - (\sum_{i=0}^{p-1} a_{1,2}^{p-1-i} a_{1,3} b_{1,3}^i + a_{1,3}^p)/2 \cdot x_2^2 x_1^{p-1} + \sum_{i=0}^{p-1} a_{1,2}^{p-i} b_{1,3}^i \cdot x_4 x_1^p \\ &+ (\sum_{i=0}^{p-1} a_{1,2}^{p-1-i} b_{1,2} b_{1,3}^i - b_{1,2}^p)/2 \cdot x_3 x_1^p + (\sum_{i=0}^{p-1} a_{1,2}^{p-1-i} a_{1,3} b_{1,3}^i - a_{1,3}^p)/2 \cdot x_2 x_1^p\end{aligned}$$

is of minimum x_4-degree $\mathrm{LC}_{x_4}(\widetilde{g_1}) = -x_1$. Therefore, $\mathbf{F}(V)^H = \mathbf{F}(x_1, \mathbf{N}_H(x_2), \mathbf{N}_H(x_3), \widetilde{g_1})$ and we have an equality of rings: $\mathbf{F}[V]^H[x_1^{-1}] = \mathbf{F}[x_1, \mathbf{N}_H(x_2), \mathbf{N}_H(x_3), \widetilde{g_1}][x_1^{-1}]$.

Proof. Applying the twisted derivations Δ_A, Δ_B yields zero in both cases. Since $\deg_{x_4}(\widetilde{g_1}) = p$ follows from the last paragraph that must be of minimum x_4-degree, hence the field equality is an application of Theorem 1.4.2.6. Finally, notice that the lead term of $\widetilde{g_1}$ as a polynomial in x_4 is $-x_1$, thus $\mathbf{F}[V]^H[x_1^{-1}] = \mathbf{F}[x_1, \mathbf{N}_H(x_2), \mathbf{N}_H(x_3), \widetilde{g_1}][x_1^{-1}]$ as a consequence of Theorem 1.4.2.6 too. □

Define $g_1 := \widetilde{g_1}/b_{1,2}^p$ so that $\mathrm{LT}(g_1) = x_3^{p+1}$ and set $\mathscr{B} := \{x_1, \mathbf{N}_H(x_2), \mathbf{N}_H(x_3), g_1\}$. We wish to apply SAGBI/divide-by-x algorithm on $\mathscr{B}$. In $\mathscr{B}$ there is only one non-trivial tête-à-tête : $(\mathbf{N}_H^{p+1}(x_3), g_1^p)$.

Lemma 4.3.3.2. *Subducting the tête-à-tête $(\mathbf{N}_H^{p+1}(x_3), g_1^p)$, yields an invariant with lead term: $(a_{1,2}^p b_{1,2}^{p^2-p} - a_{1,2}^{p^2})/b_{1,2}^{p^2} \cdot x_3^{p^2} x_2 x_1^{p-1}$.*

Proof. Set

$$\begin{aligned}\widetilde{s_1} &:= \mathbf{N}_H^{p+1}(x_3) - g_1^p + a_{1,2}^{p^2}/b_{1,2}^{p^2} \cdot \mathbf{N}_H(x_2)\mathbf{N}_H^p(x_3) \\ &+ b_{1,3}^{p^2}/b_{1,2}^{p^2} \cdot \mathbf{N}_H^p(x_2)\mathbf{N}_H(x_3) + a_{1,3}^{p^2}/b_{1,2}^{p^2} \cdot \mathbf{N}_H^{p+1}(x_2) + x_1^{p-1}\mathbf{N}_H^{p-1}(x_3) g_1.\end{aligned}$$

Follows by construction that $\widetilde{s_1} \in \mathbf{F}[V]^H$. Expanding and analyzing the definition gives: $\mathrm{LT}(\widetilde{s_1}) := (a_{1,2}^p b_{1,2}^{p^2-p} - a_{1,2}^{p^2})/b_{1,2}^{p^2} \cdot x_3^{p^2} x_2 x_1^{p-1}$. Since the resulting lead term cannot be subducted more $\widetilde{s_1}$ must be the seeking subduction. □

Let $s_1 := b_{1,2}^{p^2}/(a_{1,2}^p b_{1,2}^{p^2-p} - a_{1,2}^{p^2}) \cdot \widetilde{s}_1 x_1^{-(p-1)}$ and $\mathscr{B}_1 := \{x_1, \mathbf{N}_H(x_2), \mathbf{N}_H(x_3), g_1, s_1\}$. Note that $\deg_{x_4}(s_1) = p^2$ with monomial term: $x_4^{p^2} x_1$. This time we have two non-trivial tête-à-têtes : $(s_1^p, \mathbf{N}_H^{p^2}(x_3)\mathbf{N}_H(x_2))$, $(s_1^{p(p+1)}, g_1^{p^3}\mathbf{N}_H^{p+1}(x_2))$.

Lemma 4.3.3.3. *Subducting the tête-à-tête* $(s_1^p, \mathbf{N}_H^{p^2}(x_3)\mathbf{N}_H(x_2))$ *yields an invariant with lead term:* $1/(a_{1,2}^{p^2} b_{1,2}^{p^3-p^2} - a_{1,2}^{p^3}) \cdot x_4^{p^3} x_1^p$.

Proof. Expanding the definition of the tête-à-tête difference gives:

$$\mathrm{LT}(s_1^p - \mathbf{N}_H^{p^2}(x_3)\mathbf{N}_H(x_2)) = -b_{1,2}^{p^3-p^2} b_{1,3}^{p^2}/(a_{1,2}^{p^3} - a_{1,2}^{p^2} b_{1,2}^{p^3-p^2}) \cdot x_3^{p^2-p+1} x_2^{p^2}.$$

After explicit calculations we obtain the following expression for the first steps of the subduction

$$\begin{aligned} u_1 \;&:=\; s_1^p - \mathbf{N}_H^{p^2}(x_3)\mathbf{N}_H(x_2) + b_{1,2}^{p^3-p^2} b_{1,3}^{p^2}/(a_{1,2}^{p^3} - a_{1,2}^{p^2} b_{1,2}^{p^3-p^2}) \cdot \mathbf{N}_H^p(x_2)\mathbf{N}_H^{p^2-p+1}(x_3) \\ &+\; a_{1,3}^{p^2} b_{1,2}^{p^3-p^2}/(a_{1,2}^{p^3} - a_{1,2}^{p^2} b_{1,2}^{p^3-p^2}) \cdot \mathbf{N}_H^{p+1}(x_2)\mathbf{N}_H^{p^2-p}(x_3) \\ &-\; b_{1,3}^{p^3}/(a_{1,2}^{p^3} - a_{1,2}^{p^2} b_{1,2}^{p^3-p^2}) \cdot \mathbf{N}_H^{p^2}(x_2)\mathbf{N}_H(x_3) \\ &-\; a_{1,3}^{p^3}/(a_{1,2}^{p^3} - a_{1,2}^{p^2} b_{1,2}^{p^3-p^2}) \cdot \mathbf{N}_H^{p^2+1}(x_2) - x_1^{p-1}\mathbf{N}_H^{p^2-p}(x_3) s_1, \end{aligned}$$

with $\mathrm{LT}(u_1) = b_{1,2}^{p^2-p} b_{1,3}^p/(a_{1,2}^{p^2} - a_{1,2}^p b_{1,2}^{p^2-p}) \cdot x_3^{p^3-p+1} x_2^p x_1^{p-1}$. Consider the following invariant

$$\begin{aligned} u_2 \;&:=\; u_1 - x_1^{p-1} \cdot \Big\{ \sum_{i=1}^{p^2-p} \mathbf{N}_H^i(x_2)(c_{i,1} \cdot \mathbf{N}_H^{p^2-1-i}(x_3) g_1 + c_{i,2} \cdot \mathbf{N}_H^{p^2-p-i}(x_3) s_1) \Big\} \\ &+\; x_1^{p-1} \cdot \Big\{ \sum_{i=1}^{p-1} c_{i,3} \cdot \mathbf{N}_H^{p^2-p+i}(x_2)\mathbf{N}_H^{p-1-i}(x_3) g_1 \Big\}, \end{aligned}$$

and set

$$v_j := u_1 - x_1^{p-1} \cdot \Big\{ \sum_{i=1}^{j} \mathbf{N}_H^j(x_2)(c_{j,1} \cdot \mathbf{N}_H^{p^2-1-j}(x_3) g_1 + c_{j,2} \cdot \mathbf{N}_H^{p^2-p-j}(x_3) s_1) \Big\},\ \forall j \in \{1, ..., p^2-p\}.$$

Now define $c_{j,1} = \mathrm{LC}(v_{j-1}), c_{j,2} = \mathrm{LC}(v_{j-1} - c_{j,1} \cdot x_1^{p-1}\mathbf{N}_H^j(x_2)\mathbf{N}_H^{p^2-1-j}(x_2) g_1)$. Analyzing v_j yields $\mathrm{LT}(v_j) = c_{j+1,1} \cdot x_3^{p^3-p(j+1)+1} x_2^{p(j+1)} x_1^{p-1}$, for all $j \in \{1, ..., p^2 - p\}$. By definition, the coefficients ensure that the lead term $\mathrm{LT}(v_j)$ is canceled by $\mathrm{LT}(c_{j+1,1} \cdot x_1^{p-1}\mathbf{N}_H^{j+1}(x_2)\mathbf{N}_H^{p^2-j-2}(x_3) g_1)$ at each stage and similarly that $\mathrm{LT}(v_j -$

$c_{j+1,1}\cdot x_1^{p-1}\mathbf{N}_H^{j+1}(x_2)\mathbf{N}_H^{p^2-j}(x_3)g_1)$ is canceled by $\mathrm{LT}(c_{j+1,2}\cdot x_1^{p-1}\mathbf{N}_H^{j+1}(x_2)\mathbf{N}_H^{p^2-p+j}(x_3)s_1)$. Finally, we have $\mathrm{LM}(u_{p^2-p}) = x_3^{p^2-p+1}x_2^{p^3-p^2}x_1^{p-1}$. Hence can be subducted by the last summand in u_2: $c_{p-1,3}\cdot \mathbf{N}_H^{p^2-p+1}(x_2)\mathbf{N}_H^{p-2}(x_3)g_1$, for $c_{p-1,3} = \mathrm{LC}(v_{p^2-p})$. So we set $c_{j,3} = \mathrm{LC}(v_{p^2-p} - \sum_{k=j}^{p-1} c_{k,3}\cdot \mathbf{N}_H^{p^2-p+i}(x_2)\mathbf{N}_H^{p-1-i}(x_3)g_1)$. The last ensures that in the resulting u_2 every term has a copy of x_1^p. Since we are using grevlex order with $x_1 < x_2 < x_3 < x_4$, the term $1/(a_{1,2}^{p^2}b_{1,2}^{p^3-p^2} - a_{1,2}^{p^3})\cdot x_4^{p^3}x_1^p$ in s_1^p must be the lead term of u_2 and the claim follows. □

Define $s_2 := (a_{1,2}^{p^2}b_{1,2}^{p^3-p^2} - a_{1,2}^{p^3})\cdot u_2/x_1^p$ and $\mathscr{B}_1 := \{x_1, \mathbf{N}_H(x_2), \mathbf{N}_H(x_3), g_1, s_1, s_2\}$. Explicit computations on MAGMA over $\mathtt{F}\langle t\rangle$:=$\mathtt{GF}(p^r)$ for $r := 4$ with $a_{i,j}, b_{i,j} :=$ $\mathtt{Random}(F)$, reveal that against $\mathscr{B}_1$ the tête-à-tête $(s_1^{p(p+1)}, g_1^{p^3}\mathbf{N}_H^{p+1}(x_2))$ subducts to zero when $p = 3, 5$ and 7. Therefore, for these primes we collect evidence that $\mathscr{B}_1$ is a SAGBI basis. Furthermore, since $\mathbf{F}[\mathscr{B}_1] \subset \mathbf{F}[V]^H$ is integral with $\mathbf{F}[\mathscr{B}_1][x_1^{-1}] = \mathbf{F}[V]^H[x_1^{-1}]$ follows that $\mathbf{F}[V]^H = \mathbf{F}[\mathscr{B}_1]$ from Theorem 1.4.3.10. Hence $\mathbf{F}[V]^H$ is a complete intersection with embedding dimension six. However, even for small primes the complexity of computations is forbidding for an explicit description. When $p = 5$, MAGMA returns 1500 steps during the tête-à-tête subduction and this number increases significantly when one attempts the case $p = 7$. Therefore, we conjecture the following.

Conjecture 4.3.3.4. *Assume that V is a four-dimensional $\mathbf{F}H$-module of type-$(1,2,1)$ and socle-tabloid* $\begin{array}{|c|c|}\hline 3 & \\ \hline 2 & 2 \\ \hline 1 & \\ \hline\end{array}$. *Then $\mathbf{F}[V]^H$ is a complete intersection with embedding dimension six and two relations constructed during the tête-à-tête subductions.*

4.4 Invariants of type-(2,1,1) representations.

4.4.1 Introduction

In this section we investigate the structure of the invariant rings of type-$(2,1,1)$ representations. We remind you that the image of these representations consists of elements of the form

$$\begin{bmatrix} 1 & 0 & c_{1,3} & c_{1,4} \\ 0 & 1 & c_{2,3} & c_{2,4} \\ 0 & 0 & 1 & c_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad c_{i,j} \in \mathbf{F}.$$

Recall from Theorem 2.3.0.6 the existence of a basis $\mathscr{B}'$ so that $\rho_{\mathscr{B}'}(H)$ is generated by

$$J_{1,3} := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \widetilde{B} := \begin{bmatrix} 1 & 0 & b_{1,3} & b_{1,4} \\ 0 & 1 & b_{2,3} & b_{2,4} \\ 0 & 0 & 1 & b_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

for $b_{i,j} \in \mathbf{F}$. From [8, Theorem 3.9.2], we know that $\mathbf{F}[V]^H$ is Cohen-Macaulay since $\dim_{\mathbf{F}}(V^H) = 2$. However we have to distinguish between two cases, $b_{1,3} \neq 0$ and $b_{1,3} = 0$.

4.4.2 Case $b_{1,3} \neq 0$

We start by considering the case $b_{1,3} \neq 0$. From Theorem 2.3.0.6-(1), we fix a basis $\mathscr{B}$ such that the group of representing matrices $\rho_{\mathscr{B}}(H)$ is generated by

$$A := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B := \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & a \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

for $a, b \in \mathbf{F}$.

In this section we compute the invariant field $\mathbf{F}(V)^H$. To this end, assume $a, b \neq 0$ and think of the composition series $\langle A \rangle \triangleleft \langle A, C \rangle \triangleleft \langle A, B \rangle = H$, where

$$C = [A, B] = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Notice that $\mathbf{F}[V]^{\langle A\rangle} = \mathbf{F}[V_3 \oplus V_1]^{\langle A\rangle}$. Therefore,

$$\mathbf{F}[V]^{\langle A\rangle} = \mathbf{F}[V_3]^{\langle A\rangle} \otimes \mathbf{F}[V_1] = \mathbf{F}[x_1, \delta, \mathbf{N}_A(x_2), \mathbf{N}_A(x_3), x_4]. \tag{4.4.1}$$

The latter follows from the three-dimensional case in [7, Theorem 4.3], plus a generator in degree one induced from the trivial representation. As a reminder, we have set $\delta = x_2^2 - 2x_3x_1 - x_2x_1$.

For simplicity let $H_2 = \langle A, C\rangle$. On localization level

$$\mathbf{F}[V]^{\langle A\rangle}[x_1^{-1}] = \mathbf{F}[x_1, \delta, \mathbf{N}_A(x_2), x_4][x_1^{-1}].$$

Therefore applying the $\langle C\rangle$-action yields: $\mathbf{F}[V]^{H_2}[x_1^{-1}] = \mathbf{F}[x_1, \delta, \mathbf{N}_A(x_2), x_4]^{\langle C\rangle}[x_1^{-1}]$. As it is customary to do, we shift to degree one the algebra generators $y_1 := \delta/x_1, y_2 := \mathbf{N}_A(x_2)/x_1^{p-1}$, and think of the new $\mathbf{F}\langle C\rangle$-module spanned by these elements. On this new basis we compute

$$x_1 \cdot C := x_1 \quad , \quad y_1 \cdot C := y_1 - 2bx_1,$$
$$y_2 \cdot C := y_2 \quad , \quad x_4 \cdot C := x_4 - x_1.$$

The $\langle C\rangle$-action is Nakajima, hence $\mathbf{F}[x_1, y_1, y_2, x_4]^{\langle C\rangle} = \mathbf{F}[x_1, x_4 - 1/2b \cdot y_1, y_2, \mathbf{N}_C(x_4)]$. Thus, $\mathbf{F}[V]^{H_2}[x_1^{-1}] = \mathbf{F}[x_1, \mathbf{N}_A(x_2), \delta - 2bx_1x_4, \mathbf{N}_C(x_4)][x_1^{-1}]$ after clearing the denominators minimally. Set $\mathfrak{B} := \{x_1, g_1 := \delta - 2bx_1x_4, \mathbf{N}_A(x_2), \mathbf{N}_C(x_4)\}$. In $\mathfrak{B}$ there is a unique non-trivial tête-à-tête: $(\mathbf{N}_{H_2}^2(x_2), g_1^p)$.

Lemma 4.4.2.1. *Subducting $(\mathbf{N}_{H_2}^2(x_2), g_1^p)$ yields an invariant with lead term: $2b^px_3^px_1^p$.*

Proof. Observe that $\mathrm{LT}(\mathbf{N}_{H_2}^2(x_2) - g_1^p) = -2x_2^{p+1}x_1^{p-1}$. Therefore we set $t_1 := \mathbf{N}_{H_2}^2(x_2) - g_1^p + 2g_1^{(p+1)/2}x_1^{p-1}$. The second term in order inside $g_1^{(p+1)/2}x_1^{p-1}$ is $4bx_4x_2^{p-1}x_1^p$. Since the corresponding term in $\mathbf{N}_{H_2}^2(x_2) - g_1^p$ is $2bx_4^px_1^p$, follows $\mathrm{LT}(t_1) := 2bx_4^px_1^p$. Finally, let $t_2 := t_1 - 2b\,x_1^p\,\mathbf{N}_C(x_4)$. Expanding the definition of t_2 is easy to see that $2b^px_3^px_1^p$. □

Set $g_2 := t_2/2b^px_1^p$ and $\mathfrak{B}_1 := \{x_1, g_1, \mathbf{N}_{H_2}(x_2), g_2, \mathbf{N}_{H_2}(x_4)\}$. This time in $\mathfrak{B}_1$ there is no non-trivial tête-à-tête , hence forms a SAGBI basis of $\mathbf{F}[V]^{H_2}$.

Lemma 4.4.2.2. *$\mathbf{F}[V]^{H_2} = \mathbf{F}[x_1, g_1, \mathbf{N}_{H_2}(x_2), g_2, \mathbf{N}_{H_2}(x_4)]$, where $\mathrm{LT}(g_1) = x_2^2$, $\mathrm{LT}(\mathbf{N}_{H_2}(x_2)) = x_2^p, \mathrm{LT}(g_2) = x_3^p, \mathrm{LT}(\mathbf{N}_{H_2}(x_4)) = x_4^p$. Furthermore, we have an equality of fields $\mathbf{F}(V)^{H_2} = \mathbf{F}(x_1, \mathbf{N}_{H_2}(x_2), g_1, g_2)$.*

Proof. Follows by an application of Theorem 1.4.2.6 and 1.4.3.10. □

Now we compute $\mathbf{F}(V)^H$. On the first two variables the action is Nakajima, hence $\{x_1, \mathbf{N}_H(x_2)\}$ form invariants of minimum degree with $\mathrm{LT}(\mathbf{N}_H(x_2)) = x_2^{p^2}$. Also a routine computation shows that

$$\kappa_1 := x_2^p + \frac{b^p - b}{2\gamma} x_2^2 x_1^{p-2} - \frac{b^{p+1} - b^2}{\gamma} x_4 x_1^{p-1} - \frac{b^p - b}{\gamma} x_3 x_1^{p-1} - \frac{2a + b^p - b^2}{2\gamma} x_2 x_1^{p-1},$$

for $\gamma := a + (p-1)/2 \cdot b^2 + (p+1)/2 \cdot b$, is a minimum x_4-degree H-invariant. The only thing left is the minimum x_3-degree invariant. From Lemma 4.4.2.2 and the field inclusion $\mathbf{F}(V)^H \subset \mathbf{F}(V)^{H_2}$, we know that has degree at least p.

Theorem 4.4.2.3. *The polynomial*

$$\begin{aligned} \kappa_2 \;\; := \;\; & x_2^{2p} - 2b^{p-1} x_2^{p+1} x_1^{p-1} + 2(b^{p-1} - 1) x_3^p x_1^p + (-2a^p + 2ab^{p-1} + b^p - b)/b \cdot x_2^p x_1^p \\ + \;\; & b^{2(p-1)} x_2^2 x_1^{2(p-1)} - 2b^{p-1}(b^{p-1} - 1) x_3 x_1^{2p-1} + (2a^p - 2ab^{p-1} - b^{2p-1} + b^p)/b \cdot x_2 x_1^{2p-1}, \end{aligned}$$

forms an H-invariant of minimum x_3-degree. Therefore, $\mathbf{F}(V)^H = \mathbf{F}(x_1, \mathbf{N}_H(x_2), \kappa_1, \kappa_2)$ and since $\mathrm{LC}_{x_4}(\kappa_1) = x_1^{p-1}$ we have an equality of localized rings: $\mathbf{F}[V]^H[x_1^{-1}] = \mathbf{F}[x_1, \mathbf{N}_H(x_2), \kappa_1, \kappa_2][x_1^{-1}]$.

Remark 4.4.2.4. *For the above computations we assumed $a, b \in \mathbf{F}^*$. When $a = b = 0$, think the composition series $H_1 = \langle B \rangle \triangleleft H_2 = \langle B, C \rangle \triangleleft H = \langle A, B \rangle$. Then [8, Corollary 3.1.6] implies $\mathbf{F}[V]^{H_1} = \mathbf{F}[x_1, x_2, x_3, \mathbf{N}_B(x_4)]$ and applying the $H_2/H_1 \cong \langle C \rangle$-action, $\mathbf{F}[V]^{H_2} = (\mathbf{F}[V]^{H_1})^{H_2/H_1} = \mathbf{F}[x_1, x_2, x_3, \mathbf{N}_{H_2}(x_4)]$. Since the last algebra is polynomial, the $H/H_2 \cong \langle A \rangle$-action on $\mathbf{F}[V]^{H_2}$ gives $\mathbf{F}[V]^H = \mathbf{F}[x_1, x_2, x_3, \mathbf{N}_{H_2}(x_4)]^{\langle A \rangle}$. Thus, an application of [7, Theorem 4.3] for $W = C_p$ yields $\mathbf{F}[V]^H = \mathbf{F}[x_1, \delta, \mathbf{N}_H(x_2), \mathbf{N}_H(x_3), \mathbf{N}_H(x_4)]$, where $\delta = x_2^2 - 2x_3x_1 - x_2x_1$.*

4.4.2.5 Complete intersection property of $\mathbf{F}[V]^H$

Set $\mathscr{B} := \{x_1, \mathbf{N}_H(x_2), \kappa_1, \kappa_2\}$. In principle, we can extend $\mathscr{B}$ to a SAGBI basis for any p. However, computations on MAGMA reveal that $\mathbf{F}[V]^H$ depends on the choice of p. As a result, $\mathbf{F}[V]^H$ does not have a closed form. Below we investigate subductions of $\mathscr{B}$ that exist for all $p \geq 3$ and explicitly present the tête-à-tête subductions for small primes.

Set $S := [x_1, \kappa_1, \kappa_2, \mathbf{N}_H(x_2), \mathbf{N}_H(x_4)]$ for the list of minimum degree invariants and H-norm of x_4. Note that the x_3-norm has not been included. From the definition of H in that case, we have $\mathrm{LT}(\mathbf{N}_H(x_3)) = x_3^{p^3}$. However as we will see below $\mathbf{N}_H(x_3)$ is not the right invariant. For $p = 5, 7$ during the tête-à-tête subduction another one with lead term $x_3^{p^2}$ is constructed.

We seek for non-trivial tête-à-têtes in S. The first tête-à-tête subduction is that of (κ_2, κ_1^2). Set $h_1 := \textsc{subd}(\kappa_2 - \kappa_1^2, S)$ after normalization. Expanding the definition of h_1 shows that $\mathrm{LT}(h_1) = x_2^{p+2}$. When h_1 is attached to S, κ_2 is redundant. So let $S_1 := [x_1, \mathbf{N}_H(x_3), \kappa_1, h_1, \mathbf{N}_H(x_4)]$ denote this new list.

The second tête-à-tête subduction is $\textsc{subd}(\mathbf{N}_H(x_2) - \kappa_1^p, S_1)$. Likewise, let h_2 denote this subduction after normalization. Expanding again the definition gives $\mathrm{LT}(h_2) = x_2^{p+1}$. Now we can drop the norm $\mathbf{N}_H(x_2)$ from S_1 and attach h_2 instead. Define $S_2 := [x_1, \kappa_1, h_1, h_2, \mathbf{N}_H(x_3), \mathbf{N}_H(x_4)]$ for the new list.

Finally, in S_2 there is an additional generic non-trivial tête-à-tête , $(h_1^2, h_2\kappa_1)$. The latter defines an invariant $h_3 := (h_1^2 - h_2\kappa_1)/(\mathrm{LC}(h_1^2 - h_2\kappa_1)\, x_1)$, $\mathrm{LT}(h_3) = x_4^p x_2^{p+1}$. The new list $S_3 := [x_1, \mathbf{N}_H(x_3), \kappa_1, h_1, h_2, h_3, \mathbf{N}_H(x_4)]$ consists of H-invariants for any prime p.

Below we investigate the cases $p = 3, 5$ and 7. For each of these primes we use MAGMA to extend S_3 to a SAGBI basis. Furthermore, we are able to count the number of minimal algebraic relations and based on this evidence we conjecture that $\mathbf{F}[V]^H$ is a Cohen-Macaulay ring which is not a complete intersection. In what follows LC_i denotes the leading coefficient of the i-th subduction. With that notation for example we have $\mathrm{LC}_2 = \mathrm{LC}(\kappa_2 - \kappa_1^2), \mathrm{LC}_3 = \mathrm{LC}(h_1^2 - h_2\kappa_1)$.

Computation $p = 3$:

We apply SAGBI/divide-by-x algorithm on S_3. The invariants we obtain after the tête-à-tête subductions on MAGMA are depicted as follows:

$$\begin{aligned}
h_4 &:= (\kappa_1^{(p+3)/2} - h_2 h_1^{(p-1)/2})/\mathrm{LC}_4 x_1, \ \ \mathrm{LT}(h_4) = x_4^p x_2^{p+2},\\
h_5 &:= (h_1^{(p+1)/2} - h_2 \kappa_1^{(p+1)/2})/\mathrm{LC}_5 x_1, \ \ \mathrm{LT}(h_5) = x_4^p x_2^{2p},\\
h_6 &:= (h_3 h_1 - h_5\kappa_1 - \mathrm{LC}(h_3 h_1 - h_5\kappa_1) h_2^p)/\mathrm{LC}_6 x_1, \ \ \mathrm{LT}(h_6) = x_4^{2p} x_2^{p+2},\\
h_7 &:= (h_5 h_2 - h_3\kappa_1^2 - \mathrm{LC}(h_5 h_2 - h_3\kappa_1^2)\kappa_1 h_1^2)/\mathrm{LC}_7 x_1, \ \ \mathrm{LT}(h_7) = x_4^{2p} x_2^{2p}.
\end{aligned}$$

Let S_7 denote the resulting list $[x_1, \kappa_1, h_1, h_2, h_3, h_4, h_5, h_6, h_7, \mathbf{N}_H(x_4)]$. To check if S_7 forms a SAGBI basis we use MAGMA again; over the finite field `F` := `GF`(p^4), we construct a polynomial ring on four-variables with respect the grevlex order `S<x4,x3,x2,x1>:=PolynomialRing(F,4,"grevlex")`. Then, for randomly assigned variables `a` := `Random(F)`, `b` := `Random(F)`, MAGMA returns immediately that in S_7 every non-trivial tête-à-tête subducts to zero. From Theorem 4.4.2.3 follows also that $\mathbf{F}[S_7][x_1^{-1}] = \mathbf{F}[V]^H[x_1^{-1}]$ and $\mathbf{F}[S_7] \subset \mathbf{F}[V]^H$ is integral, so $\mathbf{F}[S_7] = \mathbf{F}[V]^H$ and S_7 is a SAGBI basis for $\mathbf{F}[V]^H$. In particular, for $p = 3$ in contrast with the other two cases below, MAGMA is able to return a minimal set of fundamental invariants using the `FundamentalInvariants()` command. The lead terms of these invariants coincide with those in S_7, so it forms a minimal generating set. To count the algebraic relations of the elements in S_7 we use the `sagbi()` function described in the first chapter. From Lemma 1.4.3.12, we know that the number of non-trivial tête-à-tête subductions in a SAGBI basis minimally generate the ideal of relations. Here `sagbi()` returns 27 relations among the elements of S_7, hence the ideal of relation of $\mathbf{F}[V]^H$ is generated by 27 elements.

Computation $p = 5$:

We follow the same procedure as in the previous case. The generators and relations of $\mathbf{F}[V]^H$ created throughout the SAGBI/divide-by-x algorithm are defined as follows:

$$\begin{aligned}
h_4 &:= (\kappa_1^{(p+3)/2} - h_2 h_1^{(p-1)/2})/\mathrm{LC}_4\, x_1,\ \ \mathrm{LT}(h_4) = x_4^5 x_2^{14},\\
h_5 &:= (h_1 h_2 h_3 - h_4 \kappa_1)/\mathrm{LC}_5\, x_1,\ \ \mathrm{LT}(h_5) = x_4^{10} x_2^{13},\\
h_6 &:= (h_1^{(p+1)/2} - h_2 \kappa_1^{(p+1)/2})/\mathrm{LC}_6\, x_1,\ \ \mathrm{LT}(h_6) = x_4^5 x_2^{15},\\
h_7 &:= (h_6 \kappa_1 - h_4 h_2)/\mathrm{LC}_7\, x_1,\ \ \mathrm{LT}(h_7) = x_4^{10} x_2^{14},\\
h_8 &:= (h_6 h_2 - h_3 \kappa_1^3)/\mathrm{LC}_8\, x_1,\ \ \mathrm{LT}(h_8) = x_4^{10} x_2^{15},\\
h_9 &:= (\kappa_1^2 h_2 h_3 - h_1 h_6)/\mathrm{LC}_9\, x_1,\ \ \mathrm{LT}(h_9) = x_4^{10} x_2^{16},\\
h_{10} &:= (h_2 h_5 - \kappa_1 h_7)/\mathrm{LC}_{10}\, x_1,\ \ \mathrm{LT}(h_{10}) = x_4^{15} x_2^{13},\\
h_{11} &:= (\kappa_1 h_8 - h_2 h_7)/\mathrm{LC}_{11}\, x_1,\ \ \mathrm{LT}(h_{11}) = x_4^{15} x_2^{14},\\
h_{12} &:= (h_2 h_8 - \kappa_1 h_9)/\mathrm{LC}_{1,2}\, x_1,\ \ \mathrm{LT}(h_{1,2}) = x_4^{15} x_2^{15},\\
h_{13} &:= (h_1 h_8 - h_2 h_9)/\mathrm{LC}_{1,3}\, x_1,\ \ \mathrm{LT}(h_{1,3}) = x_4^{15} x_2^{16},\\
h_{14} &:= (\kappa_1 h_{1,2} - h_2 h_{11} - \mathrm{LC}(\kappa_1 h_{1,2} - h_2 h_{11})\kappa_1^{p+2})/\mathrm{LC}_{14}\, x_1,\ \ \mathrm{LT}(h_{14}) = x_4^{20} x_2^{14},\\
h_{15} &:= (\kappa_1 h_{1,3} - h_2 h_{1,2} - \mathrm{LC}(\kappa_1 h_{1,3} - h_2 h_{1,2}) h_2^{p+1})/\mathrm{LC}_{15}\, x_1,\ \ \mathrm{LT}(h_{15}) = x_4^{20} x_2^{15}.
\end{aligned}$$

To complete the tête-à-tête subduction, there is one last left

$$\mathbf{N}_3 := \textsc{subd}(h_2 h_3^2 - \kappa_1 h_5, [x_1, \kappa_1, h_1, h_2, h_3, h_4, h_5, \mathbf{N}_H(x_4)])/\mathrm{LC}\, x_1^3,\ \ \mathrm{LT}(\mathbf{N}_3) = x_3^{p^2}.$$

We can confirm on MAGMA that in the resulting list, say S_{15}, every non-trivial tête-à-tête subducts to zero. We work as previously over a finite field $\mathtt{F} := \mathtt{GF}(p^4)$, with randomly assigned variables. Likewise, we have $\mathbf{F}[S_{15}] = \mathbf{F}[V]^H$. Therefore, S_{15} forms a SAGBI basis for $\mathbf{F}[V]^H$. Using the function `sagbi()` on MAGMA returns a list of 125 generators for the ideal of algebraic relations of $\mathbf{F}[V]^H$. As we said previously this list is minimal.

Computation $p = 7$:

The computations for $p = 7$ yield a SAGBI basis comprised of the following elements:

$$\begin{aligned}
h_4 &:= (\kappa_1^{(p+3)/2} - h_2 h_1^{(p-1)/2})/\mathrm{LC}_4\, x_1,\ \mathrm{LT}(h_4) = x_4^7 x_2^{27},\\
h_5 &:= (h_1^{(p+1)/2} - h_2 \kappa_1^{(p+1)/2})/\mathrm{LC}_5\, x_1,\ \mathrm{LT}(h_5) = x_4^7 x_2^{28},
\end{aligned}$$

$$
\begin{aligned}
h_6 &:= (\kappa_1 h_4 - h_3 h_2 h_2^1)/\mathrm{LC}_6\, x_1,\ \mathrm{LT}(h_6) = x_4^{14} x_2^{26},\\
h_7 &:= (h_5 \kappa_1 - h_4 h_2)/\mathrm{LC}_7\, x_1,\ \mathrm{LT}(h_7) = x_4^{14} x_2^{27},\\
h_8 &:= (h_5 h_2 - h_3 \kappa_1^4)/\mathrm{LC}_8\, x_1,\ \mathrm{LT}(h_8) = x_4^{14} x_2^{28},\\
h_9 &:= (h_5 h_1 - h_2 h_3 \kappa_1^3)/\mathrm{LC}_9\, x_1,\ \mathrm{LT}(h_9) = x_4^{14} x_2^{29},\\
h_{10} &:= (\kappa_1 h_6 - h_3^2 h_2 h_1)/\mathrm{LC}_{10}\, x_1,\ \mathrm{LT}(h_{10}) = x_4^{21} x_2^{25},\\
h_{11} &:= (h_2 h_6 - \kappa_1 h_7)/\mathrm{LC}_{11}\, x_1,\ \mathrm{LT}(h_{11}) = x_4^{21} x_2^{26},\\
h_{1,2} &:= (h_2 h_7 - \kappa_1 h_8)/\mathrm{LC}_{1,2}\, x_1,\ \mathrm{LT}(h_{1,2}) = x_4^{21} x_2^{27},\\
h_{1,3} &:= (h_2 h_8 - \kappa_1 h_9)/\mathrm{LC}_{1,3}\, x_1,\ \mathrm{LT}(h_{1,3}) = x_4^{21} x_2^{28},\\
h_{14} &:= (h_2 h_9 - h_1 h_8)/\mathrm{LC}_{14}\, x_1,\ \mathrm{LT}(h_{14}) = x_4^{21} x_2^{29},\\
h_{15} &:= (\kappa_1^2 h_2 h_3^2 - h_1 h_9)/\mathrm{LC}_{15}\, x_1,\ \mathrm{LT}(h_{15}) = x_4^{21} x_2^{30},\\
h_{16} &:= (h_2 h_{10} - \kappa_1 h_{11})/\mathrm{LC}_{16}\, x_1,\ \mathrm{LT}(h_{16}) = x_4^{28} x_2^{25},\\
h_{17} &:= (h_2 h_{11} - \kappa_1 h_{1,2})/\mathrm{LC}_{17}\, x_1,\ \mathrm{LT}(h_{17}) = x_4^{28} x_2^{26},\\
h_{18} &:= (h_2 h_{1,2} - \kappa_1 h_{1,3})/\mathrm{LC}_{18}\, x_1,\ \mathrm{LT}(h_{18}) = x_4^{28} x_2^{27},\\
h_{19} &:= (h_2 h_{1,3} - \kappa_1 h_{14})/\mathrm{LC}_{19}\, x_1,\ \mathrm{LT}(h_{19}) = x_4^{28} x_2^{28},\\
h_{20} &:= (h_2 h_{14} - \kappa_1 h_{15})/\mathrm{LC}_{20}\, x_1,\ \mathrm{LT}(h_{20}) = x_4^{28} x_2^{29},\\
h_{21} &:= (h_2 h_{15} - h_1 h_{14})/\mathrm{LC}_{21}\, x_1,\ \mathrm{LT}(h_{21}) = x_4^{28} x_2^{30},\\
h_{22} &:= (h_2 h_{17} - \kappa_1 h_{18})/\mathrm{LC}_{22}\, x_1,\ \mathrm{LT}(h_{22}) = x_4^{35} x 2_2^{26},\\
h_{2,3} &:= (h_2 h_{18} - \kappa_1 h_{19})/\mathrm{LC}_{2,3}\, x_1,\ \mathrm{LT}(h_{2,3}) = x_4^{35} x_2^{27},\\
h_{2,4} &:= (h_2 h_{19} - \kappa_1 h_{20})/\mathrm{LC}_{2,4}\, x_1,\ \mathrm{LT}(h_{2,4}) = x_4^{35} x_2^{28},\\
h_{25} &:= (h_2 h_{20} - \kappa_1 h_{21})/\mathrm{LC}_{25}\, x_1,\ \mathrm{LT}(h_{25}) = x_4^{35} x_2^{29},\\
h_{26} &:= (h_2 h_{2,3} - \kappa_1 h_{2,4} - \mathrm{LC}(h_2 h_{2,3} - \kappa_1 h_{2,4})\kappa_1^{10})/\mathrm{LC}_{26}\, x_1,\ \mathrm{LT}(h_{26}) = x_4^{42} x_2^{27},\\
h_{27} &:= (h_2 h_{2,4} - \kappa_1 h_{25} - \mathrm{LC}(h_2 h_{2,4} - \kappa_1 h_{25})\kappa_1^{9} h_2)/\mathrm{LC}_{27}\, x_1,\ \mathrm{LT}(h_{27}) = x_4^{42} x_2^{28}.
\end{aligned}
$$

To complete the tête-à-tête subduction, there is one last left

$$\mathbf{N}_3 := \textsc{subd}(h_2 h_3^3 - \kappa_1 h_{10}, [x_1, \kappa_1, h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8, h_9, \mathbf{N}_H(x_4)])/\mathrm{LC}\, x_1^3,\ \ \mathrm{LT}(\mathbf{N}_3) = x_3^{p^2}.$$

Using MAGMA as above in the resulting list, say S_{27}, we can confirm that every non-trivial tête-à-tête subducts to zero. Therefore, S_{27} forms a SAGBI basis for $\mathbf{F}[V]^H$ when $p = 7$. This time the `sagbi()` function after few hours returns a list of 401 minimal relations for $\mathbf{F}[V]^H$.

That the number of relations varies, implies that $\mathbf{F}[V]^H$ has not a closed form. Furthermore, although $\mathbf{F}[V]^H$ is Cohen-Macaulay for every prime p, we can prove that it is not a complete intersection by a simple counting argument. The rest of this section is dedicated on this.

Let B denote a finitely generated commutative $\mathbf{F}$-algebra graded over the non-negative integers. Suppose also that $S = \{f_1, ..., f_n\}$ is a minimal system of homogeneous generators for B and let $\dim(B)$ denote the Krull dimension of B. We remind you that B is called a complete intersection, if for a given presentation $\sigma : \mathbf{F}[X_1, ..., X_n] \to B,\ X_i \mapsto \sigma(X_i) = f_i$, the kernel $\ker(\sigma)$ is generated by a regular sequence.

For a given subset of elements of B, one can define the Koszul complex associated to this set. In our case, choose this set to be S. Since the Koszul homology is independent of the choice of the generating set (up to isomorphism of complexes) [4, pg.75], we can denote the Koszul homology associated to $\underline{f} = (f_1, ..., f_n)$, $K_B(\underline{f})$, just by $H_*(B)$.

We remind you the following result from the introduction, where counting the number of minimal algebraic relations for a graded local Cohen-Macaulay ring suffices to decide whether it is a complete intersection or not.

Proposition 4.4.2.6. *Suppose that B is an integral domain. Using the above notation, B is a complete intersection if and only if* $\dim_{\mathbf{F}}(H_1(B)) = n - \dim(B)$.

In our case $B = \mathbf{F}[V]^H$ and $\dim(\mathbf{F}[V]^H) = 4$. Since $\dim_{\mathbf{F}}(H_1(B))$ coincides with the cardinality of a minimal generating set of $\ker(\sigma)$, to prove our claim suffices to show that the above equality does not hold. For the case $p = 3$ we calculated 27 relations, hence $\dim_{\mathbf{F}}(H_1(\mathbf{F}[V]^H)) = 27$. Also the SAGBI basis we computed is minimal since coincides with the output of `FundamentalInvariants`, and the last returns always a minimal generating set. Hence for $p = 3$ we have

$n - \dim(B) = 10 - 4 = 6$, so $\mathbf{F}[V]^H$ is not a complete intersection.

For $p = 5, 7$ unfortunately we have no guarantee that the SAGBI bases we computed are minimal. However, the number of their elements sets an upper bound for it. For $p = 5$, we have $\dim(H_1(\mathbf{F}[V]^H)) = 125$ while a minimal generating set contains at most 19 elements. Thus, again $\mathbf{F}[V]^H$ cannot be a complete intersection from the proposition above. Finally, for $p = 7$ the corresponding numbers are $\dim(H_1(\mathbf{F}[V]^H)) = 401$ and a minimal generating set consists of at most 27 elements, so it cannot be a complete intersection too.

Conjecture 4.4.2.7. *Suppose V is a four-dimensional $\mathbf{F}H$-module of type-$(2,1,1)$ as above. Then V is a complete intersection that is not Cohen-Macaulay.*

4.4.3 Case $b_{1,3} = 0$

We recall from Theorem 2.3.0.6 that when $b_{1,3} = 0$ we have two distinct cases. If V is decomposable, with the right choice of basis the group of representing matrices is generated by

$$A := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B := \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & b_{2,3} & 0 \\ 0 & 0 & 1 & b_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

while if V is indecomposable by

$$A := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & b_{2,3} & 0 \\ 0 & 0 & 1 & b_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

So we distinguish between the subcases where $b_{1,4} = 0$ and $b_{1,4} \neq 0$.

Subcase $b_{1,4} = 0$: Note that when $b_{1,4} = 0$, H fixes x_4 and acts on the first three variables like the three-dimensional generic case. Therefore, a generating set of the invariant ring $\mathbf{F}[V]^H$ is given from Theorem 3.2.0.8 including x_4.

Subcase $b_{1,4} \neq 0$: Let $\langle A \rangle \triangleleft \langle A, C \rangle \triangleleft \langle A, B \rangle = H$ be a composition series where

$$C := [A, B] = ABA^{-1}B^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & b_{3,4} - b_{2,3} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

From equation (4.4.1) we have $\mathbf{F}[V]^{\langle A \rangle}[x_1^{-1}] = \mathbf{F}[x_1, \delta, \mathbf{N}_A(x_2), x_4][x^{-1}]$. Set $H_2 := \langle A, C \rangle$. Then $\mathbf{F}[V]^{H_2}[x_1^{-1}] = \mathbf{F}[x_1, \delta, \mathbf{N}_A(x_2), x_4]^{\langle C \rangle}[x^{-1}]$ and we shift to degree one the generators $y_1 := \delta/x_1, y_2 := \mathbf{N}_A(x_2)/x_1^{p-1}$ to obtain a new $\mathbf{F}\langle C \rangle$-module $W := \mathrm{Span}_{\mathbf{F}}\{x_1, y_1, y_2, x_4\}$. On this new basis $\{x_1, y_1, y_2, x_4\}$ we have

$$x_1 \cdot C := x_1 \quad , \quad y_1 \cdot C := y_1 - 2(b_{3,4} - b_{2,3})x_1$$
$$y_2 \cdot C := y_2 \quad , \quad x_4 \cdot C := x_4.$$

The last imply that the $\langle C \rangle$-action on W is Nakajima, hence we obtain after clearing minimally the denominators $\mathbf{F}[V]^{H_2}[x_1^{-1}] = \mathbf{F}[x_1, \mathbf{N}_C(\delta), \mathbf{N}_A(x_2), x_4][x_1^{-1}]$. We shall extend the algebra generators of the right-hand side to a SAGBI basis of $\mathbf{F}[V]^{H_2}$. In the set $\{x_1, \mathbf{N}_C(\delta), \mathbf{N}_A(x_2), x_4\}$, there is a unique non-trivial tête-à-tête: $(\mathbf{N}_C(\delta), \mathbf{N}_A^2(x_2))$.

Lemma 4.4.3.1. *Subducting the tête-à-tête* $(\mathbf{N}_C(\delta), \mathbf{N}_A^2(x_2))$*, defines an invariant with lead term:* $2x_2^{p+1}x_1^{p-1}$

Proof. Set $\widehat{g_1} := \mathbf{N}_C(\delta) - \mathbf{N}_A^2(x_2)$. Expanding the definition of $\widehat{g_1}$ gives immediately $\mathrm{LT}(\widehat{g_1}) = 2x_2^{p+1}x_1^{p-1}$. □

Let $g_1 := \widehat{g_1}/2x_1^{p-1}$ and $\mathfrak{B} := \{x_1, \mathbf{N}_A(x_2), g_1, \mathbf{N}_A(x_3), x_4\}$. We note that $\mathbf{N}_C(\delta)$ is redundant after g_1 has been attached. In $\mathfrak{B}$ there is a unique non-trivial tête-à-tête : $(g_1^p, \mathbf{N}_A^{p+1}(x_2))$.

Lemma 4.4.3.2. *The tête-à-tête* $(g_1^p, \mathbf{N}_A^{p+1}(x_2))$ *subducts to zero.*

Now in $\mathfrak{B}$ every non-trivial tête-à-tête subducts to zero.

Lemma 4.4.3.3. $\mathbf{F}[V]^{H_2} = \mathbf{F}[x_1, \mathbf{N}_A(x_2), g_1, \mathbf{N}_A(x_3), x_4]$.

Proof. In $\mathfrak{B}$ every non-trivial tête-à-tête subducts to zero, hence it is a SAGBI basis. Now our claim follows by an application of Theorem 1.4.3.10. □

Moreover, the invariant g_1 constructed above is of minimum x_3-degree with $\deg_{x_3}(g_1) = p$, hence we have in addition an equality of fields.

Lemma 4.4.3.4. $\mathbf{F}(V)^{H_2} = \mathbf{F}(x_1, \mathbf{N}_A(x_2), g_1, x_4)$.

Proof. Follows by an application of Theorem 1.4.2.6. □

Now because of the field inclusion $\mathbf{F}(V)^H \subset \mathbf{F}(V)^{H_2}$, we have obtained a lower bound for the minimum degree invariants. Follows directly that $\{x_1, \mathbf{N}_H(x_2)\}$ are of minimum degree in the first two variables. Furthermore, follows easily that the polynomial $q_1 := x_2^p - (b_{3,4}^p - b_{3,4})x_4 x_1^{p-1} - x_2 x_1^{p-1}$, forms an H-invariant of minimum x_4-degree too. Regarding the minimum x_3-degree invariant, from the field inclusion we know that has x_3-degree at least p. Therefore suffices to construct an H-invariant with that virtue.

Lemma 4.4.3.5. *The polynomial*

$$q_2 := \mathbf{N}_A^2(x_2) + \gamma_1 \cdot x_1^{p-1} g_1 - \gamma_2 \cdot x_1^p \mathbf{N}_A(x_2),$$

where

$$\begin{aligned} \gamma_1 &:= \frac{(p-1)/2 \cdot b_{3,4}^p + (p+1)/2 \cdot b_{3,4}}{(b_{2,3}^p - b_{3,4})}, \\ \gamma_2 &:= \frac{b_{2,3}^p(b_{3,4}^{2p} - 2b_{3,4}^{p+1} + b_{3,4}^2) + \sum_{i=1}^{p-1} b_{2,3}^i(-b_{3,4}^{2p+1-i} + b_{3,4}^{2p-i} + b_{3,4}^{p+2-i} - b_{3,4}^{p+1-i})}{(b_{2,3}^p - b_{3,4})(b_{3,4}^p - b_{3,4})}, \end{aligned}$$

is an H-invariant of minimum x_3-degree. Therefore, $\mathbf{F}(V)^H = \mathbf{F}(x_1, \mathbf{N}_H(x_2), q_1, q_2)$.

Proof. That $q_2 \in \mathbf{F}[V]^H$ follows from a routine calculation on $\Delta_B(q_2) = 0$, $\Delta_B := B - 1 \in \mathbf{F}H$. The field equality as an application of Theorem 1.4.2.6. □

Set $\mathscr{B} := \{x_1, \mathbf{N}_H(x_2), q_1, q_2\}$, with $\mathrm{LT}(\mathbf{N}_H(x_2)) = x_2^{p^2}, \mathrm{LT}(q_1) = x_2^p, \mathrm{LT}(q_2) = x_2^{2p}$. We shall extend this set to a SAGBI basis of $\mathbf{F}[V]^H$. The first tête-à-tête is: $(\mathbf{N}_H(x_2), q_1^p)$.

Lemma 4.4.3.6. *Subducting the tête-à-tête* $(\mathbf{N}_H(x_2), q_1^p)$*, defines an invariant with lead term:* $(b_{3,4}^{p^2} - b_{3,4}^p)x_4^p x_1^{p^2-p}$.

Proof. Set $\widehat{q_3} := \mathbf{N}_H(x_2) - q_1^p$. Observe that the second in term order of the norm $\mathbf{N}_H(x_2)$ has x_1-degree $p^2 - p$. Expanding the definition of q_1 follows immediately that $\mathrm{LT}(\widehat{q_3}) = (b_{3,4}^{p^2} - b_{3,4}^p) \cdot x_4^p x_1^{p^2-p}$. □

Let $q_3 := \widehat{q_3}/(b_{3,4}^{p^2} - b_{3,4}^p)x_1^{p^2-p}$ and $\mathscr{B}_1 := (\mathscr{B} \setminus \{\mathbf{N}_H(x_2)\}) \cup \{q_3\}$. Thus, $\mathscr{B}_1 = \{x_1, q_1, q_2, q_3\}$ and (q_1^2, q_2) forms the unique non-trivial tête-à-tête in $\mathscr{B}_1$.

Lemma 4.4.3.7. *Subducting the tête-à-tête* (q_1^2, q_2)*, defines an invariant with lead term:* $-2(b_{3,4}^p - b_{3,4})x_4 x_2^p x_1^{p-1}$.

Proof. Set $\widehat{q_4} := q_1^2 - q_2$. Expanding the definition of each part and take the difference gives immediately our claim: $\mathrm{LT}(\widehat{q_3}) = -2(b_{3,4}^p - b_{3,4})x_4 x_2^p x_1^{p-1}$. □

Let $q_4 := \widehat{q_4}/ - 2(b_{3,4}^p - b_{3,4})x_1^{p-1}$ and $\mathscr{B}_2 := (\mathscr{B}_1 \setminus \{q_2\}) \cup \{q_4\}$. Thus, $\mathscr{B}_2 = \{x_1, q_1, q_3, q_4\}$ and $(q_4^p, q_3 q_1^p)$ forms a unique non-trivial tête-à-tête .

Lemma 4.4.3.8. *Subducting the tête-à-tête* $(q_4^p, q_3 q_1^p)$*, defines an invariant with lead term:* $-(b_{2,3}^p - b_{3,4} - \delta_2)/(b_{2,3}^p - b_{3,4})^{p+1} \cdot x_2^{p^2+1} x_1^{p-1}$*, where* $\delta_2 := (b_{2,3}^{p^2} - b_{3,4})/(b_{2,3}^{p^2} - b_{3,4}^p)$.

Proof. Set $s_1 := q_4^p - q_3 q_1^p$. Then modulo $\langle x_1^p \rangle \lhd \mathbf{F}[V]$: $q_4^p \equiv_{\langle x_1^p \rangle} x_4^p x_2^{p^2} + 1/(b_{2,3}^{p^2} - b_{3,4}^p) \cdot x_2^{p^2+p}, q_3 q_1^p \equiv_{\langle x_1^p \rangle} x_4^p x_2^{p^2} - 1/(b_{3,4}^p - b_{3,4}) \cdot x_2^{p^2+p}$. Therefore, $\mathrm{LT}(s_1) = \delta_1 \cdot x_2^{p^2+p}$, where $\delta_1 := (b_{2,3}^{p^2} - b_{3,4})/(b_{2,3}^{p^2} - b_{3,4}^p)(b_{3,4}^p - b_{3,4})$.

For the next step we set: $s_2 := s_1 - \delta_1 q_1^{p+1}$. Modulo $\langle x_1^p \rangle \lhd \mathbf{F}[V]$ each part yields: $s_1 \equiv_{\langle x_1^p \rangle} \delta_1 x_2^{p^2+p} - 1/(b_{3,4}^p - b_{3,4}) \cdot x_2^{p^2+1} x_1^{p-1}, q_1^{p+1} \equiv_{\langle x_1^p \rangle} x_2^{p^2+p} - (b_{3,4}^p - b_{3,4})x_4 x_2^{p^2} x_1^{p-1} - x_2^{p^2+p} x_1^{p-1}$. Thus, for this second step $\mathrm{LT}(s_2) = \delta_2 \cdot x_4 x_2^{p^2+1} x_1^{p-1}$, $\delta_2 := (b_{2,3}^{p^2} - b_{3,4})/(b_{2,3}^{p^2} - b_{3,4}^p)$.

Finally, let $s_3 := s_2 - \delta_2 x_1^{p-1} q_1^{p-1} q_4$. Expanding the definition of each part and reducing modulo $\langle x_1^p \rangle$: $x_1^{p-1} q_1^{p-1} q_4 \equiv_{\langle x_1^p \rangle} x_4 x_2^{p^2} x_1^{p-1} + 1/(b_{2,3}^p - b_{3,4}) \cdot x_2^{p^2+1} x_4^{p-1}$. Summarizing the aforementioned yields: $\mathrm{LT}(s_3) = -(b_{2,3}^p - b_{3,4} - \delta_2)/(b_{2,3}^p - b_{3,4})^{p+1} \cdot x_2^{p^2+1} x_1^{p-1}$. □

We set $q_5 := s_3/\delta_3 x^{p-1}$ and $\mathscr{B}_3 := \mathscr{B}_2 \cup \{q_5\}$. In this new set there is a unique tête-à-tête: $(q_5^p, q_1^{p^2+1})$.

Lemma 4.4.3.9. *Subducting the tête-à-tête* $(q_5^p, q_1^{p^2+1})$*, defines an invariant with lead term:* $(b_{2,3}^{p^2} - b_{3,4}^p)/(b_{2,3}^{p^3} - b_{2,3}^{p^2}) \cdot x_3^{p^3} x_1^{p^2}$.

Proof. Let $t_1 := q_5^p - q_1^{p^2+1}$ denote the tête-à-tête difference. Expanding the definition of both invariants and reducing modulo $\langle x_1^{p+1} \rangle \lhd \mathbf{F}[V]^H$: $q_5^p \equiv_{\langle x_1^{p+1} \rangle} x_2^{p^3+p} + (b_{2,3}^{p^2} - b_{3,4}^p)/(b_{2,3}^{p^3} - b_{2,3}^{p^2}) \cdot x_3^{p^3} x_1^p - (b_{2,3}^{p^3} - b_{3,4}^p)/(b_{2,3}^{p^3} - b_{2,3}^{p^2}) \cdot x_3^{p^2} x_2^{p^3-p^2} x_1^p$, $q_1^{p^2+1} \equiv_{\langle x_1^{p+1} \rangle} x_2^{p^3+p} - (b_{3,4}^p - b_{3,4}) x_4 x_2^{p^3} x_1^{p-1} - x_2^{p^3+1} x_1^{p-1}$. Thus we have

$$\begin{aligned} t_1 \quad \equiv_{\langle x_1^{p+1} \rangle} \quad & (b_{3,4}^p - b_{3,4}) x_4 x_2^{p^3} x_1^{p-1} + x_2^{p^3+1} x_1^{p-1} + (b_{2,3}^{p^2} - b_{3,4}^p)/(b_{2,3}^{p^3} - b_{2,3}^{p^2}) \cdot x_3^{p^3} x_1^p \\ - \quad & (b_{2,3}^{p^3} - b_{3,4}^p)/(b_{2,3}^{p^3} - b_{2,3}^{p^2}) \cdot x_3^{p^2} x_2^{p^3-p^2} x_1^p \end{aligned}$$

Let $t_2 := t_1 - (b_{3,4}^p - b_{3,4}) x_1^{p-1} q_1^{p^2-1} q_4$. Reducing modulo $\langle x_1^p \rangle$ the second part of t_2: $x_1^{p-1} q_1^{p^2-1} q_4 \equiv_{\langle x_1^p \rangle} x_4 x_2^{p^3} x_1^{p-1} + 1/(b_{2,3}^p - b_{3,4}) \cdot x_2^{p^3+1} x_1^{p-1}$. Forming the difference of the two parts yields our assertion: $\mathrm{LT}(t_2) = (b_{2,3}^{p^2} - b_{3,4}^p)/(b_{2,3}^{p^3} - b_{2,3}^{p^2}) \cdot x_3^{p^3} x_1^p$. □

Finally we set $q_6 = -(b_{2,3}^{p^3} - b_{3,4}^{p^2}) \cdot t_4 / x_1^{p^2}$ and $\mathscr{B}_3 := \{x_1, q_1, q_3, q_4, q_5, q_6\}$. Now every tête-à-tête in $\mathscr{B}_3$ subducts to zero. Since $\mathrm{LT}(\mathbf{N}_H(x_3)) = \mathrm{LT}(q_6)$, we swap these two elements in $\mathscr{B}_3$ to obtain a more natural generating set. Therefore we conclude to the following theorem.

Theorem 4.4.3.10. *Let V denote a four-dimensional indecomposable left $\mathbf{F}H$-module of type-$(2,1,1)$, such that $b_{1,3} = 0$. Then $\mathscr{B}_3$ as described above, forms a SAGBI basis for $\mathbf{F}[V]^H$. In particular, the ring of invariants $\mathbf{F}[V]^H$ in that case is a complete intersection with generating relations constructed during the tête-à-tête subductions. Finally, we have* $\mathrm{LT}(\mathbf{F}[V]^H) = \mathbf{F}[x_1, x_2^p, x_2^{p^2+1}, x_3^{p^3}, x_4 x_2^p, x_4^p]$.

Appendices

Appendix A

MAGMA functions

To understand the behaviour of invariant rings and verify our claims, many times in this thesis we use the computational algebra system MAGMA. Many of the functions we use are built-in, however there are also others which have been developed independently for invariant-theoretic purposes.

For example, the SAGBI/divide-by-x algorithm starts with a finite subset and subducts all the non-trivial tête-à-têtes . This procedure stops when all the non-trivial tête-à-têtes have subducted and a SAGBI basis is returned. If the initial set has been chosen carefully, then the resulting SAGBI basis is a generating set of $\mathbf{F}[x_1, \ldots, x_n]^G$ too. MAGMA has no built-in functions to do all this. Among many, R.J. Shank and David Wehlau have constructed MAGMA functions that can do all the above.

Given a subset $\mathcal{B} := \{f_1, \ldots, f_n\} \subset \mathbf{F}[V]^G$ (for example the minimum degree homogeneous generators of $\mathbf{F}(V)^G$) and a tête-à-tête (f^I, f^J), where $f^I = f_1^{i_1} \ldots f_n^{i_n}$ for $I := (i_1, \ldots, i_n)$, the subduction $\textsc{subd}(f^I - f^J, \mathcal{B})$ can be a very painful (and many times impossible) procedure to be done by hand. The `subd`() function presented below can simplify the subduction idea and be used to carry out very complex tête-à-tête subductions. Before that we present the `factor()` function which is used in `subd`() to perform a monomial factoring:

```
factor := function(mon,mseq,j)
    if LeadingMonomial(mon) eq 1
          then exp:=[0 : m in mseq];
               return true, exp;
        end if;
    for i in [j..#mseq] do
        if IsDivisibleBy(mon,mseq[i]) then
            newmon:= mon div mseq[i];
            Test,exp:=$$(newmon,mseq,i);
            if Test then
                exp[i]:=exp[i]+1;
                return true, exp;
            end if;
        end if;
    end for;
    return false, [];
end function;

subd := function(poly,gen)
        for i in [1..#gen] do
          gen[i] := gen[i] div LeadingCoefficient(gen[i]);
        end for;
    ltgen:=[LeadingTerm(m) : m in gen];
    RP:=poly;
    while RP ne 0 do
        RM:=LeadingMonomial(RP);
        Test, exp := factor(RM,ltgen,1);
        if Test eq false then return RP;
        else
            Adj:=&*[gen[i]^exp[i] : i in [1..#gen]];
            RP:=RP-LeadingCoefficient(RP)*Adj;
```

```
        end if;
    end while;
    return RP;
end function;
```

So given poly $= f^I - f^J$, gen $:= \mathcal{B}$, we are capable every time to subtract off the leading term of the previous step based on the elements of $\mathcal{B}$ until no further subtraction can be made. Hence, the returned polynomial is the seeking subduction.

As an extension of the previous algorithm, R.J. Shank and David Wehlau constructed another useful function called `sagbi()`. This one uses the toric ideal method in [24, pg.32-33] to track down the tête-à-têtes of $\mathcal{B}$ and the `subd()` function to subduct them. Every non-zero subduction is returned and appended on the previous calculated set after normalization and the procedure starts again. When the function returns the empty set we have a SAGBI basis.

```
sagbi:=function(gen)
    for i in [1..#gen] do
      gen[i] := gen[i] div LeadingCoefficient(gen[i]);
    end for;

    ltgen:=[LeadingTerm(m):m in gen];
    S:=Parent(gen[1]);
    T:=PolynomialRing(CoefficientRing(Parent(gen[1])),#ltgen,"grevlex");
    F:=hom<T->S|ltgen>;
    f:=hom<T->S|gen>;
    time I:=PolyMapKernel(F);#Basis(I);
    miss:=[]; tat := [];
    for j in [1..#Basis(I)] do
            test:=subd(f(Basis(I)[j]),gen);
            if test ne 0
              then Append(~miss,test div LeadingCoefficient(test));
```

```
                Append(~tat ,Basis(I)[j]);
            end if;
    end for;
    return miss, tat, Basis(I);
end function;
```

Bibliography

[1] W. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics vol. 3, The American Mathematical Society, 1994.

[2] J. L. Alperin, *Local representation theory*, Cambridge University Press (1986).

[3] D. J. Benson, *Polynomial invariants of finite groups,* volume 190. Cambridge University Press, 1993

[4] W. Bruns, J. Herzog, *Cohen-Macaulay rings*, Cambridge Studies in Advanced Mathematics 39, Cambridge University Press, 1993

[5] S. Bullett, T. Fearn, F. Smith *Algebra, Logic and Combinatorics*, LTCC Advanced Mathematics Series: Volume 3, World Scientific.

[6] H. E. A. Campbell, J. Chuai, *Invariant Fields and Localized Invariant rings of p-groups,* Quarterly J. of Math. **58** (2007) 151 – 157.

[7] H. E. A. Campbell, R.J. Shank, D. L. Wehlau, *Ring of Invariants for modular representations of elementary abelian p-groups,* Transformation Groups **18** (2013) no. 1, 1 – 22.

[8] H. E. A. Campbell, D. L. Wehlau, *Modular Invariant Theory*, Encyclopaedia of Math. Sci. **139**, Invariant Theory and Algebraic Transformation Groups, VIII, Springer-Verlag, Berlin, 2011, Encyclopaedia of Mathematical Sciences.

[9] H. Derksen, G. Kemper (2002), *Computational invariant theory,* Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin, 2002, Encyclopaedia of Mathematical Sciences.

[10] M. Hochster, J. A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. **93** (1971), 1020-1058.

[11] Horan, K. and Fleischmann, P. *The finite unipotent groups consisting of bireflections.* Journal of Group Theory [Online] **22:191-230**. Available at: https://doi.org/10.1515/jgth-2018-0123.

[12] G. Kemper, *On the Cohen-Macaulay Property of Modular Invariant Rings*, Journal of Algebra Volume **215**, Issue **1**, 1 May 1999, Pages 330 − 351.

[13] H. Matsumura *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics 8, Cambridge University Press (1986).

[14] T. Miyata, *Invariants of Certain Groups. I*, Nagoya Math. J. vol. **41** (1971), 69-73.

[15] H. Mui, *Modular invariant theory and cohomology algebras of symmetric groups*, J. of Fac. Sci. Univ. Tokyo Sect. 1A Math. **22** (1975), 319-369.

[16] H. Nakajima, *Regular rings of invariants for unipotent groups,* J. Algebra **80** (1983), no. 2, 279-294.

[17] E. Noether, *"Der Endlichkeitsatz der Invarianten endlicher linearer Gruppen der Charakteristik p"*, Nachr. v. d. Ges. d. Wiss. zu Göttingen (1926), 28-35.

[18] Parsons, Christopher M. (2018) *Modular Representations and Invariants of Elementary Abelian p-Groups*, Doctor of Philosophy (PhD) thesis, University of Kent.

[19] D. J. S. Robinson, *A course in the theory of groups*, Springer-Verlag New York Inc., v.80, 1980.

[20] M. Sezer, R. James Shank, *On the coinvariants of modular representations of cyclic groups of prime order*, Journal of Pure and Applied Algebra 205 (2006) 210-225.

[21] M. Sezer, R. J. Shank, *Rings of invariants for modular representations of the Klein four group*, Transactions of the American Mathematical Society 368 (2016) no. 8, 5655 – 5673.

[22] R. J. Shank, *SAGBI bases for rings of formal modular seminvariants,* Comment. Math. Helv. 73 (1998), pp. 548-565.

[23] R. P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bulletin of the Amer. Math. Soc. (N.S.) **1** (1979), no. 3, 475-511.

[24] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Ser. **8**, Amer. Math. Society, 1996.