

# VECTOR INVARIANTS FOR THE TWO DIMENSIONAL MODULAR REPRESENTATION OF A CYCLIC GROUP OF PRIME ORDER

H E A CAMPBELL, R J SHANK, AND D L WEHLAU

ABSTRACT. In this paper, we study the vector invariants of the 2-dimensional indecomposable representation  $V_2$  of the cyclic group,  $C_p$ , of order  $p$  over a field  $\mathbf{F}$  of characteristic  $p$ ,  $\mathbf{F}[mV_2]^{C_p}$ . This ring of invariants was first studied by David Richman [21] who showed that the ring required a generator of degree  $m(p-1)$ , thus demonstrating that the result of Noether in characteristic 0 (that the ring of invariants of a finite group is always generated in degrees less than or equal to the order of the group) does not extend to the modular case. He also conjectured that a certain set of invariants was a generating set with a proof in the case  $p=2$ . This conjecture was proved by Campbell and Hughes in [3]. Later, Shank and Wehlau in [24] determined which elements in Richman's generating set were redundant thereby producing a minimal generating set.

We give a new proof of the result of Campbell and Hughes, Shank and Wehlau giving a minimal algebra generating set for the ring of invariants  $\mathbf{F}[mV_2]^{C_p}$ . In fact, our proof does much more. We show that our minimal generating set is also a SAGBI basis for  $\mathbf{F}[mV_2]^{C_p}$ . Further, our results provide a procedure for finding an explicit decomposition of  $\mathbf{F}[mV_2]$  into a direct sum of indecomposable  $C_p$ -modules. Finally, noting that our representation of  $C_p$  on  $V_2$  is as the  $p$ -Sylow subgroup of  $SL_2(\mathbf{F}_p)$ , we describe a generating set for the ring of invariants  $\mathbf{F}[mV_2]^{SL_2(\mathbf{F}_p)}$  and show that  $(p+m-2)(p-1)$  is an upper bound for the Noether number, for  $m > 2$ .

## CONTENTS

1. Introduction	2
2. Preliminaries	5
2.2. Relations involving the $u_{ij}$	6
3. Polarisation	8
4. Partial Dyck Paths	10
5. Lead Monomials	11

---

*Date:* November 20, 2009.

*1991 Mathematics Subject Classification.* 13A50.

6. A Generating Set	16
7. Decomposing $\mathbf{F}[mV_2]$ as a $C_p$ -module	21
8. A First Main Theorem for $SL_2(\mathbf{F}_p)$	24
References	28

## 1. INTRODUCTION

We suppose  $G$  is a group represented on a vector space  $V$  over a field  $\mathbf{F}$ . If  $\{x_1, x_2, \dots, x_n\}$  is a basis for the hom-dual,  $V^* = \text{hom}_{\mathbf{F}}(V, \mathbf{F})$ , of  $V$ , then we denote the symmetric algebra on  $V^*$  by

$$\mathbf{F}[V] = \mathbf{F}[x_1, x_2, \dots, x_n]$$

and we note that  $G$  acts on  $f \in \mathbf{F}[V]$  by the rule

$$\sigma(f)(v) = f(\sigma^{-1}(v)).$$

As an aside, the notation  $\mathbf{F}[V]$  is often used in the literature to denote the ring of regular functions on  $V$ . Our notation coincides with the usual notion when the field  $\mathbf{F}$  is infinite. However, for example, if  $\mathbf{F} = \mathbf{F}_p$ , the prime field, then the functions  $x_1$  and  $x_1^p$  coincide on  $V$ .

The ring of functions left invariant by this action of  $G$  is denoted  $\mathbf{F}[V]^G$ . Invariant theorists often seek to relate algebraic properties of the invariant ring to properties of the representation. For example, when  $G$  is finite of order  $|G|$  and the characteristic  $p$  of  $\mathbf{F}$  does *not* divide  $|G|$  – the *non-modular* case – then  $\mathbf{F}[V]^G$  is a polynomial algebra if and only if  $G$  is generated by reflections (group elements fixing a hyperplane of  $V$ ). This is a famous result due to Coxeter [8], Shephard and Todd [26], Chevalley [6], and Serre [22]. For another example in the non-modular case, it is known by work of Noether [19] (when  $p = 0$ ), Fogarty [12] and Fleischmann [13] (when  $p > 0$ ), that  $\mathbf{F}[V]^G$  is generated in degrees less than or equal to  $|G|$ . And, in the non-modular case with  $G$  finite, it is well-known that  $\mathbf{F}[V]^G$  is always Cohen-Macaulay.

The case when  $p > 0$ ,  $G$  is finite,  $V$  is finite dimensional and  $p$  does divide  $|G|$  is that of modular invariant theory. Many results that are well understood in the non-modular case are not yet understood or even within reach in the modular case. For example, in the modular case it is known that if  $\mathbf{F}[V]^G$  is a polynomial algebra then  $G$  must be generated by reflections, but this is far from sufficient. For another example, in the modular case  $\mathbf{F}[V]^G$  is “most often” not Cohen-Macaulay. Finally, in the modular case, there are examples where  $\mathbf{F}[V]^G$  requires generators of degrees (much) larger than  $|G|$ , see below: this paper re-examines the first known such example in considerable detail.

There are now several references for modular invariant theory, see Benson [1], Smith[27], Neusel and Smith[18], Derksen and Kemper[9], Campbell and Wehlau[3].

Invariant theorists also seek to determine generators for  $\mathbf{F}[V]^G$  and, if possible, relations among those generators. A famous example is the case of *vector invariants*, see Weyl [28]. Here we consider the vector space

$$mV = \overbrace{V \oplus V \oplus \cdots \oplus V}^{m \text{ summands}}$$

with  $G$  acting diagonally. The invariants  $\mathbf{F}[mV]^G$  are called vector invariants, and in this case, we seek to describe, determine or give constructions for, the generators of this ring, a *first main theorem for*  $(G, V)$ . Once this is done a theorem determining the relations among the generators is referred to as a *second main theorem for*  $(G, V)$ .

The cyclic group  $C_p$  has exactly  $p$  inequivalent indecomposable representations over a field  $\mathbf{F}$  of characteristic  $p$ . There is one indecomposable  $V_n$  of dimension  $n$  for each  $1 \leq n \leq p$ . To see this choose a basis for  $V_n$  with respect to which a fixed generator,  $\sigma$ , of  $C_p$  is represented by a matrix in Jordan Normal form. Since  $V_n$  is indecomposable this matrix has a single Jordan block and since  $\sigma$  has order  $p$  the common eigenvalue must be 1, the only  $p^{\text{th}}$  root of unity in a field of characteristic  $p$ . Thus  $\sigma$  is represented on  $V_n$  by the matrix

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

In order that this matrix have order  $p$  (or 1) we must have  $n \leq p$ . We call such a basis of  $V_n$  for which  $\sigma$  is in (lower triangular) Jordan Normal form a *triangular* basis.

Observe the following chain of inclusions:

$$V_1 \subset V_2 \subset \cdots \subset V_p.$$

If  $V$  is any finite dimensional  $C_p$ -module then  $V$  can be decomposed into a direct sum of indecomposable  $C_p$ -modules:

$$V \cong m_1 V_1 \oplus m_2 V_2 \cdots \oplus m_p V_p$$

where  $m_i \in \mathbb{N}$  for all  $i$ . This decomposition is far from unique but does have the property that the *multiplicities*  $m_\ell$  are unique.

We are interested in the representation  $mV_2$  and the action of  $C_p$  on  $\mathbf{F}[mV_2]$ . The ring of invariants  $\mathbf{F}[mV_2]^{C_p}$  was first studied by David Richman [21]. He showed that this ring required a generator of degree  $m(p-1)$ , showing that the result of Noether in characteristic 0 did not extend to the modular case. He also conjectured that a certain set of invariants was a generating set with a proof in the case  $p=2$ . This conjecture was proved by Campbell and Hughes in [3]: the proof is long, complex, and counter-intuitive in some respects. Later, Shank and Wehlau in [24] determined which elements in Richman's generating set were redundant thereby producing a minimal generating set.

We will show later (and the proof is not difficult), that  $\mathbf{F}[mV_2]^{C_p}$  is not Cohen-Macaulay, or see Ellingsrud and Skjelbred [11].

In this paper, we give a new proof of the result of Campbell and Hughes, Shank and Wehlau giving a minimal algebra generating set for the ring of invariants  $\mathbf{F}[mV_2]^{C_p}$ . In fact, our proof does much more. We show that our minimal generating set is also a SAGBI basis for  $\mathbf{F}[mV_2]^{C_p}$ . In our view, this result is extraordinary. Further, our techniques also yield a procedure for finding a decomposition of  $\mathbf{F}[mV_2]$  into a direct sum of indecomposable  $C_p$ -modules.

Our paper is organised as follows. In the second section of our paper, Preliminaries, we provide more details on the the representation theory of  $C_p$ , our use of graded reverse lexicographical ordering on the monomials in  $\mathbf{F}[mV_2]^{C_p}$ , and define the term *SAGBI* basis. In the next section, Polarisation, we define the polarisation map  $\mathbf{F}[V] \rightarrow \mathbf{F}[mV]$ , its (roughly speaking) inverse, known as restitution, and we note that these maps are  $G$ -equivariant, hence map  $G$ -invariants to  $G$ -invariants. These techniques allow us to focus our attention on multi-linear invariants. The next section, Partial Dyck Paths, describes a concept arising in the study of lattices in the plane, see, for example the book by Koshy [17, p. 151], and is followed by a section on Lead Monomials. Here we show that there is a bijection between the set of lead monomials of multi-linear invariants and certain collections of Partial Dyck Paths. This work requires us to count the number of indecomposable  $C_p$  summands in

$${}^m\otimes V_2 = \overbrace{V_2 \otimes V_2 \otimes \cdots \otimes V_2}^{m \text{ copies}},$$

and in fact we are able to determine a decomposition of  ${}^m\otimes V_2$  as a  $C_p$ -module, see Theorem 5.5. Following this, in section § 6, we prove that we have a generating set for our ring of invariants. The next section describes how our techniques provide a procedure for finding

a decomposition of  $\mathbf{F}[mV_2]$  as a  $C_p$ -module. In the final section, noting that our representation of  $C_p$  on  $V_2$  is as the  $p$ -Sylow subgroup of  $SL_2(\mathbf{F}_p)$ , we are able to describe a generating set for the ring of invariants  $\mathbf{F}[mV_2]^{SL_2(\mathbf{F}_p)}$ .

We thank the referee for a thorough and careful reading of our paper.

## 2. PRELIMINARIES

Suppose  $\{e_1, e_2, \dots, e_n\}$  is a triangular basis for  $V_n$ . Note that the  $C_p$ -module generated by  $e_1$  is all of  $V_n$ . We also note that the indecomposable module  $V_n^* = \text{hom}(V_n, \mathbf{F})$  is isomorphic to  $V_n$  since  $\dim(V_n^*) = \dim(V_n)$ . Because of our interest in invariants we often focus on the  $C_p$  action on  $V_n^*$  rather than on  $V_n$  itself. Therefore we will choose the dual basis  $\{x_1, x_2, \dots, x_n\}$  for  $V^*$  to the basis  $\{e_1, e_2, \dots, e_n\}$ . With this choice of basis the matrices representing  $G$  are upper-triangular on  $V^*$ . We note that  $\sigma^{-1}(x_1) = x_1$  and  $\sigma^{-1}(x_i) = x_i + x_{i-1}$  for  $2 \leq i \leq n$ : for convenience, and since  $\sigma^{-1}$  also generates  $C_p$ , we will change notation and write  $\sigma$  instead of  $\sigma^{-1}$  for the remainder of this paper. With this convention, we note that  $(\sigma - 1)^r(x_n) = x_{n-r}$  for  $r < n$  and  $\dim(V_n) = n$  is the largest value of  $r$  such that  $x_1 \in (\sigma - 1)^{r-1}(V_n^*)$ . We say that the invariant  $x_1$  has *length*  $n$  in this case and write  $\ell(x_1) = n$ . We observe that the socle of  $V_n$  is the line  $V_n^{C_p}$  spanned by  $\{e_n\}$ . Similarly  $(V_n^*)^{C_p}$  has basis  $\{x_1\}$ .

Note that the kernel of  $\sigma - 1 : V_i \rightarrow V_i$  is  $V_i^{C_p}$  which is one dimensional for all  $i$ . Thus

$$\dim((\sigma - 1)^j(V_i)) = \begin{cases} 0 & \text{if } j - 1 \geq i; \\ i - j & \text{if } j - 1 < i. \end{cases}$$

For

$$V \cong m_1 V_1 \oplus m_2 V_2 \cdots \oplus m_p V_p$$

this gives  $(p-j)m_p + (p-1-j)m_{p-1} + \cdots + (i-j)m_i = \dim((\sigma - 1)^j(V))$  for all  $0 \leq j \leq p-1$  and this system of equations uniquely determines the coefficients  $m_1, m_2, \dots, m_p$ .

Each indecomposable  $C_p$ -module,  $V_n$ , satisfies  $\dim(V_n)^{C_p} = 1$ . Therefore the number of summands occurring in a decomposition of  $V$  is given by  $m_1 + m_2 + \cdots + m_p = \dim V^{C_p}$ .

Consider  $\text{Tr} := \sum_{\tau \in C_p} \tau$ , an element of the group ring of  $C_p$ . If  $W$  is any finite dimensional  $C_p$ -representation, we also use  $\text{Tr}$  to denote the corresponding  $\mathbf{F}[W]^{C_p}$ -module homomorphism,

$$\text{Tr} : \mathbf{F}[W] \rightarrow \mathbf{F}[W]^{C_p}.$$

Similarly we define

$$N : \mathbf{F}[W] \rightarrow \mathbf{F}[W]^{C_p}$$

by  $N(w) = \prod_{\tau \in C_p} \tau(w)$ .

Note that  $(\sigma - 1)^{p-1} = \sum_{i=0}^{p-1} (-1)^i \binom{p-1}{i} \sigma^i = \sum_{i=0}^{p-1} \sigma^i = \text{Tr}$ . It follows that  $\text{Tr}(v) = 0$  if  $v \in V_n$  for  $n < p$ , while  $\text{Tr}(x_p) = x_1$  in  $V_p$ .

It is also the case that  $V_p \cong \mathbf{F}C_p$  is the only free  $C_p$ -module and hence also the only projective.

The next theorem plays an important role in our decomposition of  $\mathbf{F}[V]_{(d_1, d_2, \dots, d_m)}$  as a  $C_p$ -module (modulo projectives). A proof in the case  $V = V_n$  may be found in Hughes and Kemper [14, section 2.3], and a proof of the version cited here is in Shank and Wehlau [25, section 2]

**Theorem 2.1** (Periodicity Theorem). *Let  $V = V_{n_1} \oplus V_{n_2} \oplus \dots \oplus V_{n_m}$ . Let  $d_1, d_2, \dots, d_m$  be non-negative integers and write  $d_i = q_i p + r_i$  where  $0 \leq r_i \leq p - 1$  for  $i = 1, 2, \dots, m$ . Then*

$$\mathbf{F}[V]_{(d_1, d_2, \dots, d_m)} \cong \mathbf{F}[V]_{(r_1, r_2, \dots, r_m)} \oplus t V_p$$

as  $C_p$ -modules for some non-negative integer  $t$ .

Comparing dimensions shows that in the above theorem

$$t = \left( \prod_{i=1}^m \binom{n_i + d_i - 1}{d_i} - \prod_{i=1}^m \binom{n_i + r_i - 1}{r_i} \right) / p.$$

In this paper, we are primarily interested in the case  $V = m V_2$ . We denote the basis for the  $i^{\text{th}}$ -copy of  $V_2^*$  in this direct sum by  $\{x_i, y_i\}$  and we have  $\sigma(x_i) = x_i$  and  $\sigma(y_i) = y_i + x_i$ .

For this representation of  $C_p$ , there is another ‘‘obvious’’ family of invariants, namely the

$$u_{ij} = x_i y_j - x_j y_i = \begin{vmatrix} x_i & y_i \\ x_j & y_j \end{vmatrix}$$

for  $m \geq 2$ .

**2.2. Relations involving the  $u_{ij}$ .** We will consider now two important families of relations involving the invariants  $u_{ij} = x_i y_j - y_i x_j$ . First we consider algebraic dependencies among the  $u_{ij}$ . Suppose  $m \geq 4$  and let  $1 \leq i < j < k < \ell \leq m$ . It is easy to verify that  $0 = u_{ij} u_{k\ell} - u_{ik} u_{j\ell} + u_{i\ell} u_{jk}$ . It can be shown that these relations generate all the algebraic relations among the  $u_{st}$ .

It is useful to represent products of the various  $u_{st}$  graphically as follows. We consider the vertices of a regular  $m$ -gon and label them clockwise by  $1, 2, \dots, m$ . We represent the factor  $u_{ij}$  by an arrow or directed edge from vertex  $i$  to vertex  $j$ . Thus a product of various  $u_{st}$  is

represented by a number of directed edges joining the labelled vertices of the regular  $m$ -gon.

Returning to the relation  $u_{ij}u_{kl} - u_{ik}u_{jl} + u_{il}u_{jk}$ , we say that the middle product in this relation,  $u_{ik}u_{jl}$ , is a *crossing* since the arrows representing the two factors  $u_{ik}$  and  $u_{jl}$  cross (intersect). Rewriting the relation as  $u_{ik}u_{jl} = u_{ij}u_{kl} + u_{il}u_{jk}$ , we see that we may replace a crossing with a sum of two non-crossings. As observed by Kempe [16], since the length of two (directed) diagonals representing  $u_{ik}$  and  $u_{jl}$  exceeds both the lengths represented by the sides  $u_{ij}$  and  $u_{kl}$  and the two sides  $u_{il}$  and  $u_{jk}$ , we may repeatedly use “uncrossing” relations to rewrite any product of  $u_{st}$ ’s by a sum of such products without any crossings. Thus the space generated by the monomials in the  $u_{st}$  of degree  $d$  has a basis represented by planar directed graphs on  $m$  vertices having  $d$  directed edges. Here we allow multiple (or weighted) edges to represent powers such as  $u_{ij}^a$  for  $a \geq 2$ .

Now we consider another important class of relations, this time involving the  $u_{st}$  and the  $x_r$ . Take  $m \geq 3$ , let  $1 \leq i < j < k \leq m$  and consider the matrix

$$\begin{pmatrix} x_i & x_j & x_k \\ x_i & x_j & x_k \\ y_i & y_j & y_k \end{pmatrix}.$$

Computing the determinant by expanding along the first row we find  $x_i u_{jk} - x_j u_{ik} + x_k u_{ij} = 0$ . Since  $x_1, x_2, x_3$  is a partial homogeneous system of parameters in  $\mathbf{F}[mV_2]$  consisting of invariants it is a partial homogeneous system of parameters in  $\mathbf{F}[mV_2]^{C_p}$ . The relation  $x_1 u_{23} - x_2 u_{13} + x_3 u_{12} = 0$  shows that the product  $x_3 u_{12}$  represents 0 in the quotient ring  $\mathbf{F}[mV_2]^{C_p}/(x_1, x_2)$ . Considering degrees, it is easy to see that  $u_{12}$  and  $x_3$  do not lie in the ideal of  $\mathbf{F}[mV_2]^{C_p}$  generated by  $(x_1, x_2)$ . Thus  $x_3$  represents a zero divisor in the quotient ring  $\mathbf{F}[mV_2]^{C_p}/(x_1, x_2)$ . This shows that the partial homogeneous system of parameters  $x_1, x_2, x_3$  in  $\mathbf{F}[mV_2]^{C_p}$  does not form a regular sequence. Therefore  $\mathbf{F}[mV_2]^{C_p}$  is not a Cohen-Macaulay ring when  $m \geq 3$ . For  $m \leq 2$  the ring of invariants  $\mathbf{F}[mV_2]^{C_p}$  is Cohen-Macaulay since  $\mathbf{F}[V_2]^{C_p} = \mathbf{F}[x_1, N(y_1)]$  is a polynomial ring and  $\mathbf{F}[2V_2]^{C_p} = \mathbf{F}[x_1, x_2, u_{12}, N(y_1), N(y_2)]$  is a hypersurface ring.

Throughout this paper we will use graded reverse lexicographic term orders. We write  $\text{LM}(f)$  for the lead monomial of  $f$  and  $\text{LT}(f)$  for the lead term of  $f$ . We follow the convention that monomials are power products of variables and terms are scalar multiples of power products of variables. If  $S = \bigoplus_{d=0}^{\infty} S_d$  is a graded subalgebra of a polynomial ring then we say a set  $B$  is a *SAGBI basis* for  $S$  in degree  $d$  if for every  $f \in S_d$

we can write  $\text{LM}(f)$  as a product  $\text{LM}(f) = \prod_{g \in B} \text{LM}(g)^{e_g}$  where each  $e_g$  is a non-negative integer. If  $B$  is a SAGBI basis for  $S$  in degree  $d$  for all  $d$  then we say that  $B$  is a SAGBI basis for  $S$ . If  $B$  is a SAGBI basis for  $S$  then  $B$  is an algebra generating set for  $S$ . The word SAGBI is an acronym for “sub-algebra analogue of Gröbner bases for ideals”, and was introduced by Robbiano and Sweedler in [20] and (independently) by Kapur and Madlener in [15]. For a detailed discussion of term orders we direct the reader to Chapter 2 of Cox, Little and O’Shea [7]. For a discussion and application of SAGBI bases in modular invariant theory, we recommend Shank’s paper [23].

Given a sequence of variables  $z_1, z_2, \dots, z_m$  and an element  $E = (e_1, e_2, \dots, e_m)$  we write  $z^E$  to denote the monomial  $z_1^{e_1} z_2^{e_2} \dots z_m^{e_m}$  and we denote the degree  $e_1 + e_2 + \dots + e_m$  of this monomial by  $|E|$ .

The following well-known lemma is very useful for computing the lead term of a transfer.

**Lemma 2.3.** *Let  $t$  be a positive integer. Then*

$$\sum_{i=0}^{p-1} i^t = \begin{cases} -1, & \text{if } p-1 \text{ divides } t; \\ 0, & \text{if } p-1 \text{ does not divide } t. \end{cases}$$

For a proof of this lemma see for example, [5, Lemma 9.4].

### 3. POLARISATION

Let  $V$  be a representation of a group  $G$  and let  $r \in \mathbb{N}$  with  $r \geq 2$  and consider the map of  $G$ -representations

$$\nabla^* : rV \longrightarrow (r-1)V$$

defined by  $\nabla^*(v_1, v_2, \dots, v_r) = (v_1, v_2, \dots, v_{r-2}, v_{r-1} + v_r)$ . We also consider the morphism

$$\Delta^* : (r-1)V \longrightarrow rV$$

given by  $\Delta^*(v_1, v_2, \dots, v_{r-1}) = (v_1, v_2, \dots, v_{r-2}, v_{r-1}, v_{r-1})$ . Dual to these two maps we have the corresponding algebra homomorphisms:

$$\nabla : \mathbf{F}[(r-1)V] \longrightarrow \mathbf{F}[rV]$$

and

$$\Delta : \mathbf{F}[rV] \longrightarrow \mathbf{F}[(r-1)V]$$

given by  $\nabla(f) = f \circ \nabla^*$  and  $\Delta(F) = F \circ \Delta^*$ . We also define  $\nabla_r^* = (\nabla^*)^{r-1} : rV \rightarrow V$  and  $\Delta_r^* = (\Delta^*)^{r-1} : V \rightarrow rV$ .

Thus  $\nabla_r : \mathbf{F}[V] \longrightarrow \mathbf{F}[rV]$  is given by  $(\nabla_r(f))(v_1, v_2, \dots, v_r) = f(v_1 + v_2 + \dots + v_r)$  and  $\Delta_r : \mathbf{F}[rV] \longrightarrow \mathbf{F}[V]$  is given by  $(\Delta_r(F))(v) =$



$F(v, v, \dots, v)$ . The homomorphism  $\nabla_r$  is called (*complete*) *polarisation* and the homomorphism  $\Delta_r$  is called *restitution*.

The algebra  $\mathbf{F}[rV]$  is naturally  $\mathbb{N}^r$  graded by multi-degree:

$$\mathbf{F}[rV] = \bigoplus_{(\lambda_1, \lambda_2, \dots, \lambda_r) \in \mathbb{N}^r} \mathbf{F}[rV]_{(\lambda_1, \lambda_2, \dots, \lambda_r)}$$

where

$$\mathbf{F}[rV]_{(\lambda_1, \lambda_2, \dots, \lambda_r)} \cong \mathbf{F}[V]_{\lambda_1} \otimes \mathbf{F}[V]_{\lambda_2} \otimes \cdots \otimes \mathbf{F}[V]_{\lambda_r} .$$

For each multi-degree,  $(\lambda_1, \lambda_2, \dots, \lambda_r) \in \mathbb{N}^r$  we have the projection  $\pi_{(\lambda_1, \lambda_2, \dots, \lambda_r)} : \mathbf{F}[rV] \rightarrow \mathbf{F}[rV]_{(\lambda_1, \lambda_2, \dots, \lambda_r)}$ . Given a homogeneous element  $f \in \mathbf{F}[V]$  of total degree  $d$ , i.e.,  $f \in \mathbf{F}[V]_d$ , its *full polarisation* is the multi-linear function  $\mathcal{P}(f) = \pi_{(1,1,\dots,1)}(\nabla_d(f)) \in \mathbf{F}[dV]_{(1,1,\dots,1)}$ . Thus  $\mathcal{P} : \mathbf{F}[V]_d \rightarrow \mathbf{F}[dV]_{(1,1,\dots,1)}$ .

More generally, we may use isomorphisms of the form  $\mathbf{F}[V \oplus W] \cong \mathbf{F}[V] \otimes \mathbf{F}[W]$  to define

$$\nabla_{r_1, r_2, \dots, r_m} = \nabla_{r_1} \otimes \nabla_{r_2} \otimes \cdots \otimes \nabla_{r_m} : \mathbf{F}[\bigoplus_{i=1}^m W_i] \longrightarrow \mathbf{F}[\bigoplus_{i=1}^m r_i W_i] .$$

Again, for ease of notation, if  $f \in \mathbf{F}[\bigoplus_{i=1}^m W_i]_{(\lambda_1, \lambda_2, \dots, \lambda_m)}$  we write  $\mathcal{P}(f) = \pi_{(1,1,\dots,1)}(\nabla_{\lambda_1, \lambda_2, \dots, \lambda_m}(f)) \in \mathbf{F}[\bigoplus_{i=1}^m \lambda_i W_i]_{(1,1,\dots,1)}$ . Here again we call the multi-linear function  $\mathcal{P}(f)$  the full polarisation of  $f$ .

Similarly we define the restitution map

$$\Delta_{r_1, r_2, \dots, r_m} = \Delta_{r_1} \otimes \Delta_{r_2} \otimes \cdots \otimes \Delta_{r_m} : \mathbf{F}[\bigoplus_{i=1}^m r_i W_i] \longrightarrow \mathbf{F}[\bigoplus_{i=1}^m W_i] .$$

In this setting, if we have co-ordinate variables such as  $x_i, y_i, z_i$  for  $W_i$  we will use the symbols  $x_{ij}, y_{ij}, z_{ij}$  with  $1 \leq j \leq r_i$  to denote the co-ordinate variables for  $r_i W_i$ . In this notation, restitution is the algebra homomorphism determined by  $\Delta_{r_1, r_2, \dots, r_m}(x_{ij}) = x_i$ ,  $\Delta_{r_1, r_2, \dots, r_m}(y_{ij}) = y_i$ ,  $\Delta_{r_1, r_2, \dots, r_m}(z_{ij}) = z_i$ , etc. For this reason, restitution is sometimes referred to as *erasing subscripts*. For ease of notation, we will write  $\mathcal{R}$  to denote the algebra homomorphism  $\Delta_{\lambda_1, \lambda_2, \dots, \lambda_m}$  when restricted to  $\mathbf{F}[\bigoplus_{i=1}^m \lambda_i W_i]_{(1,1,\dots,1)}$ . Thus if  $F \in \mathbf{F}[\bigoplus_{i=1}^m \lambda_i W_i]_{(1,1,\dots,1)}$  then  $\mathcal{R}(F) \in \mathbf{F}[\bigoplus_{i=1}^m W_i]_{(\lambda_1, \lambda_2, \dots, \lambda_m)}$ . (However, we will sometimes abuse notation and use  $\mathcal{R}$  to denote  $\Delta_{\lambda_1, \lambda_2, \dots, \lambda_m}$  when the indices  $\lambda_1, \lambda_2, \dots, \lambda_m$  are clear from the context.)

It is a relatively straightforward exercise to verify that for any  $f \in \mathbf{F}[\bigoplus_{i=1}^m W_i]_{(\lambda_1, \lambda_2, \dots, \lambda_m)}$  we have  $\mathcal{R}(\mathcal{P}(f)) = (\lambda_1!, \lambda_2!, \dots, \lambda_m!)f$ .

Since  $\nabla^*$  and  $\Delta^*$  are both  $G$ -equivariant, so are all the homomorphisms  $\nabla_{r_1, r_2, \dots, r_m}$  and  $\Delta_{r_1, r_2, \dots, r_m}$ . In particular, if  $f$  is  $G$ -invariant then so is  $\mathcal{P}(f)$ . Similarly,  $\mathcal{R}(F)$  is  $G$ -invariant if  $F$  is. We also note that since the action of  $G$  preserves degree an element  $f$  is invariant if and only if all its homogeneous components are invariant.

## 4. PARTIAL DYCK PATHS

In this section we consider a generalization of Dyck paths (see the book by Koshy [17, p. 151] for an introduction to Dyck paths). For us, a lattice path is a finite sequence of steps in the first quadrant of the  $xy$ -plane starting from the origin. Each step in the path is given by either the vector  $(1,0)$  (an  $x$ -step) or the vector  $(0,1)$  (a  $y$ -step). The number of steps in the path is called its *length*. The path is said to have height  $h$  if  $h$  is the largest integer such that the path touches the line  $y = x - h$ . A lattice path has *finishing height*  $h$  if the final step ends at a point on the line  $y = x - h$ .

Associated to each lattice path of length  $d$  is a word of length  $d$ , i.e., an ordered sequence of  $d$  symbols each either an  $x$  or a  $y$ . This word encodes the path as follows: the  $i^{\text{th}}$  symbol of the word is  $x$  if the  $i^{\text{th}}$  step of the path is an  $x$ -step and the  $i^{\text{th}}$  symbol of the word is a  $y$  if the  $i^{\text{th}}$  step is a  $y$ -step.

We will consider two types of lattice paths: (i) partial Dyck paths and (ii) initial Dyck paths of escape height  $p - 1$ .

**Definition 4.1.** A *partial Dyck path* is a lattice path which stays on or below the diagonal (the line with equation  $y = x$ ). A partial Dyck path of finishing height 0, i.e., which finishes on the diagonal, is called a Dyck path.

**Definition 4.2.** An *initial Dyck path of escape height  $t$*  is a lattice path of height at least  $t$  and which if it crosses above the diagonal does so only after it touches the line  $y = x - t$ . Expressed another way, these are paths which consist of an partial Dyck path of finishing height  $t$  followed by an entirely arbitrary sequence of  $x$ -steps and  $y$ -steps.

Clearly there are  $2^d$  lattice paths of length  $d$ . We may associate these paths with the  $2^d$  monomials in  $\mathbf{F}[d V_2]_{(1,1,\dots,1)} \cong \otimes^d V_2$ . The lattice path  $\gamma$  of length  $d$  is associated to the word  $\gamma_1 \gamma_2 \cdots \gamma_d$  and is associated to the multi-linear monomial  $\Lambda(\gamma) = z_1 z_2 \cdots z_d$  where 
$$\begin{cases} z_i = x_i, & \text{if } \gamma_i = x; \\ z_i = y_i, & \text{if } \gamma_i = y. \end{cases}$$

We let  $\text{PDP}_{\leq q}^d$  denote the set of all partial Dyck paths of length  $d$  and height at most  $q$ . Furthermore, we will denote by  $\text{PDP}_{\leq q}^d(h)$  the set of partial Dyck paths of length  $d$ , height at most  $q$  and finishing height  $h$ . We write  $\text{IDP}_q^d$  to denote the set of all initial Dyck paths of escape height  $q$  and length  $d$ .

## 5. LEAD MONOMIALS

We wish to consider the  $C_p$ -representation  $\mathbf{F}[dV_2]_{(1,1,\dots,1)} \cong \otimes^d V_2$ . We consider a decomposition of  $\otimes^d V_2$  into a direct sum of indecomposable  $C_p$ -representations. Each summand  $V_h$  has a one dimensional socle spanned by an element  $f$  and we associate to this summand the monomial  $\text{LM}(f)$ . We say that the invariant  $f$  has *length*  $h$  and we write  $\ell(f) = h$ . In general a non-zero invariant has length  $h$  if  $h - 1$  is the maximal value of  $r$  for which  $f$  lies in the image of  $(\sigma - 1)^r$ .

In order to study  $\mathbf{F}[dV_2]_{(1,1,\dots,1)}^{C_p} \cong (\otimes^d V_2)^{C_p}$  we use the graded reverse lexicographic order determined by  $y_1 > x_1 > y_2 > x_2 \cdots > y_d > x_d$  and consider

$$M = \{\text{LM}(f) \mid f \in (\otimes^d V_2)^{C_p}\} .$$

We will show that the set map

$$\Lambda : \text{PDP}_{\leq p-2}^d \sqcup \text{IDP}_{p-1}^d \longrightarrow M$$

is a bijection.

We begin by showing that the image of  $\Lambda$  lies inside  $M$ . In fact we will show that if  $\gamma \in \text{PDP}_{\leq p-2}^d(h)$  then  $\Lambda(\gamma)$  is the lead monomial of an invariant of length  $h + 1$ . Furthermore if  $\gamma \in \text{IDP}_{p-1}^d$  then  $\Lambda(\gamma)$  is the lead monomial of an invariant of length  $p$ , i.e, an invariant lying in  $\text{Tr}(\otimes^d V_2)$ .

Consider a path  $\gamma \in \text{PDP}_{\leq p-1}^d(h)$  and let  $\gamma_1 \gamma_2 \cdots \gamma_d$  be the associated word. We wish to match each symbol  $\gamma_j$  which is a  $y$  with an earlier symbol  $\gamma_{\rho(j)}$  which is an  $x$ . We do this recursively as follows. Choose the smallest value  $j$  such that  $\gamma_j = y$  and for which we have not yet found a matching  $x$ . Take  $i$  to be maximal such that  $i < j$ ,  $\gamma_i = x$  and  $i \neq \rho(s)$  for all  $s < j$ . Then we define  $\rho(j) = i$ . Let  $I_1 = \{j \mid \gamma_j = y\}$ ,  $I_2 = \rho(I_1)$  and  $I_3 = \{1, 2, \dots, d\} \setminus (I_1 \sqcup I_2)$ . Then  $|I_1| = |I_2| = (d-h)/2$ ,  $|I_3| = h$  and  $\gamma_i = x$  for all  $i \in I_3$ .

Define

$$\theta_0(\gamma) = \left( \prod_{j \in I_1} u_{\rho(j),j} \right) \prod_{i \in I_3} x_i \text{ and } \theta'_0(\gamma) = \left( \prod_{j \in I_1} u_{\rho(j),j} \right) \prod_{i \in I_3} y_i .$$

Then  $\theta_0(\gamma) \in (\otimes^d V_2)^{C_p}$  and

$$\text{LM}(\theta_0(\gamma)) = \prod_{j \in I_1} \text{LM}(u_{\rho(j),j}) \prod_{i \in I_3} x_i = \prod_{j \in I_1} x_{\rho(j)} y_j \prod_{i \in I_3} x_i = \Lambda(\gamma) .$$

**Lemma 5.1.**  $(\sigma - 1)^h(\theta'_0(\gamma)) = h! \theta_0(\gamma)$  and thus  $\ell(\theta_0(\gamma)) \geq h + 1$ .

*Proof.* We will prove a more general statement. We will show that

$$(\sigma - 1)^{|E|}(y^E) = |E|! x^E .$$

Note that this also implies that  $(\sigma - 1)^{|E|+1}(y^E) = 0$ . We proceed by induction on  $|E|$ . The result is clear for  $|E| = 0, 1$ . Assume, without loss of generality, that  $e_i \geq 1$  for all  $i$  and define  $Z_i \in \mathbb{N}^d$  by  $x_i = x^{Z_i}$ . For  $|E| \geq 2$  we have

$$\begin{aligned}
(\sigma - 1)^{|E|}(y^E) &= (\sigma - 1)^{|E|-1}(\sigma - 1)(y^E) \\
&= (\sigma - 1)^{|E|-1} \left( \sum_i e_i x_i y^{E-Z_i} + \text{terms divisible by some } x_k x_\ell \right) \\
&= (\sigma - 1)^{|E|-1} \left( \sum_i e_i x_i y^{E-Z_i} \right) \\
&\quad \text{since the other terms lie in the kernel of } (\sigma - 1)^{|E|-1} \\
&= \sum_i e_i x_i (\sigma - 1)^{|E|-1} (y^{E-Z_i}) \\
&= \sum_i e_i x_i (|E| - 1)! x^{E-Z_i} \text{ by induction} \\
&= \sum_i e_i (|E| - 1)! x^E = \left( \sum_i e_i \right) (|E| - 1)! x^E \\
&= |E| (|E| - 1)! x^E = |E|! x^E
\end{aligned}$$

□

If  $\gamma \in \text{PDP}_{\leq p-2}^d$  then we define  $\theta(\gamma) = \theta_0(\gamma)$  and  $\theta'(\gamma) = \theta'_0(\gamma)$ .

Suppose instead that  $\gamma \in \text{IDP}_{p-1}^d$  and let  $\gamma_1 \gamma_2 \cdots \gamma_d$  be the word associated to  $\gamma$ . Take  $s$  minimal such that the path  $\gamma'$  associated to  $\gamma_1 \gamma_2 \cdots \gamma_s$  is a partial Dyck path of finishing height  $p - 1$ . Since  $\gamma' \in \text{PDP}_{\leq p-1}^s(p - 1)$ , from the above we have  $I_1 = \{j \leq s \mid \gamma_j = y\}$ ,  $I_2 = \rho(I_1)$  and  $I_3 = \{1, 2, \dots, s\} \setminus (I_1 \sqcup I_2)$  with  $|I_1| = |I_2| = (s - p + 1)/2$ ,  $|I_3| = p - 1$  and  $\gamma_i = x$  for all  $i \in I_3$ . We further define  $I_4 = \{i > s \mid \gamma_i = x\}$  and  $I_5 = \{i > s \mid \gamma_i = y\}$ . Define

$$\theta'(\gamma) = \theta'_0(\gamma') \prod_{i \in I_5} y_i \prod_{i \in I_4} x_i = \prod_{j \in I_1} u_{\rho(j), j} \prod_{i \in I_3 \cup I_5} y_i \prod_{i \in I_4} x_i$$

and

$$\theta(\gamma) = \text{Tr}(\theta'_0(\gamma')) \prod_{i \in I_5} y_i \prod_{i \in I_4} x_i = \text{Tr} \left( \prod_{i \in I_3 \cup I_5} y_i \right) \prod_{j \in I_1} u_{\rho(j), j} \prod_{i \in I_4} x_i$$

Then  $\theta(\gamma) \in \text{Tr}(\otimes^d V_2) \subset (\otimes^d V_2)^{C_p}$  and  $\ell(\theta(\gamma)) = p$ .

By Lemma 2.3

$$\begin{aligned} \text{LM}(\theta(\gamma)) &= \left( \prod_{i \in I_4} x_i \prod_{j \in I_1} \text{LM}(u_{\rho(j),j}) \right) \text{LM}(\text{Tr}(\prod_{i \in I_3 \cup I_5} y_i)) \\ &= \left( \prod_{i \in I_4} x_i \prod_{j \in I_1} x_{\rho(j)} y_j \right) \prod_{i \in I_3} x_i \prod_{i \in I_5} y_i = \Lambda(\gamma) \end{aligned}$$

In summary, if  $\gamma \in \text{PDP}_{\leq p-2}^d(h)$  then  $\theta(\gamma)$  is an invariant of length at least  $h+1$  and lead monomial  $\Lambda(\gamma)$ . If  $\gamma \in \text{IDP}_{p-1}^d$  then  $\theta(\gamma)$  is an invariant of length  $p$  and with lead monomial  $\Lambda(\gamma)$ . Note that since these lead monomials are all distinct, the maps  $\theta$  and  $\Lambda$  are injective.

It remains to show that  $\Lambda$  is onto  $M$  and to determine the exact length of the invariants  $\theta(\gamma)$  when  $\gamma \in \text{PDP}_{\leq p-2}^d$ . We will show that  $\Lambda$  is onto by showing  $|M| = |\text{PDP}_{\leq p-2}^d \sqcup \text{IDP}_{p-1}^d|$ . To determine  $|M|$  we examine the number of indecomposable summands in the decomposition of  $\otimes^d V_2$ .

Define non-negative integers  $\mu_p^d(h)$  by the direct sum decomposition of the  $C_p$ -module  $\otimes^d V_2$  over  $\mathbf{F}$ :

$$\bigotimes^d V_2 \cong \bigoplus_{h=1}^p \mu_p^d(h) V_h .$$

Using the convention  $\otimes^0 V_2 = V_1$ , we have the following lemma.

**Lemma 5.2.** *Let  $p \geq 3$ . Then*

$$\mu_p^0(h) = \delta_h^1 \text{ and } \mu_p^1(h) = \delta_h^2,$$

and

$$\mu_p^{d+1}(h) = \begin{cases} \mu_p^d(2), & \text{if } h = 1; \\ \mu_p^d(h-1) + \mu_p^d(h+1), & \text{if } 2 \leq h \leq p-2; \\ \mu_p^d(p-2), & \text{if } h = p-1; \\ \mu_p^d(p-1) + 2\mu_p^d(p), & \text{if } h = p; \end{cases}$$

for  $d \geq 1$ .

*Proof.* The initial conditions are clear. The recursive conditions follow immediately from the following three equations which may be found for example in Hughes and Kemper [14, Lemma 2.2]:

$$\begin{aligned} V_1 \otimes V_2 &\cong V_2 \\ V_h \otimes V_2 &\cong V_{h-1} \oplus V_{h+1} \text{ for all } 2 \leq h \leq p-1 \\ V_p \otimes V_2 &\cong 2V_p. \end{aligned}$$

□

Next we count lattice paths. Let  $\nu_q^d(h) = |\text{PDP}_{\leq q}^d(h)|$  for  $1 \leq h \leq q$ . We also define  $\bar{\nu}_q^d = |\text{IDP}_q^d|$ . With this notation we have the following lemma.

**Lemma 5.3.** *Let  $q \geq 2$ . Then*

$$\begin{aligned} \nu_q^0(h) &= \delta_h^0 \text{ and } \nu_q^1(h) = \delta_h^1, \\ \bar{\nu}_q^0 &= 0 \text{ and } \bar{\nu}_q^1 = 0, \end{aligned}$$

and

$$\nu_q^{d+1}(h) = \begin{cases} \nu_q^d(1), & \text{if } h = 0; \\ \nu_q^d(h-1) + \nu_q^d(h+1), & \text{if } 1 \leq h \leq q-1; \\ \nu_q^d(q-1), & \text{if } h = q; \end{cases}$$

and

$$\bar{\nu}_q^{d+1} = \nu_{q-1}^d(q-1) + 2\bar{\nu}_q^d$$

for all  $d \geq 1$ .

*Proof.* All of these equations are easily seen to hold except perhaps the final one. Its left-hand term  $\bar{\nu}_q^{d+1} = |\text{IDP}_q^{d+1}|$  is the number of initial Dyck paths of length  $d+1$  and escape height  $q$ . We divide such paths into two classes: those which first achieve height  $q$  on their final step and those which achieve height  $q$  sometime during the first  $d$  steps. Paths in the first class are partial Dyck paths of length  $d$ , height at most  $q-1$  and finishing height  $q-1$  followed by an  $x$ -step for the  $(d+1)$ <sup>st</sup> step. There are  $\nu_{q-1}^d(q-1) = |\text{PDP}_{\leq q-1}^d(q-1)|$  such paths. The second class consists of initial Dyck paths of escape height  $q$  and length  $d$  followed by a final step which may be either an  $x$ -step or a  $y$ -step. Clearly there are  $2|\text{IDP}_q^d| = 2\bar{\nu}_q^d$  paths of this kind. □

**Corollary 5.4.** *For all  $d \in \mathbb{N}$ , all primes  $p$  and all  $h = 1, 2, \dots, p-1$  we have*

$$\mu_p^d(h) = \nu_{p-2}^d(h-1) \quad \text{and} \quad \mu_p^d(p) = \bar{\nu}_{p-1}^d.$$

*Proof.* Comparing the recursive expressions and initial conditions for  $\mu_p^d(h)$  and  $\nu_{p-2}^d(h-1)$  and for  $\mu_p^d(p)$  and  $\bar{\nu}_{p-1}^d$  given in the previous two lemmas makes the result clear for  $p \geq 5$ .

For  $p = 2$  it is easy to see that  $\mu_2^d(1) = \nu_0^d(0) = \delta_d^0$  for  $d \geq 0$  and  $\mu_2^d(2) = 2^{d-1} = \bar{\nu}_1^d$  for  $d \geq 1$ .

For  $p = 3$  and  $h = 1, 2$  we have

$$\mu_3^d(h) = \nu_1^d(h-1) = \begin{cases} 1, & \text{if } h+d \text{ is odd;} \\ 0, & \text{if } h+d \text{ is even.} \end{cases}$$

Hence  $\mu_3^d(3) = \lfloor \frac{2^d-1}{3} \rfloor$  for  $d \geq 0$ . From the recursive relation  $\bar{\nu}_2^{d+1} = \nu_1^d(1) + 2\bar{\nu}_2^d$  it is easy to see that  $\bar{\nu}_2^d = \lfloor \frac{2^d-1}{3} \rfloor = \mu_3^d(3)$ .  $\square$

This corollary implies that the map  $\Lambda$  is a bijection. Furthermore for all  $d$ , every element of  $\{\text{LM}(f) \mid f \in (\otimes^d V_2)^{C_p}\}$  may be written as a product with factors from the set  $\{\text{LM}(g) \mid g \in B\}$  where

$$B := \{x_i \mid 1 \leq i \leq d\} \cup \{u_{ij} \mid 1 \leq i < j \leq d\} \\ \cup \left\{ \text{Tr} \left( \prod_{i=1}^d y_i^{e_i} \right) \mid 0 \leq e_i \leq 1, \forall i = 1, 2, \dots, d \right\}.$$

We record and extend these results in the following theorem.

**Theorem 5.5.** *Let  $p$  be a prime, let  $d \in \mathbb{N}$  and suppose  $0 \leq h \leq p-2$ . Let  $\gamma \in \text{PDP}_{\leq p-2}^d \cup \text{IDP}_{p-1}^d$ . Then*

- (1)  $\text{LM}(\theta(\gamma)) = \Lambda(\gamma)$ .
- (2) *If  $\gamma \in \text{PDP}_{\leq p-2}^d(h)$  then the invariant  $\theta(\gamma)$  lies in*

$$\mathbf{F}[dV_2]_{(1,1,\dots,1)}^{C_p} \cong (\otimes^d V_2)^{C_p}$$

*and has length  $h+1$ .*

- (3) *If  $\gamma \in \text{IDP}_{p-1}^d$  then the invariant  $\theta(\gamma)$  lies in*

$$\mathbf{F}[dV_2]_{(1,1,\dots,1)}^{C_p} \cong (\otimes^d V_2)^{C_p}$$

*and has length  $p$ .*

- (4)  *$B$  is a SAGBI basis in multi-degree  $(1, 1, \dots, 1)$  for  $\mathbf{F}[dV_2]^{C_p}$ .*

*Furthermore, we have the following decomposition of the  $C_p$  representation  $\otimes^d V_2$  into indecomposable summands:*

$$\bigotimes^d V_2 \cong \bigoplus_{\gamma \in \text{PDP}_{\leq p-2}^d \cup \text{IDP}_{p-1}^d} V(\gamma)$$

*where  $V(\gamma) \cong V_{h+1}$  is a  $C_p$ -module generated by  $\theta'(\gamma)$ , with socle spanned by  $\theta(\gamma)$  and*

$$h = \ell(\theta(\gamma)) - 1 = \begin{cases} \text{the finishing height of } \gamma; & \text{if } \gamma \in \text{PDP}_{\leq p-2}^d(h); \\ p-1 & \text{if } \gamma \in \text{IDP}_{p-1}^d. \end{cases}$$

*Proof.* The assertions (1) and (3) have already been proved.

To prove the other assertions we consider the  $C_p$ -module

$$W = \sum_{\gamma \in \text{PDP}_{\leq p-2}^d \cup \text{IDP}_{p-1}^d} V(\gamma)$$

generated by the set  $\{\theta'(\gamma) \mid \gamma \in \text{PDP}_{\leq p-2}^d \cup \text{IDP}_{p-1}^d\}$ . The set of vectors  $\{\theta(\gamma) \mid \gamma \in \text{PDP}_{\leq p-2}^d \cup \text{IDP}_{p-1}^d\}$  spanning the socles of the  $V(\gamma)$  is linearly independent since these vectors have distinct lead monomials. This implies that the above sum is direct:

$$W = \bigoplus_{\gamma \in \text{PDP}_{\leq p-2}^d \cup \text{IDP}_{p-1}^d} V(\gamma) .$$

Thus  $\dim W = (\sum_{h=0}^{p-2} (h+1) \cdot \nu_p^d(h)) + p \cdot \bar{\nu}_p^d$ . Applying Corollary 5.4, yields  $\dim W = \dim \otimes^d V_2$ . Since  $W$  is a submodule of  $\otimes^d V_2$  we see that  $W = \otimes^d V_2$ . Furthermore, any set of (spanning vectors for the) socles in any direct sum decomposition of  $\otimes^d V_2$  there will be exactly  $\nu_p^d(h)$  invariants of length  $h+1$  for  $0 \leq h \leq p-2$  (and  $\bar{\nu}_p^d$  of length  $p$ ). Combining this fact with  $\ell(\theta(\gamma)) \geq h+1$  for all  $\gamma \in \text{PDP}_{\leq p-2}^d(h)$ , we get  $\ell(\theta(\gamma)) = h+1$  for all  $\gamma \in \text{PDP}_{\leq p-2}^d(h)$ , completing the proof of assertion (2) as well as the final assertion of the theorem. Assertion (4) also follows now since we have  $\{\text{LM}(f) \mid f \in (\otimes^d V_2)^{C_p}\} = \{\text{LM}(\theta(\gamma)) \mid \gamma \in \text{PDP}_{\leq p-2}^d \cup \text{IDP}_{p-1}^d\}$  and each of these lead monomials may be factored into a product of lead monomials of elements of  $B$ .  $\square$

## 6. A GENERATING SET

Consider the set

$$\begin{aligned} \mathcal{B} = & \{x_i, N(y_i) \mid 1 \leq i \leq m\} \cup \{u_{ij} \mid 1 \leq i < j \leq m\} \\ & \cup \{\text{Tr}(y^E) \mid 0 \leq e_i \leq p-1\} . \end{aligned}$$

We will show that  $\mathcal{B}$  is a generating set, in fact a SAGBI basis for  $\mathbf{F}[m V_2]^{C_p}$ . Let  $f \in \mathbf{F}[m V_2]^{C_p}$  be monic and multi-homogeneous, of multi-degree  $(\lambda_1, \lambda_2, \dots, \lambda_m)$ . Let  $A$  denote the subalgebra  $\mathbf{F}[\mathcal{B}]$ . We proceed by induction on the total degree  $d = \lambda_1 + \lambda_2 + \dots + \lambda_m$  of  $f$ . Clearly if  $f$  has total degree 0 then  $f$  is constant,  $f \in A$  and  $\text{LM}(f) = 1$  and there is nothing more to prove.

Suppose then that the total degree  $d$  of  $f$  is positive. First suppose that  $\lambda_i \geq p$  for some  $i$ . We consider  $f$  as a polynomial in  $y_i$  and write  $f = \sum_{j=0}^{\lambda_i} f_j y_i^j$  where  $f_j$  is a polynomial which is homogeneous of degree  $\lambda_i - j$  in  $x_i$ . Dividing  $f$  by  $N(y_i)$  in  $\mathbf{F}[m V_2]$  yields  $f = q N(y_i) + r$  where the remainder  $r$  is a polynomial whose degree in  $y_i$  is at most  $p-1$ . Applying  $\sigma$  we have  $f = \sigma(f) = \sigma(q) N(y_i) + \sigma(r)$ . Since applying  $\sigma$  cannot increase the degree in  $y_i$ , we see that  $\sigma(r)$  also has degree at most  $p-1$  in  $y_i$ . By the uniqueness of remainders and quotients we must have  $\sigma(r) = r$  and  $\sigma(q) = q$ , i.e.,  $q, r \in \mathbf{F}[m V_2]^{C_p}$ . Since  $\lambda_i \geq p$ , we see that  $x_i$  divides  $r$  and so we have  $f = q N(y_i) + x_i r'$  with



$q, r' \in \mathbf{F}[mV_2]^{C_p}$ . By induction  $q, r' \in A$  and thus  $f \in A$ . Also by induction we have that  $\text{LM}(q)$  and  $\text{LM}(r')$ , hence also  $\text{LM}(f)$  may be written as products with factors from  $\text{LM}(\mathcal{B})$ .

Therefore, we may assume that  $\lambda_i < p$  for all  $i = 1, 2, \dots, m$ . Then  $\kappa = \lambda_1! \lambda_2! \cdots \lambda_m! \neq 0$ . Define

$$F = \mathcal{P}(f) \in \mathbf{F}[dV_2]_{(1,1,\dots,1)}^{C_p} = (\otimes_{i=1}^d V_2)^{C_p}.$$

At this point we want to fix some notation. We will use  $\{x_{ij}, y_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq \lambda_i\}$  as co-ordinate variables for  $\lambda_1 V_2 \oplus \lambda_2 V_2 \oplus \cdots \oplus \lambda_m V_2$ . We write  $u_{ij,kl} = x_{ij}y_{kl} - x_{kl}y_{ij}$ . We use a graded reverse lexicographic order on  $\mathbf{F}[\oplus_{i=1}^m \lambda_i V_2]$  after ordering these variables such that the following conditions hold

- $y_{ij} > x_{ij}$ ,
- if  $i < k$  then  $y_{ij} > y_{kl}$  and  $x_{ij} > x_{kl}$ ,
- if  $j < \ell$  then  $y_{ij} > y_{i\ell}$  and  $x_{ij} > x_{i\ell}$ .

We will first show that  $\mathcal{B}$  generates  $\mathbf{F}[mV_2]^{C_p}$  as an  $\mathbf{F}$ -algebra and then show that it is a SAGBI basis. Of course, the former statement follows from the latter but we include a separate proof of the former since the proof is short and illustrates the main idea we will need for the latter proof.

By Theorem 5.5, we may write

$$F = \sum_I \alpha_I \prod_{ij} x_{ij} \prod_{ij,kl} u_{ij,kl} \prod_E \text{Tr}(\prod_{ij} y_{ij}^{e_{ij}}).$$

Let  $e_i = \sum_j e_{ij}$ .

$$\begin{aligned} f &= \kappa^{-1} \mathcal{R}(\mathcal{P}(f)) = \kappa^{-1} \mathcal{R}(F) \\ &= \kappa^{-1} \mathcal{R} \left( \sum_I \alpha_I \prod_{ij} x_{ij} \prod_{ij,kl} u_{ij,kl} \prod_E \text{Tr}(\prod_{ij} y_{ij}^{e_{ij}}) \right) \\ &= \kappa^{-1} \sum_I \alpha_I \prod_{ij} \mathcal{R}(x_{ij}) \prod_{ij,kl} \mathcal{R}(u_{ij,kl}) \prod_E \mathcal{R}(\text{Tr}(\prod_{ij} y_{ij}^{e_{ij}})) \\ &= \kappa^{-1} \sum_I \alpha_I \prod_{ij} x_i \prod_{ij,kl} u_{ik} \prod_E \text{Tr}(\prod_i y_i^{e_i}) \in A \end{aligned}$$

where the last equality follows from the following equalities

$$\begin{aligned} \mathcal{R}(\text{Tr}(y^E)) &= \mathcal{R} \left( \sum_{\tau \in C_p} \tau(y^E) \right) = \sum_{\tau \in C_p} \mathcal{R}(\tau(y^E)) = \sum_{\tau \in C_p} \tau(\mathcal{R}(y^E)) \\ &= \text{Tr}(\mathcal{R}(y^E)). \end{aligned}$$

This completes the proof that  $\mathcal{B}$  generates  $\mathbf{F}[m V_2]^{C_p}$  as an  $\mathbf{F}$ -algebra. We continue with the proof that  $\mathcal{B}$  is a SAGBI basis. First we prove a lemma relating our term orders and polarisation.

**Lemma 6.1.** *Suppose  $\gamma_1, \gamma_2$  are two monomials in  $\mathbf{F}[m V_2]_{(\lambda_1, \lambda_2, \dots, \lambda_m)}$  with  $\gamma_1 > \gamma_2$ . Then  $\text{LT}(\mathcal{P}(\gamma_1)) > \text{LT}(\mathcal{P}(\gamma_2))$ .*

*Proof.* Write  $\gamma_1 = \prod_{i=1}^m x_i^{a_i} y_i^{\lambda_i - a_i}$  and  $\gamma_2 = \prod_{i=1}^m x_i^{b_i} y_i^{\lambda_i - b_i}$ . Choose  $s$  such that  $a_s \neq b_s$  but  $a_{s+1} = b_{s+1}, \dots, a_m = b_m$ . Since  $\gamma_1 > \gamma_2$  we must have  $b_s > a_s$ .

Now

$$\text{LT}(\mathcal{P}(\gamma_1)) = \prod_{i=1}^m \prod_{j=1}^{a_i} x_{ij} \prod_{j=a_i+1}^{\lambda_i} y_{ij} \text{ and } \text{LT}(\mathcal{P}(\gamma_2)) = \prod_{i=1}^m \prod_{j=1}^{b_i} x_{ij} \prod_{j=b_i+1}^{\lambda_i} y_{ij}.$$

Writing

$$\Gamma_1 = \prod_{i=1}^{s-1} \prod_{j=1}^{a_i} x_{ij} \prod_{j=a_i+1}^{\lambda_i} y_{ij}, \quad \Gamma_2 = \prod_{i=1}^{s-1} \prod_{j=1}^{b_i} x_{ij} \prod_{j=b_i+1}^{\lambda_i} y_{ij}$$

$$\text{and } \Gamma_0 = \prod_{i=s+1}^m \prod_{j=1}^{a_i} x_{ij} \prod_{j=a_i+1}^{\lambda_i} y_{ij}$$

we have

$$\text{LT}(\mathcal{P}(\gamma_1)) = \Gamma_0 \Gamma_1 \prod_{j=1}^{a_s} x_{sj} \prod_{j=a_s+1}^{\lambda_s} y_{sj}$$

and

$$\text{LT}(\mathcal{P}(\gamma_2)) = \Gamma_0 \Gamma_2 \prod_{j=1}^{b_s} x_{sj} \prod_{j=b_s+1}^{\lambda_s} y_{sj}.$$

Since  $a_s < b_s$  we see that  $\text{LT}(\mathcal{P}(\gamma_1)) > \text{LT}(\mathcal{P}(\gamma_2))$ .  $\square$

Write  $f = \gamma_1 + \gamma_2 + \dots + \gamma_s$  where each  $\gamma_i$  is a term and  $\text{LM}(f) = \text{LT}(f) = \gamma_1$  since  $f$  was assumed to be monic. Define  $F = \mathcal{P}(f)$ . By Lemma 6.1,  $\text{LM}(F) = \text{LM}(\mathcal{P}(\gamma_1))$ . Furthermore, each monomial of  $\mathcal{P}(\gamma_1)$  restitutes to  $\gamma_1$ . In particular,  $\mathcal{R}(\Gamma_1) = \gamma_1$  where  $\Gamma_1 = \text{LM}(F)$ . By Proposition 5.5(4), we may write

$$\begin{aligned} \Gamma_1 &= \text{LM}(F) = \text{LM} \left( \prod_{ij} x_{ij} \prod_{ij,kl} u_{ij,kl} \prod_E \text{Tr}(\prod_{ij} y_{ij}^{e_{ij}}) \right) \\ &= \prod_{ij} x_{ij} \prod_{ij,kl} \text{LM}(u_{ij,kl}) \prod_E \text{LM}(\text{Tr}(\prod_{ij} y_{ij}^{e_{ij}})). \end{aligned}$$

Restituting we find

$$\begin{aligned}
\gamma_1 = \mathcal{R}(\Gamma_1) &= \mathcal{R} \left( \prod_{ij} x_{ij} \prod_{ij,kl} \text{LM}(u_{ij,kl}) \prod_E \text{LM}(\text{Tr}(\prod_{ij} y_{ij}^{e_{ij}})) \right) \\
&= \prod_{ij} \mathcal{R}(x_{ij}) \prod_{ij,kl} \mathcal{R}(\text{LM}(u_{ij,kl})) \prod_E \mathcal{R}(\text{LM}(\text{Tr}(\prod_{ij} y_{ij}^{e_{ij}}))) \\
&= \prod_{ij} x_i \prod_{ij,kl} \text{LM}(u_{i,k}) \prod_E \text{LM}(\text{Tr}(\prod_i y_i^{\sum_j e_{ij}}))
\end{aligned}$$

where the last equality follows using Lemma 6.2 below. Thus  $\text{LM}(f)$  may be written as a product of factors from  $\text{LM}(\mathcal{B})$ . This shows that  $\mathcal{B}$  is a SAGBI basis for  $\mathbf{F}[mV_2]^{C_p}$ .

**Lemma 6.2.** *Let  $y^E = \prod_{i=1}^m \prod_{j=1}^{\lambda_i} y_{ij}^{e_{ij}}$  where  $e_{ij} \in \{0, 1\}$  for all  $i, j$ . Let  $e_i = \sum_{j=1}^{\lambda_i} e_{ij}$ . If  $e_i < p$  for all  $i = 1, 2, \dots, m$  then*

$$\mathcal{R}(\text{LM}(\text{Tr}(y^E))) = \text{LM}(\text{Tr}(\mathcal{R}(y^E))) .$$

*Proof.* Let  $s$  be minimal such that  $e_1 + e_2 + \dots + e_s \geq p - 1$ . (If no such  $s$  exists then  $\text{Tr}(y^E) = 0$  and  $\text{Tr}(\mathcal{R}(y^E)) = 0$ .) Let  $r$  be minimal such that  $e_1 + e_2 + \dots + e_{s-1} + e_{s1} + e_{s2} + \dots + e_{sr} = p - 1$ . By Lemma 2.3

$$\text{LM}(\text{Tr}(y^E)) = \left( \prod_{i=1}^{s-1} \prod_{j=1}^{\lambda_i} x_{ij}^{e_{ij}} \right) \prod_{j=1}^r x_{sj}^{e_{sj}} \prod_{j=r+1}^{\lambda_s} y_{sj}^{e_{sj}} \left( \prod_{i=s+1}^m \prod_{j=1}^{\lambda_i} y_{ij}^{e_{ij}} \right) .$$

Since  $\mathcal{R}(y^E) = \prod_{i=1}^m y_i^{e_i}$ , again using Lemma 2.3 we see that

$$\text{LM}(\text{Tr}(\mathcal{R}(y^E))) = \left( \prod_{i=1}^{s-1} x_i^{e_i} \right) x_s^t y_s^{e_s - t} \left( \prod_{i=s+1}^m y_i^{e_i} \right)$$

where  $t = (p - 1) - (e_1 + e_2 + \dots + e_{s-1}) = \sum_{j=1}^r e_{sj}$ . Thus

$$\mathcal{R}(\text{LM}(\text{Tr}(y^E))) = \text{LM}(\text{Tr}(\mathcal{R}(y^E)))$$

as required.  $\square$

**Theorem 6.3.** *The set*

$$\begin{aligned}
\mathcal{B}' &= \{x_i, N(y_i) \mid 1 \leq i \leq m\} \cup \{u_{ij} \mid 1 \leq i < j \leq m\} \\
&\cup \{\text{Tr}(y^E) \mid 0 \leq e_i \leq p - 1, 2(p - 1) < |E|\}
\end{aligned}$$

*is both a minimal algebra generating set and a SAGBI basis for  $\mathbf{F}[mV_2]^{C_p}$ .*

*Proof.* We start by showing  $\mathcal{B}'$  is a SAGBI basis. We need to see why we do not need invariants of the form  $\text{Tr}(y^E)$  where  $|E| \leq 2(p - 1)$  as generators. To see this, consider such a transfer  $\text{Tr}(y^E)$ . By Lemma 2.3

its lead term is  $x_r^{p-1-t+e_r} y_r^{t-p+1} \prod_{i=1}^{r-1} x_i^{e_i} \prod_{i=r+1}^d y_i^{e_i}$  where  $r$  is minimal such that  $t = \sum_{i=1}^r e_i \geq p-1$ . (We may assume that  $r$  exists since if  $|E| < p-1$  then  $\text{Tr}(y^E) = 0$ .)

Write  $\text{LM}(\text{Tr}(y^E)) = x_{i_1} x_{i_2} \cdots x_{i_{p-1}} y_{i_p} y_{i_{p+1}} \cdots y_{i_e}$  where  $1 \leq i_1 \leq i_2 \leq \cdots \leq i_e \leq m$ . Consider  $f = \prod_{j=1}^{2p-2-|E|} x_{i_j} \prod_{j=1}^{|E|-(p-1)} u_{i_{p-j}, i_{p-1+j}}$ . Then  $\text{LM}(f) = \text{LM}(\text{Tr}(y^E))$ . Thus  $\{\text{LM}(f) \mid f \in \mathcal{B}'\}$  generates the same algebra as  $\{\text{LM}(f) \mid f \in \mathcal{B}\}$  which shows that  $\mathcal{B}'$  is a SAGBI basis (and hence a generating set) for  $\mathbf{F}[m V_2]^{C_p}$ .

Now we show that  $\mathcal{B}'$  is a minimal generating set. It is clear that the elements  $x_i$  and  $u_{ij}$  cannot be written as polynomials in the other elements of  $\mathcal{B}'$ . Furthermore, since  $\text{LM}(\text{N}(y_i)) = y_i^p$  is the only monomial occurring in any element of  $\mathcal{B}'$  which is a pure power of  $y_i$ , we see that  $\text{N}(y_i)$  is required as a generator. This leaves elements of the form  $\text{Tr}(y^E)$  with  $|E| > 2(p-1)$ . We proceed similarly to the proof of [24, Lemma 4.3]. Assume by way of contradiction that  $\text{Tr}(y^E) = \gamma_1 + \gamma_2 + \cdots + \gamma_r$  where each  $\gamma_i$  is a scalar times a product of elements from  $\mathcal{B}' \setminus \{\text{Tr}(y^E)\}$  and that  $\text{LM}(\gamma_1) \geq \text{LM}(\gamma_2) \cdots \geq \text{LM}(\gamma_r)$ . Then  $\text{LM}(\text{Tr}(y^E)) \leq \text{LM}(\gamma_1)$ . First we suppose that  $\text{LM}(\gamma_1) = \text{LT}(\text{Tr}(y^E))$ . As above we have

$$\text{LM}(\gamma_1) = \text{LM}(\text{Tr}(y^E)) = x^A y^B = x_r^{p-1-t+e_r} y_r^{t-p+1} \prod_{i=1}^{r-1} x_i^{e_i} \prod_{i=r+1}^d y_i^{e_i}$$

where  $r$  is minimal such that  $t = \sum_{i=1}^r e_i \geq p-1$ .

Since each  $e_i < p$  and  $\text{LM}(\text{N}(y_i)) = y_i^p$  we see that  $\text{N}(y_i)$  does not divide  $\gamma_1$ . But then since  $|A| = p-1$  we see that  $|A| < |E| - |A| = |B|$  and thus there must be at least one transfer which divides  $\gamma_1$ . Conversely since  $|A| = p-1$  exactly one transfer (to the first power) may divide  $\gamma_1$ . But then the lead monomials of the other factors must divide  $y^B$  and no element of  $\mathcal{B}'$  has a lead monomial satisfying this constraint. This shows that for  $|E| > 2(p-1)$ , the monomial  $\text{LM}(\text{Tr}(y^E))$  cannot be properly factored using lead monomials from  $\mathcal{B}'$ .

Therefore we must have  $\text{LM}(\gamma_1) > \text{LM}(\text{Tr}(y^E))$  (and  $\text{LM}(\gamma_1) = \text{LM}(\gamma_2)$ ). Since we may assume that each term of each  $\gamma_i$  is homogeneous of degree  $E$ , we may write  $\text{LM}(\gamma_1) = x^C y^D$  where  $C + D = E$ . But  $\text{LM}(\text{Tr}(y^E)) = x^A y^B$  is the biggest monomial in degree  $E$  which satisfies  $|A| \geq p-1$ . Hence  $\text{LM}(\gamma_1) > \text{LM}(\text{Tr}(y^E))$  implies that  $|C| < p-1$ . Therefore  $\gamma_1$  must be a product of elements of the form  $x_i, u_{ij}$  and  $\text{N}(y_i)$  from  $\mathcal{B}'$ . As above, since each  $e_i < p$ , no  $\text{N}(y_i)$  can divide  $\gamma_1$ . But then  $\text{LM}(\gamma_1)$  is a product of factors of the form  $x_i$

and  $\text{LM}(u_{ij}) = x_i y_j$  and this forces  $|C| \geq |D| = |E| - |C|$ . Therefore  $2(p-1) > 2|C| \geq |E|$ . This contradiction shows that we cannot express  $\text{Tr}(y^E)$  as a polynomial in the other elements of  $\mathcal{B}'$  when  $|E| > 2(p-1)$ .  $\square$

## 7. DECOMPOSING $\mathbf{F}[mV_2]$ AS A $C_p$ -MODULE

In this section we show that our techniques give a decomposition of the homogeneous component

$$\mathbf{F}[mV_2]_{(d_1, d_2, \dots, d_m)}$$

as a  $C_p$ -module. We will describe  $\mathbf{F}[mV_2]_{(d_1, d_2, \dots, d_m)}$  modulo projectives, i.e., we compute the multiplicities of the indecomposable summands  $V_k$  of this component for which  $k < p$ . Having done this, a simple dimension computation will give the complete decomposition.

By the Periodicity Theorem (Theorem 2.1), we may assume that each  $d_i < p$ . Let  $d = d_1 + d_2 + \dots + d_m$ . The symmetric group on  $d$  letters,  $\Sigma_d$ , acts on  $\otimes^d V_2$  by permuting the factors. This action commutes with the action of  $C_p$  (in fact with the action of all of  $GL(V_2)$ ). The image of the polarization map consists of those tensors which are fixed by the Young subgroup  $Y = \Sigma_{d_1} \times \Sigma_{d_2} \times \dots \times \Sigma_{d_m}$  of  $\Sigma_d$ . Since each  $d_i < p$ , we see that  $Y$  is a non-modular group. Maschke's Theorem then implies that polarization embeds  $\mathbf{F}[mV_2]_d$  into  $\otimes^d V_2$  as a  $C_p$ -summand. Therefore  $\ell(\mathcal{P}(f)) = \ell(f)$  for all  $f \in \mathbf{F}[mV_2]_{(d_1, d_2, \dots, d_m)}^{C_p}$  and  $\ell(\mathcal{R}(F)) = \ell(F)$  for all  $F \in (\otimes^d V_2)^{C_p \times Y}$ .

Using the relations given in Section 2.2, it is straightforward to write down a basis, consisting of products of  $u_{ij}$ 's and  $x_i$ 's, for the invariants in multi-degree  $(d_1, d_2, \dots, d_m)$  which lie in the subring generated by  $\{x_i \mid 1 \leq i \leq m\} \cup \{u_{i,j} \mid 1 \leq i < j \leq m\}$ . Associated to the lead term of each invariant in this basis is an indecomposable summand of  $\mathbf{F}[mV_2]_{(d_1, d_2, \dots, d_m)}$ . The dimension of this summand may be found using Theorem 5.5. More directly, consider a product of  $u_{ij}$ 's and  $x_i$ 's, say

$$f := \prod_{i=1}^m x_i^{a_i} \cdot \prod_{1 \leq i < j \leq m} u_{i,j}^{b_{i,j}} \in \mathbf{F}[mV_2]^{C_p}.$$

It is not too difficult to show that  $\text{LT}(f)$  is the lead term of an element of the transfer if and only if there exists  $r$  with  $1 \leq r \leq m$  such that

$$\sum_{i=1}^r a_i + \sum_{\substack{1 \leq i \leq r \leq j \leq m \\ i < j}} b_{i,j} \geq p - 1.$$

If no such  $r$  exists then  $\ell(f) = 1 + \sum_{i=1}^m a_i$  gives the dimension of the associated summand.

Rather than working with the invariants lying in  $\mathbf{F}[m V_2]$  directly, one may instead use Theorem 5.5 to decompose  $\otimes^d V_2$ . It is then possible to perturb this decomposition so that it is a refinement of the splitting given by polarisation/restitution and thus gives a decomposition of  $\mathbf{F}[m V_2]_{(d_1, \dots, d_m)}$ .

*Example 7.1.* As an example we compute the decomposition of

$$\mathbf{F}[4 V_2]_{(p+1, 1, 1, p+2)}.$$

This space has dimension  $(p+2)(2)(2)(p+3) = 4p^2 + 20p + 24$ . By Theorem 2.1, we know

$$\mathbf{F}[4 V_2]_{(p+1, 1, 1, p+2)} \cong \mathbf{F}[4 V_2]_{(1, 1, 1, 2)} \oplus (4p+20)V_p$$

and we need to compute the decomposition of

$$\mathbf{F}[4 V_2]_{(1, 1, 1, 2)} = V_2 \otimes V_2 \otimes V_2 \otimes S^2(V_2).$$

We have available the invariants  $x_1, x_2, x_3, x_4$  and  $u_{12}, u_{13}, u_{14}, u_{23}, u_{24}, u_{34}$ . Suppose now that  $p \geq 7$ . The products of these 10 invariants which lie in degree  $(1, 1, 1, 2)$  are as follows (sorted by length):

$$\begin{aligned} \ell = 2: & x_4 u_{12} u_{34}, x_4 u_{13} u_{24}, x_4 u_{14} u_{23}, x_1 u_{24} u_{34}, x_2 u_{14} u_{34}, x_3 u_{14} u_{24} \\ \ell = 4: & x_3 x_4^2 u_{12}, x_1 x_4^2 u_{23}, x_1 x_2 x_4 u_{34}, x_2 x_4^2 u_{13}, x_1 x_3 x_4 u_{24}, x_2 x_3 x_4 u_{14} \\ \ell = 6: & x_1 x_2 x_3 x_4^2 \end{aligned}$$

Consider the invariants of length 2. Among the available relations for those of length 2 we have:

$$\begin{aligned} 0 &= x_4(u_{12}u_{34} - u_{13}u_{24} + u_{14}u_{23}), \\ 0 &= u_{34}(x_1u_{24} - x_2u_{14} + x_4u_{23}), \text{ and} \\ 0 &= u_{14}(x_2u_{34} - x_3u_{24} + x_4u_{23}). \end{aligned}$$

Using these three relations we see that the three invariants

$$x_4 u_{13} u_{24}, \quad x_2 u_{14} u_{34}, \quad x_3 u_{14} u_{24}$$

may be expressed in terms of the other three invariants

$$x_4 u_{12} u_{34}, \quad x_4 u_{14} u_{23}, \quad x_1 u_{24} u_{34}.$$

Furthermore there are no relations involving only these latter three invariants and thus they represent the socles of 3 summands isomorphic to  $V_2$ .

Among the available relations involving invariants of length 4 we have

$$\begin{aligned} 0 &= x_4^2(x_1u_{23} - x_2u_{13} + x_3u_{12}), \\ 0 &= x_1x_4(x_2u_{34} - x_3u_{24} + x_4u_{23}), \text{ and} \\ 0 &= x_3x_4(x_1u_{24} - x_2u_{14} + x_4u_{12}). \end{aligned}$$

These allow us to express the three invariants

$$x_2x_4^2u_{13}, \quad x_1x_3x_4u_{24}, \quad x_2x_3x_4u_{14}$$

using only

$$x_3x_4^2u_{12}, \quad x_1x_4^2u_{23}, \quad x_1x_2x_4u_{34}.$$

Again these there are no relations involving only these latter 3 invariants and so they represent the socles of 3 summands isomorphic to  $V_4$ .

Since  $x_1x_2x_3x_4^2$  spans the socle of a summand isomorphic to  $V_6$  we conclude that

$$\mathbf{F}[4V_2]_{(1,1,1,2)} \cong 3V_2 \oplus 3V_4 \oplus V_6 \quad \text{for } p \geq 7.$$

For  $p = 5$ , the foregoing is all correct except that the lattice paths corresponding to  $x_1x_2x_3x_4^2$  and  $x_1x_2x_3x_4y_4 = \text{LT}(x_1x_2u_{34}x_4)$  both attain height  $p - 1 = 4$ . Thus in this case these two invariants both represent a projective summand and we have the decomposition

$$\mathbf{F}[4V_2]_{(1,1,1,2)} \cong 3V_2 \oplus 2V_4 \oplus 2V_5 \quad \text{for } p = 5.$$

For  $p = 2, 3$  all the relevant lattice paths attain height  $p - 1$  and so the summand is projective. Thus

$$\begin{aligned} \mathbf{F}[4V_2]_{(1,1,1,2)} &\cong 8V_3 \quad \text{for } p = 3, \text{ and} \\ \mathbf{F}[4V_2]_{(1,1,1,2)} &\cong 12V_2 \quad \text{for } p = 2. \end{aligned}$$

We will also illustrate how to use the decomposition of  $\otimes^5 V_2$  to find the decomposition of  $\mathbf{F}[4V_2]_{(1,1,1,2)}$ . By the results of Section 5, we have  $\otimes^5 V_2 \cong 5V_2 \oplus 4V_4 \oplus V_6$  for  $p \geq 7$ . Here the lead monomials are

$$\begin{aligned} \ell = 2: & x_1y_2x_3y_4x_5, \quad x_1x_2y_3y_4x_5, \quad x_1y_2x_3x_4y_5, \quad x_1x_2y_3x_4y_5, \quad x_1x_2x_3y_4y_5 \\ \ell = 4: & x_1y_2x_3x_4x_5, \quad x_1x_2y_3x_4x_5, \quad x_1x_2x_3y_4x_5, \quad x_1x_2x_3x_4y_5 \\ \ell = 6: & x_1x_2x_3x_4x_5 \end{aligned}$$

and the corresponding invariants are

$$\begin{aligned} \ell = 2: & x_5u_{12}u_{34}, \quad x_5u_{14}u_{23}, \quad x_4u_{12}u_{35}, \quad x_1u_{23}u_{45}, \quad x_1u_{25}u_{34} \\ \ell = 4: & x_3x_4x_5u_{12}, \quad x_1x_4x_5u_{23}, \quad x_1x_2x_5u_{34}, \quad x_1x_2x_3u_{45} \\ \ell = 6: & x_1x_2x_3x_4x_5 \end{aligned}$$

The Young subgroup  $Y := \Sigma_1 \times \Sigma_1 \times \Sigma_1 \times \Sigma_2$  acts by simultaneously interchanging  $x_4$  with  $x_5$  and  $y_4$  with  $y_5$ . Clearly the action preserves length. The  $C_p \times Y$  invariants are

$$\begin{aligned} \ell = 2: & \quad x_5 u_{12} u_{34} + x_4 u_{12} u_{35}, \quad x_5 u_{14} u_{23} + x_4 u_{15} u_{23}, \quad x_4 u_{12} u_{35} + x_5 u_{12} u_{34}, \\ & \quad x_1 u_{23} u_{45} + x_1 u_{23} u_{54} = 0, \quad x_1 u_{25} u_{34} + x_1 u_{24} u_{35} \\ \ell = 4: & \quad x_3 x_4 x_5 u_{12}, \quad x_1 x_4 x_5 u_{23}, \quad x_1 x_2 x_5 u_{34} + x_1 x_2 x_4 u_{35}, \\ & \quad x_1 x_2 x_3 u_{45} + x_1 x_2 x_3 u_{54} = 0 \\ \ell = 6: & \quad x_1 x_2 x_3 x_4 x_5 \end{aligned}$$

We now reconstitute these  $C_p \times Y$  invariants to  $\mathbf{F}[4V_2]_{(1,1,1,2)}^{C_p}$ . We find

$$\begin{aligned} \mathcal{R}(x_5 u_{12} u_{34} + x_4 u_{12} u_{35}) &= 2x_4 u_{12} u_{34}, \\ \mathcal{R}(x_5 u_{14} u_{23} + x_4 u_{15} u_{23}) &= 2x_4 u_{14} u_{23}, \\ \mathcal{R}(x_1 u_{25} u_{34} + x_1 u_{24} u_{35}) &= 2x_1 u_{24} u_{34}. \end{aligned}$$

Thus we find 3 summands of  $\mathbf{F}[4V_2]_{(1,1,1,2)}$  isomorphic to  $V_2$ .

Reconstituting the invariants of length 4 we find

$$\begin{aligned} \mathcal{R}(x_3 x_4 x_5 u_{12}) &= x_3 x_4^2 u_{12}, \\ \mathcal{R}(x_1 x_4 x_5 u_{23}) &= x_1 x_4^2 u_{23}, \quad \text{and} \\ \mathcal{R}(x_1 x_2 x_5 u_{34} + x_1 x_2 x_4 u_{35}) &= 2x_1 x_2 x_4 u_{34}. \end{aligned}$$

Thus we have 3 summands isomorphic to  $V_4$ . Since  $\mathcal{R}(x_1 x_2 x_3 x_4 x_5) = x_1 x_2 x_3 x_4^2$ , we see that

$$\mathbf{F}[4V_2]_{(1,1,1,2)} \cong 3V_2 \oplus 3V_4 \oplus V_6 \quad \text{for } p \geq 7.$$

For  $p = 2, 3, 5$ , the lengths of the above invariants change and we must adjust our conclusions accordingly as we did earlier. For  $p = 2$  we must also use the Periodicity Theorem again since  $d_4 = 2 = p$ .

## 8. A FIRST MAIN THEOREM FOR $SL_2(\mathbf{F}_p)$

The purpose of this section is to use the relative transfer homomorphism to describe the ring of vector invariants,  $\mathbf{F}[mV_2]^{SL_2(\mathbf{F}_p)}$ . Let  $P$  denote the upper triangular Sylow  $p$ -subgroup of  $SL_2(\mathbf{F}_p)$ , giving  $\mathbf{N}(y) = \mathbf{N}^P(y) = y^p - yx^{p-1}$ . The ring of invariants of the defining representation of  $SL_2(\mathbf{F}_p)$  is generated by  $L = x\mathbf{N}(y)$  and  $D = \mathbf{N}(y)^{p-1} + x^p$  (see Dickson [10], Wilkerson [29], or Benson [1, §8.1]). For  $\lambda \in \mathbb{N}^m$ , define  $L_\lambda = \pi_\lambda \nabla_m(L)$  and  $D_\lambda = \pi_\lambda \nabla_m(D)$ , the multi-degree  $\lambda$  polarisations. Further define  $L_i$  to be the polarisation of  $L$  corresponding to  $\lambda_i = p + 1$  and  $\lambda_j = 0$  for  $j \neq i$ . It is easy to verify that  $L_i = x_i y_i^p - x_i^p y_i$  is the Dickson invariant for the  $i^{\text{th}}$  summand.



Let  $L_{ij}$  denote the polarisation corresponding to  $\lambda_i = 1$ ,  $\lambda_j = p$ , and  $\lambda_k = 0$  otherwise. So, for example,  $L_{32} = L_{(0,p,1,0,\dots,0)}$ . Define

$$\mathcal{D}_m = \left\{ \lambda \in \mathbb{N}^m \mid p \text{ divides } \lambda_i \text{ for all } i \text{ and } \sum_{i=1}^m \lambda_i = p(p-1) \right\}.$$

Further define

$$\begin{aligned} \mathcal{S}_m &= \{u_{ij} \mid i < j \leq m\} \cup \{L_i, L_{ij} \mid i, j \in \{1, \dots, m\}, i \neq j\} \\ &\cup \{D_\lambda \mid \lambda \in \mathcal{D}_m\}. \end{aligned}$$

**Theorem 8.1.** *The ring of vector invariants,  $\mathbf{F}[mV_2]^{SL_2(\mathbf{F}_p)}$ , is generated by  $\mathcal{S}_m$  and elements from the image of the transfer.*

Note that the elements of  $\mathcal{S}_m$  are clearly  $SL_2(\mathbf{F}_p)$ -invariant and include a system of parameters. Let  $A$  denote the algebra generated by  $\mathcal{S}_m$  and let  $\mathfrak{a}$  denote the ideal in  $\mathbf{F}[mV_2]^P$  generated by  $\mathcal{S}_m$ . A basis for the finite dimensional vector space  $\mathbf{F}[mV_2]^P/\mathfrak{a}$  lifts to a set of  $A$ -module generators for  $\mathbf{F}[mV_2]^P$ , say  $\mathcal{M}$ . Since the relative transfer homomorphism is a surjective  $A$ -module morphism,  $\mathbf{F}[mV_2]^{SL_2(\mathbf{F}_p)}$  is generated by  $\mathcal{S}_m \cup \text{Tr}_P^{SL_2(\mathbf{F}_p)}(\mathcal{M})$ . The elements of  $\mathcal{M}$  may be chosen to be monomials in the generators of  $\mathbf{F}[mV_2]^P$ . Since we are working modulo the image of the transfer, it is sufficient to consider monomials of the form  $N(y)^\alpha x^\beta$ .

Let  $\mathfrak{u}$  denote the ideal in  $\mathbf{F}[mV_2]^P$  generated by  $\{u_{ij} \mid i < j \leq m\}$ .

**Lemma 8.2.** *For  $i < j \leq m$ ,  $L_{ij} = x_i N(y_j) + u_{ij} x_j^{p-1}$  and  $L_{ji} = x_j N(y_i) - u_{ij} x_i^{p-1}$ , giving  $L_{ij} \equiv_{\mathfrak{u}} x_i N(y_j)$  and  $L_{ji} \equiv_{\mathfrak{u}} x_j N(y_i)$ .*

*Proof.* Applying  $\nabla_m$  to  $L$  gives

$$(x_1 + \dots + x_m) (y_1^p + \dots + y_m^p - (y_1 + \dots + y_m)(x_1 + \dots + x_m)^{p-1}).$$

Expanding gives

$$(x_1 + \dots + x_m) (y_1^p + \dots + y_m^p) - (y_1 + \dots + y_m)(x_1 + \dots + x_m)^p.$$

Collecting the appropriate multi-degrees gives  $L_{ij} = x_i y_j^p - y_i x_j^p$  and  $L_{ji} = x_j y_i^p - y_j x_i^p$ . Using  $u_{ij} = x_i y_j - x_j y_i$  and  $N(y) = y^p - x^{p-1}y$  gives

$$x_i N(y_j) + u_{ij} x_j^{p-1} = x_i y_j^p - x_i y_j x_j^{p-1} + x_i y_j x_j^{p-1} - x_j^p y_i = L_{ij}$$

and

$$x_j N(y_i) - u_{ij} x_i^{p-1} = x_j y_i^p - x_j y_i x_i^{p-1} - y_j x_i^p + x_i^{p-1} x_j y_i = L_{ji}.$$

□

Since  $\mathfrak{u} \subset \mathfrak{a}$ , the preceding lemma and the formula  $L_i = x_i N(y_i)$  show that it is sufficient to compute  $\mathrm{Tr}_P^{SL_2(\mathbf{F}_p)}$  on monomials of the form  $N(y)^\alpha$  or  $x^\beta$ .

Let  $B$  denote the Borel subgroup containing  $P$ , i.e., the upper triangular elements of  $SL_2(\mathbf{F}_p)$ . Define a weight function on  $\mathbf{F}[mV_2]$  by  $\mathrm{wt}(x_i) \equiv_{(p-1)} 1$  and  $\mathrm{wt}(y_i) \equiv_{(p-1)} -1$ . Note that  $N(y_i)$  is isobaric of weight  $-1$ . Furthermore,  $\mathbf{F}[mV_2]^B$  consists of the span of the weight zero elements of  $\mathbf{F}[mV_2]^P$ . The relative transfer  $\mathrm{Tr}_P^B$  is determined by weight:

$$\mathrm{Tr}_P^B(N(y)^\alpha x^\beta) = \begin{cases} -N(y)^\alpha x^\beta, & \text{if } (|\beta| - |\alpha|) \equiv_{(p-1)} 0; \\ 0, & \text{otherwise.} \end{cases}$$

Since  $\mathrm{Tr}_P^{SL_2(\mathbf{F}_p)} = \mathrm{Tr}_B^{SL_2(\mathbf{F}_p)} \mathrm{Tr}_P^B$ , it is sufficient to compute  $\mathrm{Tr}_B^{SL_2(\mathbf{F}_p)}$  on  $N(y)^\alpha$  with  $|\alpha|$  a multiple of  $p-1$  and  $x^\beta$  with  $|\beta|$  a multiple of  $p-1$ . However, if  $|\beta| \geq p-1$ , then  $x^\beta \in \mathrm{Tr}^P(\mathbf{F}[mV_2])$  and  $\mathrm{Tr}_P^{SL_2(\mathbf{F}_p)}(x^\beta) \in \mathrm{Tr}^{SL_2(\mathbf{F}_p)}(\mathbf{F}[mV_2])$ . Thus it is sufficient to compute  $\mathrm{Tr}_B^{SL_2(\mathbf{F}_p)}(N(y)^\alpha)$  with  $|\alpha|$  a multiple of  $p-1$ .

For  $\lambda \in \mathcal{D}_m$ , define

$$N(y)^{\lambda/p} = \prod_{i=1}^m N(y_i)^{\lambda_i/p}.$$

**Lemma 8.3.**  $\nabla_m(D) \equiv_{\mathfrak{u}} (N(y_1) + \cdots + N(y_m))^{p-1} + (x_1 + \cdots + x_m)^{p(p-1)}$ , giving  $D_\lambda \equiv_{\mathfrak{u}} \binom{p-1}{\lambda/p} (N(y)^{\lambda/p} + x^\lambda)$  and  $N(y)^{\lambda/p} \equiv_{\mathfrak{a}} -x^\lambda$ .

*Proof.* The proof is by induction on  $m$ . Note that  $\nabla_m = \nabla^{m-1}$ . Thus  $\nabla_1(D) = \nabla^0(D) = D = N(y)^{p-1} + x^{p(p-1)}$ , as required. Recall that the action of  $\nabla$  on  $\mathbf{F}[mV_2]$  is determined by  $\nabla(x_m) = x_m + x_{m+1}$ ,  $\nabla(y_m) = y_m + y_{m+1}$ ,  $\nabla(x_i) = x_i$ , and  $\nabla(y_i) = x_i$  for  $i < m$ . Thus  $\nabla(u_{ij}) = u_{ij}$  if  $i < j < m$  and  $\nabla(u_{im}) = y_i(x_m + x_{m+1}) - x_i(y_m + y_{m+1}) = u_{im} + u_{i,m+1}$ . Therefore  $\nabla$  induces an algebra morphism on  $\mathbf{F}[mV_2]^P/\mathfrak{u}$ . Furthermore  $\nabla(N(y_i)) = N(y_i)$  if  $i < j < m$  and  $\nabla(N(y_m)) = y_m^p + y_{m+1}^p - (x_m + x_{m+1})^{p-1}(y_m + y_{m+1}) = N(y_m) + N(y_{m+1}) - u_{m,m+1} \sum_{j=0}^{p-2} (-x_m)^j x_{m+1}^{p-2-j}$ . By induction,

$$\begin{aligned} \nabla_{m+1}(D) &= \nabla(\nabla_m(D)) \in \nabla((N(y_1) + \cdots + N(y_m))^{p-1} \\ &\quad + (x_1 + \cdots + x_m)^{p(p-1)} + \mathfrak{u}). \end{aligned}$$

Evaluating the algebra morphism  $\nabla$  gives

$$\begin{aligned} \nabla_{m+1}(D) &\in (\nabla(\mathbf{N}(y_1)) + \cdots + \nabla(\mathbf{N}(y_m)))^{p-1} + (x_1 + \cdots + x_{m+1})^{p(p-1)} \\ &\quad + \nabla(\mathbf{u}) \\ &\in (\mathbf{N}(y_1) + \cdots + \mathbf{N}(y_{m+1}))^{p-1} + (x_1 + \cdots + x_{m+1})^{p(p-1)} + \mathbf{u}, \end{aligned}$$

as required.  $\square$

Using the lemma, if  $p - 1$  divides  $|\alpha|$  then  $\mathrm{Tr}_B^{SL_2(\mathbf{F}_p)}(\mathbf{N}(y)^\alpha)$  is decomposable modulo the image of the transfer, completing the proof of Theorem 8.1

To complete the calculation of a generating set for  $\mathbf{F}[mV_2]^{SL_2(\mathbf{F}_p)}$  and compute an upper bound for the Noether number, we need only identify a set of  $A$ -module generators for  $\mathbf{F}[mV_2]$ . This can be done by applying the Buchberger algorithm to  $\mathcal{S}_m$ . For example, a Magma [2] calculation for  $m = 3$  and  $p = 3$ , produces 522  $A$ -module generators giving rise to 74 non-zero elements in the image of the transfer. Subducting the transfers against  $\mathcal{S}_m$  gives 11 new generators and 29 in total. Magma's *MinimalAlgebraGenerators* command reduces the number of generators to 28, occurring in degrees 2, 4, 6 and 8. The same calculation for  $p = 5$  and  $m = 3$  gives a Noether number of 24. Thus for  $p \in \{3, 5\}$  and  $m = 3$ , the Noether number is  $(p + m - 2)(p - 1) = (p + 1)(p - 1)$ .

**Theorem 8.4.**  $\mathbf{F}[mV_2]^{SL_2(\mathbf{F}_p)}$  is generated as an  $A$ -module in degrees less than or equal to  $(p + m - 2)(p - 1)$ .

*Proof.* Define  $\mathfrak{a}'$  to be the ideal in  $\mathbf{F}[mV_2]$  generated by  $\mathcal{S}_m$ , i.e.,

$$\mathfrak{a}' = A^+ \mathbf{F}[mV_2].$$

A basis for  $\mathbf{F}[mV_2]/\mathfrak{a}'$  lifts to a set of  $A$ -module generators for  $\mathbf{F}[mV_2]$ . We may choose the  $A$ -module generators to be monomials,  $y^\alpha x^\beta$ , which are minimal representatives of their mod- $\mathfrak{a}'$  congruence class. For convenience, denote  $d = |\alpha| + |\beta|$ . For  $i < j$ , using  $u_{ij} = x_i y_j - x_j y_i$ , if  $x_i$  divides  $y^\alpha x^\beta$ , then  $y_j$  does not. For  $j \leq i$ , using  $L_i$  and  $L_{ij}$ , if  $x_i$  divides  $y^\alpha x^\beta$ , then  $y_j^p$  does not. The remaining representatives fall into two classes:  $y^\alpha$  and  $y_1^{\alpha_1} \cdots y_k^{\alpha_k} x_k^{\beta_k} \cdots x_m^{\beta_m}$  with  $\beta_k \neq 0$  and  $\alpha_i \leq p - 1$ .

Case 1:  $y^\alpha$ . Using  $D_\lambda$  with  $\lambda \in \mathcal{D}_m$ , we see that, for  $|\gamma| \geq p - 1$ ,  $(y^\gamma)^p$  does not divide  $y^\alpha$ . Write  $\alpha_i = q_i p + r_i$  with  $r_i < p$ . Then  $y^\alpha = (y^q)^p y^r$  with  $|q| \leq p - 2$ . Thus  $|\alpha| = p|q| + |r| \leq p(p - 2) + m(p - 1) = (p + m - 1)(p - 1) - 1$ . However,  $\mathrm{Tr}(y^\alpha) = 0$  unless  $p - 1$  divides  $|\alpha|$ . Therefore, the  $A$ -module generators of the form  $\mathrm{Tr}(y^\alpha)$  satisfy  $d = |\alpha| \leq (p + m - 2)(p - 1)$ .

Case 2:  $y_1^{\alpha_1} \cdots y_k^{\alpha_k} x_k^{\beta_k} \cdots x_m^{\beta_m}$  with  $\beta_k \neq 0$  and  $\alpha_i \leq p - 1$ . For  $i < j$ , let  $x^\gamma$  be a monomial in  $x_1, \dots, x_{j-1}$ . If  $|\gamma| = p - 1$ , then

$x^\gamma L_{ij} = x^\gamma(x_i y_j^p - x_j^p y_i) \equiv_{\mathfrak{u}} y^\gamma y_i x_j^p - x^\gamma y_i x_j^p$ . Therefore, if  $\beta_j \geq p$  for any  $j > k$ , then  $|\alpha| < p$ . If  $|\gamma| \leq p-1$  then  $x^\gamma L_j = x^\gamma(x_j y_j^p - x_j^p y_j) \equiv_{\mathfrak{u}} y^\gamma y_j^{p-|\gamma|} x_j^{|\gamma|+1} - x^\gamma y_j x_j^p$ . Therefore, if  $\beta_k \geq p$ , we also have  $|\alpha| < p$ . If  $|\beta_j| < p$  for all  $j \geq k$ , then  $|\alpha| + |\beta| \leq (m-k+2)(p-1) \leq (p+m-2)(p-1)$  if  $k > 1$ . Hence it is sufficient to consider the case  $|\alpha| < p$ . However the transfer is zero unless  $p-1$  divides  $|\alpha|$  so we may assume  $|\alpha| = p-1$ . If  $|\alpha| = p-1$ , a straightforward calculation with binomial coefficients gives  $\text{Tr}^P(y^\alpha x^\beta) = -x^{\alpha+\beta}$ . Furthermore,  $\text{Tr}_P^B(x^{\alpha+\beta}) = 0$  unless  $p-1$  divides  $|\alpha|+|\beta|$ . Write  $\alpha_i + \beta_i = q_i p + r_i$  with  $r_i < p$ . Then  $x^{\alpha+\beta} = (x^q)^p x^r$ . If  $|q| \geq p-1$  and  $|r| > 0$ , we may choose  $i$  so that  $r_i > 0$ , choose  $\lambda \in \mathcal{D}_m$  so that  $x^\lambda$  divides  $x^{pq}$  and choose  $j$  so that  $x_j$  divides  $x^\lambda$ . By Lemma 8.2,  $x_i N(y_j) \in \mathfrak{a}'$ . Form the S-polynomial between  $D_\lambda$  and  $x_i N(y_j)$ . Using Lemma 8.3, this S-polynomial reduces to  $x_i x^\lambda$ . Thus either  $|q| < p-1$  or  $|q| = p-1$  and  $|r| = 0$ . If  $|r| = 0$  and  $|q| = p-1$ , then  $d = (p-1)(p-1) \leq (p+m-2)(p-1)$ . Suppose  $|q| < p-1$ . Then  $d \leq m(p-1) + p(p-2) = (p+m-1)(p-1) - 1$ . Since  $d$  must be a multiple of  $p-1$ , we have  $d \leq (p+m-2)(p-1)$ .  $\square$

**Corollary 8.5.** *For  $m > 2$ , the Noether number for  $\mathbf{F}[m V_2]^{SL_2(\mathbf{F}_p)}$  is less than or equal to  $(p+m-2)(p-1)$ . For  $m = 2$  and  $p > 2$ , the Noether number is  $p(p-1)$  and for  $m = 2$ ,  $p = 2$ , the Noether number is  $p+1 = 3$ .*

*Proof.* The elements of  $\mathcal{S}_m$  lie in degrees 2,  $p+1$  and  $p(p-1)$ . Clearly  $L_1$  and  $D_{(p(p-1), 0, \dots, 0)}$  are indecomposable.  $\square$

For  $p = 2$  and  $m \in \{3, 4\}$ , Magma calculations give the Noether number  $(p+m-2)(p-1) = m$ .

## REFERENCES

- [1] D. J. Benson, *Polynomial Invariants of Finite Groups*, Lond. Math. Soc. Lecture Note Ser. **190** (1993), Cambridge Univ. Press.
- [2] W. Bosma, J. J. Cannon and C. Playoust, *The Magma algebra system I: the user language*, J. Symbolic Comput. **24** (1997), 235–265.
- [3] H. E. A. Campbell and I. P. Hughes, *Vector invariants of  $U_2(\mathbf{F}_p)$ : A proof of a conjecture of Richman*, Adv. in Math. **126** (1997), 1–20.
- [4] H. E. A. Campbell and David L. Wehlau, *Modular Invariant Theory*, to appear.
- [5] H. E. A. Campbell, I. P. Hughes, R. J. Shank and D. L. Wehlau, *Bases for rings of coinvariants*, Transformation Groups **1** (4) (1996), 307–336.
- [6] C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782.
- [7] D. Cox, J. Little, and D. O’Shea, *Ideals, varieties, and algorithms*, (1992) Springer-Verlag.
- [8] H. S. M. Coxeter, *The product of the generators of a finite group generated by reflections*, Duke Math. J. **18** (1951), 765–782.

- [9] H. Derksen and G. Kemper, *Computational invariant theory*, Invariant Theory and Algebraic Transformation Groups, I, **130** (2002), Encyclopaedia of Mathematical Sciences, Springer-Verlag.
- [10] L. E. Dickson, *A Fundamental System of Invariants of the General Modular Linear Group with a Solution of the Form Problem*, Trans. Amer. Math. Soc. **12** (1911), 75–98.
- [11] G. Ellingsrud and T. Skjelbred, *Profondeur d’anneaux d’invariants en caractéristique  $p$* , Compositio Math. **41** No. 2 (1980), 233–244.
- [12] J. Fogarty, *On Noether’s bound for polynomial invariants of a finite group*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 5–7.
- [13] P. Fleischmann, *The Noether bound in invariant theory of finite groups*, Adv. in Math. **152** (2000) no. 1, 23–32.
- [14] I. P. Hughes and G. Kemper, *Symmetric powers of modular representations, Hilbert series and degree bounds*, Comm. in Alg. **28** (2000), 2059–2088.
- [15] D. Kapur and K. Madlener, *A completion procedure for computing a canonical basis of a  $k$ -subalgebra*, Proceedings of Computers and Mathematics **89** (1989), ed. E. Kaltofen and S. Watt, MIT, 1–11.
- [16] A. Kempe, *On regular difference terms*, Proc. London Math. Soc. **25** (1894), 343–350.
- [17] T. Koshy, *Catalan Numbers with Application* Oxford University Press, (November 2008).
- [18] M. D. Neusel and L. Smith, *Invariant theory of finite groups*, American Mathematical Society, Providence, RI, 2002, Mathematical Surveys and Monographs, **94**.
- [19] E. Noether, *Der Endlichkeitssatz der invarianten endlicher Gruppen*, Math. Ann. **77**, 1915, 89–92; reprinted in: Collected Papers, Springer-Verlag, Berlin, 1983, 181–184.
- [20] L. Robbiano and M. Sweedler, *Subalgebra bases*, Lecture Notes in Math. **1430** Springer (1990), 61–87.
- [21] D. R. Richman, *On vector invariants over finite fields*, Adv. in Math. **81** (1990) no.1, 30–65.
- [22] J.-P. Serre, *Groupes finis d’automorphismes d’anneaux locaux réguliers*, Colloque d’Algèbre (Paris, 1967), Exp. 8, Secrétariat mathématique, Paris, 1968, p. 11.
- [23] R. J. Shank, *S.A.G.B.I. bases for rings of formal modular seminvariants*, Comment. Math. Helv. **73** (1998) no. 4, 548–565.
- [24] R. J. Shank and D. L. Wehlau, *Computing modular invariants of  $p$ -groups*, J. Symbolic Comput. **34** (2002) no. 5, 307–327.
- [25] R. J. Shank and D. L. Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order*, Bull. London Math. Soc. **34** (2002) no. 4, 438–450.
- [26] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canadian J. Math. **6** (1954), 274–304.
- [27] L. Smith, *Polynomial invariants of finite groups*, Research Notes in Mathematics, vol. 6, A K Peters Ltd., Wellesley, MA, 1995.
- [28] H. Weyl, *The classical groups*, Princeton University Press, 1997.
- [29] C. W. Wilkerson, *A Primer on the Dickson Invariants*, Amer. Math. Soc. Contemp. Math. Series **19** (1983), 421–434.

MATHEMATICS & STATISTICS DEPARTMENT,  
MEMORIAL UNIVERSITY OF NEWFOUNDLAND, ST JOHN'S NL A1A 5S7, CANADA  
*E-mail address:* eddy@mun.ca

SCHOOL OF MATHEMATICS, STATISTICS & ACTUARIAL SCIENCE,  
UNIVERSITY OF KENT, CANTERBURY, CT2 7NF, UK  
*E-mail address:* R.J.Shank@kent.ac.uk

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE,  
ROYAL MILITARY COLLEGE, KINGSTON, ONTARIO, CANADA, K7K 5L0  
*E-mail address:* wehlau@rmc.ca