Comment. Math. Helv. 73 (1998) 548–565
0010-2571/98/040548-18 $ 1.50+0.20/0

Commentarii Mathematici Helvetici

S.A.G.B.I. bases for rings of formal modular seminvariants

R. James Shank

Abstract. We use the theory of S.A.G.B.I. bases to construct a generating set for the ring of invariants for the four and five dimensional indecomposable modular representations of a cyclic group of prime order. We observe that for the four dimensional representation the ring of invariants is generated in degrees less than or equal to $2p-3$, and for the five dimensional representation the ring of invariants is generated in degrees less than or equal to $2p-2$.

Mathematics Subject Classification (1991). 13A50.

Keywords. Invariant theory, Indecomposable modular representation.

Introduction

Let $\mathbf{k}$ be a field and let $\mathbf{k}[x_1,\ldots,x_n]$ denote the polynomial algebra in the variables $x_1,\ldots,x_n$. Define an algebra automorphism, σ, of $\mathbf{k}[x_1,\ldots,x_n]$ by

$$\sigma(x_i)=\begin{cases} x_1 & \text{if } i=1,\\ x_{i-1}+x_i & \text{if } i>1.\end{cases}$$

If $f\in\mathbf{k}[x_1,\ldots,x_n]$ and $\sigma(f)=f$, then f will be called *σ-invariant.* Since σ is a degree preserving map, any σ-invariant polynomial is a sum of homogeneous σ-invariant polynomials. Let $\mathbf{k}[x_1,\ldots,x_n]^\sigma$ denote the ring of σ-invariant polynomials. Suppose that p is a prime number and let $\mathbf{F}_p$ denote the field with p elements. If $\mathbf{k}=\mathbf{F}_p$ and $n\le p$, then σ generates a group isomorphic to $\mathbf{Z}/p$ and we denote $\mathbf{k}[x_1,\ldots,x_n]^\sigma$ by $\mathbf{F}_p[x_1,\ldots,x_n]^{\mathbf{Z}/p}$. The action of $\mathbf{Z}/p$ induced by σ on the degree one polynomials of $\mathbf{F}_p[x_1,\ldots,x_n]$ is the indecomposable modular representation of dimension n. The study of $\mathbf{F}_p[x_1,\ldots,x_n]^{\mathbf{Z}/p}$ has a long history going back at least to L. E. Dickson's Madison Colloquium [5]. From Dickson's perspective the problem is an extension of classical invariant theory and the elements of $\mathbf{F}_p[x_1,\ldots,x_n]^{\mathbf{Z}/p}$ are the *formal modular seminvariants* of a binary $(n-1)$–form [5, III]. Dickson gave a complete description of $\mathbf{F}_p[x_1,\ldots,x_n]^{\mathbf{Z}/p}$ for $n=2$ and $n=3$. He gave a generating set for $n=4$, $p=5$. G. Almkvist, in [1], described the set of relations for $n=4$, $p=5$. W. L. G. Williams, in [14], constructed a generating set for $n = 4$, $p = 7$. K. Stråhlén, in a masters thesis [12] supervised by G. Almkvist, studied the relations among Williams' generators and showed that the generating set is not minimal. The primary purpose of this paper is to describe a generating set for $n = 4$ and $n = 5$ for all $p \geq 5$.

If the characteristic of $\mathbf{k}$ is zero, then σ generates a group isomorphic to $\mathbf{Z}$. In this case we denote $\mathbf{k}[x_1, \ldots, x_n]^{\sigma}$ by $\mathbf{k}[x_1, \ldots, x_n]^{\mathbf{Z}}$. Let $\mathbf{Q}$ denote the rational numbers. For any element $f \in \mathbf{Q}[x_1, \ldots, x_n]^{\mathbf{Z}}$, a suitable scalar multiple of f lies in $\mathbf{Z}[x_1, \ldots, x_n]^{\mathbf{Z}}$. By reducing coefficients modulo p, an element of $\mathbf{Z}[x_1, \ldots, x_n]^{\mathbf{Z}}$ gives rise to an element of $\mathbf{F}_p[x_1, \ldots, x_n]^{\mathbf{Z}/p}$. We will call elements of $\mathbf{F}_p[x_1, \ldots, x_n]^{\mathbf{Z}/p}$ constructed in this fashion *rational invariants*. G. Almkvist has shown that, if $f \in \mathbf{F}_p[x_1, \ldots, x_n]^{\mathbf{Z}/p}$ and the degree of f is small compared to p, then f is a rational invariant [1, 2.5]. Thus characteristic zero computations can provide us with some of our generators. In fact, a rational invariant corresponds to the source of a covariant of a binary $(n-1)$–form (see [1]) and so classical invariant theory can be used to compute rational invariants (see, for example, [6] and [13]).

Two additional constructions are needed to provide us with the remaining generators. The first of these is the transfer. The *transfer* is a homomorphism of $\mathbf{F}_p[x_1, \ldots, x_n]^{\mathbf{Z}/p}$–modules from $\mathbf{F}_p[x_1, \ldots, x_n]$to $\mathbf{F}_p[x_1, \ldots, x_n]^{\mathbf{Z}/p}$ defined by

$$\mathrm{Tr}(f) = \sum_{c=1}^{p} \sigma^c(f).$$

The second construction is the norm. For an element, f, of $\mathbf{F}_p[x_1, \ldots, x_n]$ the *norm* of f is defined by

$$\mathrm{N}(f) = \prod_{c=1}^{p} \sigma^c(f).$$

We shall see that, at least for $n = 4$ and $n = 5$, $\mathbf{F}_p[x_1, \ldots, x_n]^{\mathbf{Z}/p}$ is generated by $\mathrm{N}(x_n)$, selected rational invariants and elements from the image of the transfer.

We compute generating sets by constructing a collection of invariants and then using the theory of S.A.G.B.I. bases, introduced by L. Robbiano and M. Sweedler in [9], to prove that the given collection of invariants form a generating set. In Section 1 we define a S.A.G.B.I. basis and discuss the properties of S.A.G.B.I. bases required for our purposes. Section 2 is devoted primarily to constructing rational invariants with particular lead monomials. In this section we also discuss the ring $\mathbf{Q}[V_\infty]^{\mathbf{Z}}$ formed by taking the union over n of $\mathbf{Q}[x_1, \ldots, x_n]^{\mathbf{Z}}$. We are able to construct a vector space basis for $\mathbf{Q}[V_\infty]^{\mathbf{Z}}$. In Section 3 we compute the lead monomials of certain families of elements in the image of the transfer. Section 4 contains the proof that a certain collection of invariants is a generating set for $\mathbf{F}_p[x_1, \ldots, x_4]^{\mathbf{Z}/p}$ and Section 5 contains the analogous result for $\mathbf{F}_p[x_1, \ldots, x_5]^{\mathbf{Z}/p}$. Section 6 is devoted to conclusions and conjectures.

We recommend [10] as a good general reference for the invariant theory of finite groups. Preliminary calculations, including the construction of a generating

set for $n = 4$ with $p = 11$, were performed using G. Kemper's Maple package INVAR ([7], [8]). I would like to thank Catherine Chambers for implementing the most recent version of INVAR on our computing facilities and for supervising the computations. I would also like to thank Eddy Campbell, Ian Hughes and David Wehlau for their assistance and encouragement.

1. S.A.G.B.I. bases

Throughout the paper we use the graded reverse lexicographic monomial order with $x_m < x_{m+1}$. We direct the reader to Chapter 2 of [4] for the appropriate definitions and a detailed discussion of monomial orders. We use the convention that a monomial is a product of variables and that a term is a monomial with a non-zero coefficient. Note that that the zero polynomial is neither a monomial nor a term. We extend the monomial order to a partial order on polynomials by comparing lead monomials. We consider the zero polynomial to be smaller than any non-zero polynomial.

Suppose that $\mathcal{A}$ is a subalgebra of $\mathbf{k}[x_1, \ldots, x_n]$. Let $\mathrm{LT}(\mathcal{A})$ denote the vector space spanned by the lead terms of elements of $\mathcal{A}$. $\mathrm{LT}(\mathcal{A})$ is a subalgebra of $\mathbf{k}[x_1, \ldots, x_n]$. If $\mathcal{C}$ is a subset of $\mathcal{A}$ then let $\mathrm{LM}(\mathcal{C})$ denote the set of lead monomials of elements of $\mathcal{C}$. If $\mathrm{LM}(\mathcal{C})$ generates the algebra $\mathrm{LT}(\mathcal{A})$ then $\mathcal{C}$ is called a *S.A.G.B.I. basis* for $\mathcal{A}$.

Proposition 1.1. *If $\mathcal{C}$ is a S.A.G.B.I. basis for $\mathcal{A}$ then $\mathcal{C}$ generates the algebra $\mathcal{A}$.*

Proof. See [9, 1.16]. □

Suppose that $\mathcal{M}$ is a subspace of $\mathbf{k}[x_1, \ldots, x_n]$. Let $\mathcal{M}_d$ denote the homogeneous component of degree d. The Poincaré series of $\mathcal{M}$ is given by

$$P(\mathcal{M}, t) = \sum_{d=0}^{\infty} \dim_{\mathbf{k}}(\mathcal{M}_d) t^d.$$

Proposition 1.2. *If $\mathcal{A}$ is a subalgebra of $\mathbf{k}[x_1, \ldots, x_n]$, then $P(\mathcal{A}, t) = P(\mathrm{LT}(\mathcal{A}), t)$.*

Proof. We will prove that $\mathcal{A}_d$ has a basis, $\mathcal{B}$, with distinct lead monomials and hence $\mathrm{LM}(\mathcal{B})$ is a basis for $\mathrm{LT}(\mathcal{A})_d$.

In $\mathbf{k}[x_1, \ldots, x_n]$, the monomials of degree d form an ordered basis for the vector space of homogeneous polynomials of degree d. We can use this basis to assign a row vector of coefficients to each homogeneous polynomial. Choose a basis for $\mathcal{A}_d$. For each vector in this basis there is a corresponding row vector of coefficients. Form a matrix from these row vectors. The rows of this matrix are linearly independent. Using row operations put the matrix in echelon form. The rows of the echelon form are the coefficients of a new basis, say $\mathcal{B}$, for $\mathcal{A}_d$. Since the coefficient matrix corresponding to $\mathcal{B}$ is in echelon form, the lead monomials of the elements of $\mathcal{B}$ are distinct. □

2. Lead monomials of invariants

In this section we construct rational invariants with particular lead monomials. We also characterize those monomials which are the lead monomial of a σ–invariant. We will use LM to denote the operation which associates to a polynomial its lead monomial. For convenience we set $\mathrm{LM}(0) = 0$.

Lemma 2.1. *If β is a monomial in $\mathbf{k}[x_1, \ldots, x_{m-1}]$ then βx_m and βx_{m-1} are consecutive elements in the order.*

Proof. Suppose that γ is a monomial with $\beta x_{m-1} < \gamma \leq \beta x_m$. We will prove that βx_{m-1} and βx_m are consecutive by showing $\gamma = \beta x_m$.

Let b_i be the exponent of x_i in β and let e_i be the exponent of x_i in γ. Let j be the first position at which the exponent sequence of βx_{m-1} differs from the exponent sequence of γ. Since βx_{m-1} and γ have the same degree, we can assume that $j < m$. Thus $b_i = e_i$ for $i < j$. If $j < m-1$ then $\gamma > \beta x_m$, contradicting our hypotheses. Thus $j = m-1$. Since the exponent of x_{m-1} in βx_{m-1} is $b_{m-1}+1$ and $\gamma > \beta x_{m-1}$, we conclude that $b_{m-1}+1 > e_{m-1}$. Furthermore, since the exponent of x_{m-1} in βx_m is b_{m-1} and $\gamma \leq \beta x_m$, we have $e_{m-1} \geq b_{m-1}$. Therefore $b_{m-1} = e_{m-1}$ and $\gamma = \beta x_m$. □

It will be convenient to define the function $\partial = \sigma - 1$. Note that ∂ is linear and, if f and g are elements of $\mathbf{k}[x_1, \ldots, x_n]$, then $\partial(fg) = \partial(f)g + \sigma(f)\partial(g)$. Therefore the function ∂ is a twisted σ-derivation.

Theorem 2.2. *Suppose that $n \geq m > 1$ and β is a monomial in $\mathbf{k}[x_1, \ldots, x_{m-1}]$. Then βx_m is not the lead monomial of a σ–invariant in $\mathbf{k}[x_1, \ldots, x_n]$.*

Proof. Suppose that $f \in \mathbf{k}[x_1, \ldots, x_n]$ and that the lead term of f is βx_m. Then $f = \beta x_m + h$ for some polynomial h with $\mathrm{LM}(h) < \mathrm{LM}(f) = \beta x_m$. We will prove that $\mathrm{LM}(\partial(f)) = \beta x_{m-1}$ and thus f is not σ–invariant.

Evaluating $\sigma(x_m)$ and rearranging terms gives

$$\partial(f) = (x_m + x_{m-1})\partial(\beta) + \beta x_{m-1} + \partial(h).$$

We extend the monomial order to a partial order on polynomials by comparing lead monomials. We consider the zero polynomial to be less than every non-zero polynomial. Note that, for any monomial γ, $\partial(\gamma) < \gamma$. Thus $\partial(\beta) < \beta$ and

$x_m\partial(\beta) < x_m\beta$. Furthermore, if h is not the zero polynomial, $\partial(h) < h$. From Lemma 2.1, βx_m and βx_{m-1} are consecutive in the order. Thus $\partial(h) < \beta x_{m-1}$ and $\mathrm{LM}(x_m\partial(\beta)) \leq \beta x_{m-1}$. Since βx_{m-1} is in $\mathbf{k}[x_1,\ldots,x_{m-1}]$, $\mathrm{LM}(x_m\partial(\beta))$ is not equal to βx_{m-1}. Therefore $\mathrm{LM}(\partial(f)) = \beta x_{m-1}$. □

Theorem 2.3. *If β is a monomial in $\mathbf{k}[x_1,\ldots,x_{m-1}]$ and $i \geq 2$ then βx_m^i is the lead monomial of a σ–invariant in $\mathbf{k}[x_1,\ldots,x_n]$ for sufficiently large n.*

Proof. We prove the theorem by introducing an algorithm for constructing a σ-invariant with lead monomial βx_m^i.

Apply ∂ to βx_m^i and observe that, as long as i is not the characteristic of $\mathbf{k}$, the lead term of $\partial(\beta x_m^i)$ is $i\beta x_{m-1}x_m^{i-1}$. Define $f_1 = \beta x_m^i - i\beta x_{m-1}x_m^{i-2}x_{m+1}$. Note that $\mathrm{LM}(\partial(f_1)) < \beta x_{m-1}x_m^{i-1}$. For $j > 1$, if $\partial(f_{j-1}) = 0$ then f_{j-1} is σ-invariant, otherwise write the lead term of $\partial(f_{j-1})$ as γx_r^k with $\gamma \in \mathbf{k}[x_1,\ldots,x_{r-1}]$ and $k > 0$ and define $f_j = f_{j-1} - \gamma x_r^{k-1}x_{r+1}$. Observe that $\mathrm{LM}(\partial(f_j)) < \mathrm{LM}(\partial(f_{j-1}))$. Thus, as long as $\partial(f_j)$ is non-zero, $LM(\partial(f_1)),\ldots,\mathrm{LM}(\partial(f_j))$ is a strictly decreasing sequence of monomials in a fixed degree.

It is not difficult to prove that the set of monomials in countably many variables is well ordered by the graded reverse lexicographic order. Therefore the algorithm terminates. However, we prefer to give an argument which provides us with an upper bound on n.

For a monomial $\lambda = \prod_s x_s^{i_s}$, we define the weight of λ by $\mathrm{wt}(\lambda) = \sum_s s i_s$. Note that the monomials appearing in $\partial(\lambda)$ all have weight less than $\mathrm{wt}(\lambda)$. Furthermore $\mathrm{wt}(\gamma x_r^{k-1}x_{r+1}) = \mathrm{wt}(\gamma x_r^k) + 1$. Hence any monomial appearing in f_j has weight less than or equal to $\mathrm{wt}(\beta x_m^i)$. Since there are only a finite number of monomials in a given degree with a given weight, we see that there are only finitely many f_j. In fact, if we let d denote the degree of βx_m^i and define $\ell = \mathrm{wt}(\beta x_m^i) - d + 1$, then $x_1^{d-1}x_\ell$ is the smallest monomial of degree d and weight $\mathrm{wt}(\beta x_m^i)$, and $f_j \in \mathbf{k}[x_1,\ldots,x_\ell]$. □

Note that all monomials except those of the form x_1^i satisfy the hypotheses of either Theorem 2.2 or Theorem 2.3. We will call a monomial *admissible* if it satisfies the hypotheses of Theorem 2.3 or if the monomial is of the form x_1^i.

Corollary 2.4. $\mathrm{LM}(\mathbf{Q}[V_\infty]^{\mathbf{Z}})$ *is the set of admissible monomials.*

Suppose γ is a monomial satisfying the hypotheses of Theorem 2.3. Then let $\mathrm{inv}(\gamma)$ be the invariant produced by the algorithm. For convenience we define $\mathrm{inv}(x_1^i) = x_1^i$.

Remark 2.5. Suppose that γ is an admissible monomial. Reviewing the algorithm, we observe that γ is the only admissible monomial appearing in $\mathrm{inv}(\gamma)$. Furthermore, if $\ell = \mathrm{wt}(\gamma) - \mathrm{degree}(\gamma) + 1$, then $\mathrm{inv}(\gamma)$ is in $\mathbf{k}[x_1,\ldots,x_\ell]^\sigma$. David

Wehlau and I have recently proved that the variable x_ℓ does appear in $\mathrm{inv}(\gamma)$. In other words, $\mathrm{inv}(\gamma)$ in is not an element of $\mathbf{k}[x_1, \ldots, x_{\ell-1}]^\sigma$.

Let $\mathcal{B}$ denote the set $\{\mathrm{inv}(\gamma) \mid \gamma \text{ is admissible}\}$.

Theorem 2.6. *$\mathcal{B}$ is a basis for the vector space $\mathbf{Q}[V_\infty]^{\mathbf{Z}}$.*

Proof. Since the elements of $\mathcal{B}$ have distinct lead monomials the set is linearly independent. To see that $\mathcal{B}$ is a spanning set, consider a polynomial $f \in \mathbf{Q}[V_\infty]^{\mathbf{Z}}$. Let Γ be the set of admissible monomials appearing in f and, for $\gamma \in \Gamma$, let c_γ denote the coefficient of γ in f. Let

$$\widetilde{f} = \sum_{\gamma \in \Gamma} c_\gamma \ \mathrm{inv}(\gamma).$$

Since no admissible monomial appears in the invariant $f - \widetilde{f}$, it follows from Corollary 2.4 that $f - \widetilde{f} = 0$. Thus $\mathcal{B}$ spans $\mathbf{Q}[V_\infty]^{\mathbf{Z}}$ as required. □

We can use the algorithm from the proof of Theorem 2.3 to describe the rational invariants which will appear as generators in Sections 4 and 5. It is easy to see that $\mathrm{inv}(x_2^2) = x_2^2 - x_1(x_2 + 2x_3)$, $\mathrm{inv}(x_3^2) = x_3^2 - x_2(x_3 + 2x_4) + x_1(x_3 + 3x_4 + 2x_5)$, and $\mathrm{inv}(x_2^3) = x_2^3 + x_1^2(3x_4 - x_2) - 3x_1x_2x_3$. Explicit calculation shows that, although $\mathrm{inv}(x_3^3)$ involves x_1 through x_7, if we define $\overline{\mathrm{inv}}(x_3^3) = 2\ \mathrm{inv}(x_3^3) - 3\ \mathrm{inv}(x_2x_3^2) + 9x_1\ \mathrm{inv}(x_4^2)$, we get an element of $\mathbf{k}[x_1, \ldots, x_5]^\sigma$ with lead monomial x_3^3. Similarly define

$$\overline{\mathrm{inv}}(x_2^2x_3^2) = 3\ \mathrm{inv}(x_2^2x_3^2) + x_1\left(6\ \mathrm{inv}(x_2x_3^2) - 8\ \mathrm{inv}(x_3^3)\right) - x_1^2\left(9\ \mathrm{inv}(x_4^2) + 8\ \mathrm{inv}(x_3^2)\right),$$

and $\overline{\mathrm{inv}}(x_2^2x_3^2x_4^2) = 4\ \mathrm{inv}(x_3^2)^3 - \overline{\mathrm{inv}}(x_3^3)^2$. Clearly $\mathrm{LM}(\overline{\mathrm{inv}}(x_2^2x_3^2)) = x_2^2x_3^2$. Careful computation shows that $\overline{\mathrm{inv}}(x_2^2x_3^2) \in \mathbf{k}[x_1, \ldots, x_4]^\sigma$, $\mathrm{LM}(\overline{\mathrm{inv}}(x_2^2x_3^2x_4^2)) = x_2^2x_3^2x_4^2$ and $\overline{\mathrm{inv}}(x_2^2x_3^2x_4^2) \in \mathbf{k}[x_1, \ldots, x_5]^\sigma$.

3. Lead monomials of transfers

In this section we compute the lead monomial for various elements in the image of the transfer. We assume throughout that $p > 2$. When $p = 2$, with the exception of Theorem 3.5 with $i = 0$, the results stated here are true and the proofs are elementary.

Observe that

$$\sigma^c(x_m) = x_m + \binom{c}{1} x_{m-1} + \binom{c}{2} x_{m-2} + \cdots + \binom{c}{m-1} x_1. \tag{3.1}$$

Therefore

$$\operatorname{Tr}\left(x_{m-1}^{i}x_{m}^{j}\right)=\sum_{c\in\mathbf{F}_p}\left(\sum_{k=0}^{m-2}\binom{c}{k}x_{m-1-k}\right)^{i}\left(\sum_{\ell=0}^{m-1}\binom{c}{\ell}x_{m-\ell}\right)^{j}. \tag{3.2}$$

Note that $\binom{c}{i}$ is a polynomial in c of degree i. The following lemma is well known.

Lemma 3.1. *Suppose that ℓ is a positive integer. Then*

$$\sum_{c\in\mathbf{F}_p}c^{\ell}=\begin{cases}-1 & \textit{if } p-1 \textit{ divides } \ell;\\ 0 & \textit{if } p-1 \textit{ does not divide } \ell.\end{cases}$$

Proof. See, for example, [3, 9.4]. □

Theorem 3.2. *If $(p-1)/2\leq i\leq p-1$ then*

$$\operatorname{LM}\left(\operatorname{Tr}\left(x_{m}^{i}\right)\right)=x_{m-2}^{p-1-i}x_{m-1}^{2i-(p-1)}.$$

Proof. Using Equation 3.1, we see that the coefficient of $x_{m-2}^{p-1-i}x_{m-1}^{2i-(p-1)}$ in $\sigma^{c}(x_{m}^{i})$ is $\binom{c}{2}^{p-1-i}\binom{c}{1}^{2i-(p-1)}\binom{i}{p-1-i}$. Using Lemma 3.1, we see that

$$\sum_{c\in\mathbf{F}_p}\binom{c}{2}^{p-1-i}\binom{c}{1}^{2i-(p-1)}\binom{i}{p-1-i}=-\left(\frac{1}{2}\right)^{p-1-i}\binom{i}{p-1-i}$$

and, since $i\leq p-1$, this is non-zero. All of the monomials appearing in $\sigma^{c}(x_{m}^{i})$ which are greater than $x_{m-2}^{p-1-i}x_{m-1}^{2i-(p-1)}$ have coefficients which, as polynomials in c, have degree less than $p-1$ and hence, by Lemma 3.1, these monomials do not appear in $\operatorname{Tr}(x_{m}^{i})$. □

Theorem 3.3. *If $1\leq i\leq p-1$ then*

$$\operatorname{LM}\left(\operatorname{Tr}\left(x_{m-1}^{i}x_{m}^{p-1}\right)\right)=x_{m-1}^{i+p-1}.$$

Proof. Using Equation 3.2 we see that the coefficient of x_{m-1}^{i+p-1} in $\sigma^{c}(x_{m-1}^{i}x_{m}^{p-1})$ is c^{p-1}. Thus, using Lemma 3.1, the coefficient of x_{m-1}^{i+p-1} in $\operatorname{Tr}(x_{m-1}^{i}x_{m}^{p-1})$ is -1. All of the monomials appearing in $\sigma^{c}(x_{m-1}^{i}x_{m}^{p-1})$ which are greater than x_{m-1}^{i+p-1}

have coefficients which, as polynomials in c, have degree less than $p-1$ and hence, by Lemma 3.1, these monomials do not appear in $\mathrm{Tr}(x_{m-1}^i x_m^{p-1})$. $\square$

Theorem 3.4. *If* $2 \leq i \leq p-1$ *then*

$$\mathrm{LM}\left(\mathrm{Tr}\left(x_{m-1}^i x_m^{p-2}\right)\right) = x_{m-2} x_{m-1}^{i+p-3}.$$

Proof. Using Equation 3.2 we see that the coefficient of $x_{m-2}x_{m-1}^{i+p-3}$ in $\sigma^c(x_{m-1}^i x_m^{p-2})$ is $ic^{p-1} + (p-2)\binom{c}{2}c^{p-3}$. Thus, using Lemma 3.1, the coefficient of x_{m-1}^{i+p-1} in $\mathrm{Tr}(x_{m-1}^i x_m^{p-1})$ is $-i+1$. As long as $i \neq 1$, this coefficient is non-zero. All of the monomials appearing in $\sigma^c(x_{m-1}^i x_m^{p-2})$ which are greater than $x_{m-2}x_{m-1}^{i+p-3}$ have coefficients which, as polynomials in c, have degree less than $p-1$ and hence, by Lemma 3.1, these monomials do not appear in $\mathrm{Tr}(x_{m-1}^i x_m^{p-2})$. $\square$

Theorem 3.5. *If* $(p-1)/2 - 1 \leq i \leq p-1$ *then*

$$\mathrm{LM}\left(\mathrm{Tr}\left(x_{m-1}^2 x_m^i\right)\right) = x_{m-2}^{p-1-i} x_{m-1}^{2i-p+3}.$$

Proof. We use Equation 3.2 to compute the coefficient of $x_{m-2}^{p-1-i}x_{m-1}^{2i-p+3}$ in $\sigma^c(x_{m-1}^2 x_m^i)$. $\sigma^c(x_{m-1}^2)$ contributes x_{m-1}^2, $2cx_{m-1}x_{m-2}$ or $c^2x_{m-2}^2$ with the rest of the term coming from $\sigma^c(x_m^i)$. Thus the coefficient of $x_{m-2}^{p-1-i}x_{m-1}^{2i-p+3}$ in $\sigma^c(x_{m-1}^2 x_m^i)$ is

$$c^{2i-p+1}\binom{c}{2}^{p-1-i}\binom{i}{p-1-i} + 2c^{2i-p+3}\binom{c}{2}^{p-2-i}\binom{i}{p-2-i}$$
$$+c^{2i-p+5}\binom{c}{2}^{p-3-i}\binom{i}{p-3-i}.$$

Thus, using Lemma 3.1, the coefficient of $x_{m-2}^{p-1-i}x_{m-1}^{2i-p+3}$ in $\mathrm{Tr}(x_{m-1}^2 x_m^i)$ is

$$-\left(\frac{1}{2}\right)^{p-1-i}\binom{i}{p-1-i} - 2\left(\frac{1}{2}\right)^{p-2-i}\binom{i}{p-2-i} - \left(\frac{1}{2}\right)^{p-3-i}\binom{i}{p-3-i}.$$

We need to show that this coefficient is non-zero. If $i = p-1$ or $i = p-2$ then the coefficient is -1. If $i < p-2$ then, after factoring, simplifying and reducing modulo p, the coefficient is

$$\frac{-1}{2(i+2)}\left(\frac{1}{2}\right)^{p-3-i}\binom{i}{p-3-i}.$$

Thus the coefficient is non-zero. All of the monomials appearing in $\sigma^c(x_{m-1}^2 x_m^i)$ which are greater than $x_{m-2}^{p-1-i} x_{m-1}^{2i-p+3}$ have coefficients which, as polynomials in c, have degree less than $p-1$ and hence, by Lemma 3.1, these monomials do not appear in $\mathrm{Tr}(x_{m-1}^2 x_m^i)$. □

Theorem 3.6. *Suppose that* $\mathrm{Tr}(\beta)$ *is non-zero and* $\mathrm{LM}\,(\mathrm{Tr}(\beta))$ *is in* $\mathbf{F}_p[x_m, \ldots, x_n]$. *Then*

$$\mathrm{LM}\,(\mathrm{Tr}(x_m\beta)) = x_m\,\mathrm{LM}\,(\mathrm{Tr}(\beta))\,.$$

Proof. Using Equation 3.1, we see that

$$\begin{aligned}\mathrm{Tr}(x_m\beta) &= \sum_{c\in\mathbf{F}_p} \sigma^c(x_m)\sigma^c(\beta)\\ &= \sum_{c\in\mathbf{F}_p}\left(\sum_{j=0}^{m-1}\binom{c}{j}x_{m-j}\right)\sigma^c(\beta)\\ &= x_m\,\mathrm{Tr}(\beta) + \sum_{c\in\mathbf{F}_p}\left(\sum_{j=1}^{m-1}\binom{c}{j}x_{m-j}\right)\sigma^c(\beta).\end{aligned}$$

Thus $\mathrm{Tr}(x_m\beta)$ is congruent, modulo the ideal generated by x_1 through x_{m-1}, to $x_m\,\mathrm{Tr}(\beta)$. Since $\mathrm{LM}\,(\mathrm{Tr}(\beta))$ is in $\mathbf{F}_p[x_m, \ldots, x_n]$, the lead monomial of $\mathrm{Tr}(x_m\beta)$ comes from $x_m\,\mathrm{Tr}(\beta)$. Therefore $\mathrm{LM}\,(\mathrm{Tr}(x_m\beta)) = x_m\,\mathrm{LM}\,(\mathrm{Tr}(\beta))$. □

4. The four dimensional representation

In this section we construct a generating set for $\mathbf{F}_p[x_1, \ldots, x_4]^{\mathbf{Z}/p}$. If $p \equiv 1 \pmod 3$ then define $\ell = (p-1)/3$ and $q = 2\ell+1$. If $p \equiv -1 \pmod 3$ then define $\ell = (p+1)/3$ and $q = 2\ell - 1$. If i is a integer, define $\varepsilon(i)$ to be 0 if i is even and 1 if i is odd.

Theorem 4.1. $\mathbf{F}_p[x_1, \ldots, x_4]^{\mathbf{Z}/p}$ *is generated by* x_1, $\mathrm{inv}(x_2^2)$, $\mathrm{inv}(x_2^3)$, $\overline{\mathrm{inv}}(x_2^2x_3^2)$, $\mathrm{N}(x_4)$ *and the following families:*
(i) $\mathrm{Tr}(x_3^i x_4^{p-1})$ *for* $0 \le i \le p-2$,
(ii) $\mathrm{Tr}(x_3^i x_4^{p-2})$ *for* $3 \le i \le p-2$,
(iii) $\mathrm{Tr}(x_4^j)$ *for* $q \le j \le p-2$ *and*
(iv) $\mathrm{Tr}(x_3^2 x_4^j)$ *for* $2\ell - 1 \le j \le p-2$.

The rest of this section is devoted to the proof of Theorem 4.1. Let $\mathcal{C}$ denote the collection of invariants given in the statement of the preceding theorem. We prove the theorem by showing that $\mathcal{C}$ is a S.A.G.B.I. basis for $\mathbf{F}_p[x_1, \ldots, x_4]^{\mathbf{Z}/p}$, i.e., the lead monomials of the elements of $\mathcal{C}$ generate the lead term algebra of $\mathbf{F}_p[x_1,\ldots,x_4]^{\mathbf{Z}/p}$. We do this by computing the Poincaré series of the algebra generated by the lead monomials of $\mathcal{C}$ and comparing the result with the Poincaré series of $\mathbf{F}_p[x_1,\ldots,x_4]^{\mathbf{Z}/p}$ as computed by G. Almkvist and R. Fossum [2, 3.1]. We observe that the two series are equal and, using Proposition 1.2, we conclude that the lead monomials of $\mathcal{C}$ generate the lead term algebra of $\mathbf{F}_p[x_1,\ldots,x_4]^{\mathbf{Z}/p}$. Therefore, by Proposition 1.1, $\mathcal{C}$ generates $\mathbf{F}_p[x_1,\ldots,x_4]^{\mathbf{Z}/p}$.

Let $\mathcal{A}$ denote the algebra generated by the lead monomials of $\mathcal{C}$. We wish to compute the Poincaré series of $\mathcal{A}$. Using Theorem 3.2 and the fact that the lead monomial of $\mathrm{N}(x_n)$ is x_n^p, we have

$$\mathrm{LM}\{x_1, \mathrm{inv}(x_2^2), \mathrm{Tr}(x_4^{p-1}), \mathrm{N}(x_4)\} = \{x_1, x_2^2, x_3^{p-1}, x_4^p\}.$$

Note that this set is algebraically independent. Let R denote the ring generated by $\{x_1, x_2^2, x_3^{p-1}, x_4^p\}$, then

$$P(R,t) = \frac{1}{(1-t)(1-t^2)(1-t^{p-1})(1-t^p)}$$

We will use the R–module structure of $\mathcal{A}$ to compute its Poincaré series. In order to understand the R–module structure we need to find module generators for $\mathcal{A}$. Let

$$\mathcal{D} = \{\mathrm{Tr}(x_3x_4^{p-1})\cdot\mathrm{Tr}(x_4^{p-2})\}\cup\{\overline{\mathrm{inv}}(x_2^2x_3^2)^{i+1}, \mathrm{inv}(x_2^3)\cdot\overline{\mathrm{inv}}(x_2^2x_3^2)^i \mid 1 \le i \le \ell/2-1\}$$

and let $\mathcal{M}$ be the R–submodule of $\mathcal{A}$ generated by 1, $\mathrm{LM}(\mathcal{C})$ and $\mathrm{LM}(\mathcal{D})$. We will start by computing the Poincaré series of $\mathcal{M}$. We shall see that the Poincaré series of $\mathcal{M}$ is equal to the Poincaré series of $\mathbf{F}_p[x_1,\ldots,x_4]^{\mathbf{Z}/p}$ and thus $\mathcal{M} = \mathcal{A} = \mathrm{LT}(\mathbf{F}_p[x_1,\ldots,x_4]^{\mathbf{Z}/p})$.

We impose a $\mathbf{Z}/2\times\mathbf{Z}/(p-1)$–grading on $\mathbf{F}_p[x_1,\ldots,x_4]$. A monomial $x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}$ will be assigned the multidegree $(i_2,i_3) \in \mathbf{Z}/2\times\mathbf{Z}/(p-1)$. Observe that the action of R preserves the multidegree. Since $\mathcal{A}$ is generated by monomials, $\mathcal{A}$ is a $\mathbf{Z}/2\times\mathbf{Z}/(p-1)$–graded R–module. Therefore all generators and relations can be chosen to be homogeneous with respect to the $\mathbf{Z}/2\times\mathbf{Z}/(p-1)$–grading.

If β and γ are monomials in $\mathbf{F}_p[x_1,\ldots,x_4]$ with the same multidegree, then the intersection of $R\beta$ with $R\gamma$ is the free R–module generated by the least common multiple of β and γ. In particular, an R–module generated by two monomials with the same multidegree has a single free relation.

We can use the results of Section 3 to describe $\mathrm{LM}(\mathcal{C})$. From Theorem 3.2 we see that, for $q \le j \le p-2$, we have $\mathrm{LM}(\mathrm{Tr}(x_4^j)) = x_2^{p-1-j}x_3^{2j-(p-1)}$. From Theorem 3.3 we see that, for $1 \le i \le p-2$, we have $\mathrm{LM}(\mathrm{Tr}(x_3^ix_4^{p-1})) = x_3^{i+p-1}$. From Theorem 3.4 we see that, for $3 \le i \le p-2$, we have $\mathrm{LM}(\mathrm{Tr}(x_3^ix_4^{p-2})) = x_2x_3^{i+p-3}$. Using Theorem 3.5 we see that, for $2\ell-1 \le j \le p-2$, we have $\mathrm{LM}(\mathrm{Tr}(x_3^2x_4^j)) = x_2^{p-1-j}x_3^{2j-p+3}$. Therefore

$$\mathrm{LM}(\mathcal{D}) = \{x_2x_3^{2p-3}\} \cup \{(x_2^2x_3^2)^{i+1}, x_2^3(x_2^2x_3^2)^i \mid 1 \le i \le \ell/2-1\}$$

and the R–module $\mathcal{M}$ is generated by the following families of monomials:
(i) 1 and $x_2x_3^{2p-3}$,
(ii) $(x_2^2x_3^2)^i$, $x_2^3(x_2^2x_3^2)^{i-1}$ for $1 \le i \le \ell/2$,
(iii) x_3^{p-1+i} for $1 \le i \le p-2$,
(iv) $x_2x_3^{p-3+i}$ for $3 \le i \le p-2$,
(v) $x_2^{p-1-j}x_3^{2j-p+1}$ for $q \le j \le p-2$ and
(vi) $x_2^{p-1-j}x_3^{2j-p+3}$ for $2\ell-1 \le j \le p-2$.

This list of monomials contributes either one or two elements to each multidegree. When there is one element in a given multidegree then the homogeneous component of $\mathcal{M}$ in that multidegree is a free R–module of rank one. If there are two elements in a given multidegree then the homogeneous component has two generators and a single free relation. Therefore we can write the Poincaré series of $\mathcal{M}$ as

$$P(\mathcal{M},t) = \frac{g(t)-r(t)}{(1-t)(1-t^2)(1-t^{p-1})(1-t^p)}$$

where $g(t)$ is the Poincaré series for the generators and $r(t)$ is the Poincaré series for the relations. Referring to our list of generators we see that

$$g(t) = 1 + t^{2p-2} + \sum_{i=1}^{\ell/2}\left(t^{4i}+t^{4i-1}\right) + \sum_{i=1}^{p-2} t^{p-1+i} + \sum_{i=3}^{p-2} t^{p-2+i} + \sum_{j=q}^{p-2} t^j + \sum_{j=2\ell-1}^{p-2} t^{j+2}.$$

To compute $r(t)$ we need to identify the multidegrees containing two generators and compute the degree of the least common multiple of the two generators. Sorting our generators into homogeneous components leads to the following relations:
(i) $\mathrm{lcm}((x_2x_3)^{2i}, x_3^{2i+p-1}) = x_2^{2i}x_3^{2i+p-1}$ for $1 \le i \le \ell/2$,
(ii) $\mathrm{lcm}(x_2^{2i+1}x_3^{2i-2}, x_2x_3^{2i+p-3}) = x_2^{2i+1}x_3^{2i+p-3}$ for $1 \le i \le \ell/2$,
(iii) $\mathrm{lcm}(x_2^{p-1-j}x_3^{2j-p+1}, x_2^{\varepsilon(j)}x_3^{2j}) = x_2^{p-1-j}x_3^{2j}$ for $q \le j \le p-3$, and
(iv) $\mathrm{lcm}(x_2^{p-1-j}x_3^{2j-p+3}, x_2^{\varepsilon(j)}x_3^{2j+2}) = x_2^{p-1-j}x_3^{2j+2}$ for $2\ell-1 \le j \le p-3$.

Thus

$$r(t) = \sum_{i=1}^{\ell/2}\left(t^{4i+p-1}+t^{4i+p-2}\right) + \sum_{j=q}^{p-3} t^{p-1+j} + \sum_{j=2\ell-1}^{p-3} t^{p+1+j}.$$

Form the polynomial $g(t)-r(t)$, evaluate the geometric series, and simplify, to get

$$g(t)-r(t) = \left(\frac{1-t^{p-1}}{1-t^4}\right)\left(1+t^3+t^q+t^{q+1}+t^{q+2}+t^{q+3}+t^{2\ell+1}+t^{2\ell+2}\right).$$

If $p \equiv 1 \pmod 3$, then $2\ell = q-1$ and

$$P(\mathcal{M},t) = \frac{1+t^3+2t^q+2t^{q+1}+t^{q+2}+t^{q+3}}{(1-t)(1-t^2)(1-t^4)(1-t^p)}.$$

If $p \equiv -1 \pmod 3$, then $2\ell = q+1$ and

$$P(\mathcal{M},t) = \frac{1+t^3+t^q+t^{q+1}+2t^{q+2}+2t^{q+3}}{(1-t)(1-t^2)(1-t^4)(1-t^p)}.$$

Comparing with [2, 3.1] we see that $P(\mathcal{M},t) = P(\mathbf{F}_p[x_1,\ldots,x_4]^{\mathbf{Z}/p},t)$ as required.

Remark 4.2. The simplification of $g(t)-r(t)$ was done by hand. The result can be confirmed using a computer algebra program such as Maple. If $f(t)$ denotes the numerator in the Poincaré series produced by Almkvist and Fossum, then the polynomial $(g(t)-r(t))\,(1-t^4) - f(t)(1-t^{p-1})$ is zero.

Corollary 4.3. *$\mathbf{F}_p[x_1,\ldots,x_4]^{\mathbf{Z}/p}$ is generated by homogeneous polynomials of degree less than or equal to $2p-3$.*

5. The five dimensional representation

Theorem 5.1. *$\mathbf{F}_p[x_1,\ldots,x_5]^{\mathbf{Z}/p}$ is generated by x_1, $\mathrm{inv}(x_2^2)$, $\mathrm{inv}(x_3^2)$, $\mathrm{inv}(x_2^3)$, $\overline{\mathrm{inv}}(x_3^3)$, $\overline{\mathrm{inv}}(x_2^2x_3^2x_4^2)$, $\mathrm{N}(x_5)$, $\mathrm{Tr}(x_2x_3x_5^{(p-1)/2})$ and the following families:*
(i) $\mathrm{Tr}(x_4^ix_5^{p-1})$ and $\mathrm{Tr}(x_2x_4^ix_5^{p-1})$ for $0 \le i \le p-2$,
(ii) $\mathrm{Tr}(x_4^ix_5^{p-2})$ and $\mathrm{Tr}(x_2x_4^ix_5^{p-2})$ for $3 \le i \le p-2$,
(iii) $\mathrm{Tr}(x_4^2x_5^j)$ and $\mathrm{Tr}(x_2x_4^2x_5^j)$ for $(p-1)/2 \le j \le p-2$.
(iv) $\mathrm{Tr}(x_5^j)$ for $(p+1)/2 \le j \le p-1$, and
(v) $\mathrm{Tr}(x_2x_5^j)$ for $(p-1)/2 \le j \le p-2$.

This section is devoted the proof of Theorem 5.1. The methods used are similar to those used in Section 4.

Let $\mathcal{C}$ denote the collection of invariants given in the statement of the preceding theorem. Let $\mathcal{A}$ denote the algebra generated by the lead monomials of $\mathcal{C}$. Using Theorem 3.2, we see that

$$\mathrm{LM}\{x_1, \mathrm{inv}(x_2^2), \mathrm{inv}(x_3^2), \mathrm{Tr}(x_5^{p-1}), \mathrm{N}(x_5)\} = \{x_1, x_2^2, x_3^2, x_4^{p-1}, x_5^p\}.$$

This is an algebraically independent subset of $\mathcal{A}$. Let R denote the ring generated by $\{x_1, x_2^2, x_3^2, x_4^{p-1}, x_5^p\}$. As in Section 4, if $p \equiv 1 \pmod 3$ then define $\ell = (p-1)/3$

and $q = 2\ell + 1$, if $p \equiv -1 \pmod 3$ then define $\ell = (p+1)/3$ and $q = 2\ell - 1$, and if i is a integer, define $\varepsilon(i)$ to be 0 if i is even and 1 if i is odd. Let

$$\mathcal{D}' = \{\mathrm{inv}(x_2^3)^i \cdot \overline{\mathrm{inv}}(x_3^3)^j \cdot \overline{\mathrm{inv}}(x_2^2x_3^2x_4^2)^k \mid i, j \in \{0,1\}, 0 \leq k \leq \ell/2 - 1 - j\},$$

and let

$$\mathcal{D} = \{\mathrm{Tr}(x_4x_5^{p-1}) \cdot \mathrm{Tr}(x_5^{p-2}), \mathrm{Tr}(x_2x_4x_5^{p-1}) \cdot \mathrm{Tr}(x_5^{p-2})\} \cup \mathcal{D}'.$$

Let $\mathcal{M}$ be the R–module generated by $\mathrm{LM}(\mathcal{C})$ and $\mathrm{LM}(\mathcal{D})$. Note that $\mathcal{M}$ is a subset of $\mathcal{A}$. We impose a $\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/(p-1)$–grading on $\mathbf{F}_p[x_1, \ldots, x_5]^{\mathbf{Z}/p}$. A monomial $x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}x_5^{i_5}$ will be assigned the multidegree

$$(i_2, i_3, i_4) \in \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/(p-1).$$

Observe that the action of R preserves the multidegree. Since $\mathcal{M}$ is generated by monomials, all generators and relations can be chosen to be homogeneous with respect to the $\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/(p-1)$–grading.

We can use the results of Section 3 to describe $\mathrm{LM}(\mathcal{C})$. From Theorem 3.2, for $(p-1)/2 \leq j \leq p-1$, we have $\mathrm{LM}(\mathrm{Tr}(x_5^j)) = x_3^{p-1-j}x_4^{2j-(p-1)}$. From Theorem 3.3, for $1 \leq i \leq p-2$, we have $\mathrm{LM}(\mathrm{Tr}(x_4^ix_5^{p-1})) = x_4^{i+p-1}$. From Theorem 3.4, for $3 \leq i \leq p-2$, we have $\mathrm{LM}(\mathrm{Tr}(x_4^ix_5^{p-2})) = x_3x_4^{i+p-3}$. Using Theorem 3.5 we see that, for $(p-1)/2 \leq j \leq p-2$, we have $\mathrm{LM}(\mathrm{Tr}(x_4^2x_5^j)) = x_3^{p-1-j}x_4^{2j-p+3}$. These results in conjunction with Theorem 3.6 allow us to compute $\mathrm{LM}(\mathrm{Tr}(x_2x_3x_5^{(p-1)/2}))$ and $\mathrm{LM}(\mathrm{Tr}(x_2x_4^ix_5^j))$ for the required values of i and j. Therefore

$$\mathrm{LM}(\mathcal{D}) = \{x_3x_4^{2p-3}, x_2x_3x_4^{2p-3}\} \cup \mathrm{LM}(\mathcal{D}')$$

and $\mathcal{M}$ is generated by the following families of monomials:

(i) 1, $x_3x_4^{2p-3}$ and $x_2x_3x_4^{2p-3}$,

(ii) $(x_2x_3x_4)^{2i}$, $x_3^{2i+1}(x_2x_4)^{2(i-1)}$ and $(x_2x_3)^{2i+1}x_4^{2(i-1)}$ for $1 \leq i \leq \ell/2 - 1$,
$x_2^{2i+1}(x_3x_4)^{2(i-1)}$ for $1 \leq i \leq \ell/2$,

(iii) x_4^{p-1+i} for $1 \leq i \leq p-2$, $x_2x_4^{p-1+i}$ for $0 \leq i \leq p-2$,
$x_3x_4^{p-3+i}$ and $x_2x_3x_4^{p-3+i}$ for $3 \leq i \leq p-2$, and

(iv) $x_2x_3^{p-1-j}x_4^{2j-p+1}$ and $x_3^{p-1-j}x_4^{2j-p+3}$ for $(p-1)/2 \leq j \leq p-2$,
$x_2x_3^{p-1-j}x_4^{2j-p+3}$ for $(p-1)/2 - 1 \leq j \leq p-2$,
$x_3^{p-1-j}x_4^{2j-p+1}$ for $(p+1)/2 \leq j \leq p-2$.

Thus the Poincaré series of the generators is given by

$$\begin{aligned} g(t) = 1 + (1+t)t^{2p-2} + t^{3\ell-3} + \sum_{i=1}^{\ell/2-1} \left(2t^{6i} + 2t^{6i-3}\right) \\ + \sum_{i=1}^{p-2} t^{p-1+i} + \sum_{i=0}^{p-2} t^{p+i} + (1+t)\sum_{i=3}^{p-2} t^{p-2+i} \\ + \sum_{j=(p+1)/2}^{p-2} t^j + \sum_{j=(p-1)/2}^{p-2} t^j(t+t^2) + \sum_{j=(p-3)/2}^{p-2} t^{j+3}. \end{aligned}$$

Evaluating the geometric series and simplifying gives

$$g(t) = \left(\frac{1+t^3}{1-t^3}\right)(1-t^{3\ell-3}) - t^{p-1} + \left(\frac{1+t}{1-t}\right)\left[2t^{(p+1)/2} - (1+t^2)t^{2p-3}\right].$$

Observe that each homogeneous component contains one, two, or three generators. If the component contains one generator then the component is a free module of rank one. If the component contains two generators then there is a single free relation generated by the least common multiple. If the component contains three generators then there are three relations given by the pairwise least common multiples and a single syzygy given by the least common multiple of all three generators. Thus the Poincaré series can be written as

$$P(\mathcal{M}, t) = \frac{g(t) - r_1(t) + s(t) - r_2(t)}{(1-t)(1-t^2)^2(1-t^{p-1})(1-t^p)}$$

where $r_1(t)$ is the Poincaré series for the free relations, $s(t)$ is the Poincaré series for the syzygies and $r_2(t)$ is the Poincaré series for the relations associated to the homogeneous components with three generators.

The free relations are given by:

(i) $\operatorname{lcm}(x_3^3, x_3x_4^{p-1}) = x_3^3x_4^{p-1}$,

(ii) $\operatorname{lcm}(x_3^{p-1-j}x_4^{2j-p+1}, x_3^{\varepsilon(j)}x_4^{2j}) = x_3^{p-1-j}x_4^{2j}$ and
$\operatorname{lcm}(x_2x_3^{p-1-j}x_4^{2j-p+1}, x_2x_3^{\varepsilon(j)}x_4^{2j}) = x_2x_3^{p-1-j}x_4^{2j}$ for $2\ell - 1 \le j \le p-3$,

(iii) $\operatorname{lcm}(x_3^{p-1-j}x_4^{2j-p+3}, x_3^{\varepsilon(j)}x_4^{2j+2}) = x_3^{p-1-j}x_4^{2j+2}$ and
$\operatorname{lcm}(x_2x_3^{p-1-j}x_4^{2j-p+3}, x_2x_3^{\varepsilon(j)}x_4^{2j+2}) = x_2x_3^{p-1-j}x_4^{2j+2}$ for $q-2 \le j \le p-3$.

Thus

$$r_1(t) = t^{p+2} + (1+t)t^{p-1}\left(\sum_{j=2\ell-1}^{p-3} t^j + \sum_{j=q-2}^{p-3} t^{j+2}\right).$$

Evaluate the geometric series to get

$$r_1(t) = t^{p+2} + (1+t)t^{p-1}\left(\frac{t^{2\ell-1} - t^{p-2} + t^q - t^p}{1-t}\right).$$

We need to describe the syzygies and the relations associated the homogeneous components with three generators. In the first line we list the three generators and in the second line we give the pairwise least common multiples followed by the least common multiple of the three monomials.

(i) $x_3^{p-1-j}x_4^{2j-p+1}, x_3^{\varepsilon(j)}x_4^{2j}, x_3^{3\varepsilon(j)}(x_2x_3x_4)^{2j-p+1}$
$x_3^{p-1-j}x_4^{2j}, x_3^{p-1-j}(x_2x_4)^{2j-p+1}, x_2^{2j-p+1}x_3^{2j-p+1+3\varepsilon(j)}x_4^{2j}; x_2^{2j-p+1}x_3^{p-1-j}x_4^{2j}$
for $(p+1)/2 \leq j \leq 2\ell-2$.

(ii) $x_2x_3^{p-1-j}x_4^{2j-p+1}, x_2x_3^{\varepsilon(j)}x_4^{2j}, x_2^3x_3^{3\varepsilon(j)}(x_2x_3x_4)^{2j-p+1}x_2x_3^{p-1-j}x_4^{2j},$
$x_2^3x_3^{p-1-j}(x_2x_4)^{2j-p+1}, x_2^{2j-p+4}x_3^{2j-p+1+3\varepsilon(j)}x_4^{2j}; x_2^{2j-p+4}x_3^{p-1-j}x_4^{2j}$
for $(p-1)/2 \leq j \leq 2\ell-2$.

(iii) $x_3^{p-1-j}x_4^{2j-p+3}, x_3^{\varepsilon(j)}x_4^{2j+2}, x_3^{3\varepsilon(j)}(x_2x_3x_4)^{2j-p+3}x_3^{p-1-j}x_4^{2j+2},$
$x_3^{p-1-j}(x_2x_4)^{2j-p+3}, x_2^{2j-p+3}x_3^{2j-p+3+3\varepsilon(j)}x_4^{2j+2}; x_2^{2j-p+3}x_3^{p-1-j}x_4^{2j+2}$
for $(p-1)/2 \leq j \leq q-3$.

(iv) $x_2x_3^{p-1-j}x_4^{2j-p+3}, x_2x_3^{\varepsilon(j)}x_4^{2j+2}, x_2^3x_3^{3\varepsilon(j)}(x_2x_3x_4)^{2j-p+3}x_2x_3^{p-1-j}x_4^{2j+2},$
$x_2^3x_3^{p-1-j}(x_2x_4)^{2j-p+3}, x_2^{2j-p+6}x_3^{2j-p+3+3\varepsilon(j)}x_4^{2j+2}; x_2^{2j-p+6}x_3^{p-1-j}x_4^{2j+2}$
for $(p-1)/2 - 1 \leq j \leq q-3$.

Thus

$$s(t) = \sum_{j=(p+1)/2}^{2\ell-2} t^{3j} + \sum_{j=(p-1)/2}^{2\ell-2} t^{3j+3} + \sum_{j=(p-1)/2}^{q-3} t^{3j+4} + \sum_{j=(p-3)/2}^{q-3} t^{3j+7}.$$

Evaluating the geometric series and simplifying gives

$$s(t) = \left(\frac{1}{1-t^3}\right)\left[2t^{3(p+1)/2}(1+t) - (1+t^3)(t^{6\ell-3} + t^{3q-2})\right].$$

The Poincaré series for the relations associated the homogeneous components with three generators is given by

$$\begin{aligned}
r_2(t) = {} & \sum_{j=(p+1)/2}^{2\ell-2} t^{j+p-1} + \sum_{j=(p-1)/2}^{2\ell-2} t^{j+p} + \sum_{j=(p-1)/2}^{q-3} t^{j+p+1} + \sum_{j=(p-3)/2}^{q-3} t^{j+p+2} \\
& + \sum_{j=(p+1)/2}^{2\ell-2} t^{3j-p+1} + \sum_{j=(p-1)/2}^{2\ell-2} t^{3j-p+4} + \sum_{j=(p-1)/2}^{q-3} t^{3j-p+5} + \sum_{j=(p-3)/2}^{q-3} t^{3j-p+8} \\
& + \sum_{j=(p+1)/2}^{2\ell-2} t^{6j-2(p-1)+3\varepsilon(j)} + \sum_{j=(p-1)/2}^{2\ell-2} t^{6j-2(p-1)+3\varepsilon(j)+3} \\
& + \sum_{j=(p-1)/2}^{q-3} t^{6j-2(p-1)+3\varepsilon(j)+6} + \sum_{j=(p-3)/2}^{q-3} t^{6j-2(p-1)+3\varepsilon(j)+9}.
\end{aligned}$$

Evaluating the geometric series in the first two lines, reindexing, and reorganizing the sums in the third and fourth lines gives

$$\begin{aligned}
r_2(t) = {} & \left(\frac{1}{1-t}\right)\Big[2t^{3(p-1)/2+1} - t^{2\ell+p-2} - t^{2\ell+p-1} + 2t^{3(p-1)/2+2} - t^{q+p-1} - t^{q+p})\Big] \\
& + \left(\frac{1}{1-t^3}\right)\Big[2t^{(p-1)/2+3} - t^{6\ell-p-2} - t^{6\ell-p+1} + 2t^{(p-1)/2+4} - t^{3q-p-1} - t^{3q-p+2}\Big] \\
& + \sum_{i=1}^{\ell/2-1} t^{6j+(p-1)} + \sum_{i=0}^{\ell/2-1} t^{6j+(p-1)+3} + \sum_{i=1}^{\ell/2-2} t^{6j+(p-1)+3} + \sum_{j=0}^{\ell/2-2} t^{6j+(p-1)+6}.
\end{aligned}$$

Let $n(t) = g(t) - r_1(t) + s(t) - r_2(t)$. Combining the previous expressions and simplifying gives

$$n(t) = \left(\frac{1-t^{p-1}}{1-t^3}\right)\left[(1+t^3)(1-t^{3\ell-3}+t^{6\ell-p-2}+t^{3q-p-1}) + 2t^{(p+1)/2}(1+t)^2\right].$$

Note that, for any prime p, $t^{3q-p-1} + t^{6\ell-p-2} - t^{3\ell-3} = t^p$. Thus

$$P(\mathcal{M},t) = \frac{(1+t^3)(1+t^p) + 2t^{(p+1)/2}(1+t)^2}{(1-t)(1-t^2)^2(1-t^3)(1-t^p)}.$$

Comparing with [2, 3.1] we see that $P(\mathcal{M},t) = P(\mathbf{F}_p[x_1,\ldots,x_5]^{\mathbf{Z}/p},t)$ as required. This completes the proof of Theorem 5.1.

Remark 5.2. As in Section 4, the simplification of the Poincaré series was done by hand but can be confirmed by a computer algebra program such as Maple. If we use $f(t)$ to denote the numerator of the Poincaré series produced by Almkvist and Fossum, then the polynomial $n(t)(1-t^3)-f(t)(1-t^{p-1})$ is zero.

Corollary 5.3. $\mathbf{F}_p[x_1,\ldots,x_5]^{\mathbf{Z}/p}$ *is generated by homogeneous polynomials of degree less than or equal to* $2p-2$.

6. Concluding remarks

We believe that, in principle, the methods used here could be extended to $n>5$ but that the computations required will become increasingly more complicated. Instead we suggest a more conceptual approach along the lines of the following conjecture. We remind the reader that rational invariants are the invariants in the image of the projection from $\mathbf{Z}[x_1,\ldots,x_n]^{\mathbf{Z}}$ to $\mathbf{F}_p[x_1,\ldots,x_n]^{\mathbf{Z}/p}$.

Conjecture 6.1. $\mathbf{F}_p[x_1,\ldots,x_n]^{\mathbf{Z}/p}$ *is generated by rational invariants, the image of the transfer and* $\mathrm{N}(x_n)$*.*

A proof of this conjecture would reduce the problem of finding an upper bound on the degrees of the generators to the relatively accessible problem of computing the image of the transfer. As philosophical evidence for the conjecture we include the following theorem.

Theorem 6.2. $\mathbf{F}_p[x_1,\ldots,x_n]^{\mathbf{Z}/p}$ *is an integral extension of the subalgebra generated by* $\mathrm{N}(x_n)$ *and the image of the transfer.*

Proof. It is sufficient to find a homogeneous system of parameters for $\mathbf{F}_p[x_1,\ldots,x_n]$ inside the subalgebra generated by $\mathrm{N}(x_n)$ and the image of the transfer. Consider the set

$$\mathcal{C}=\{\mathrm{Tr}(x_2^{p-1}),\mathrm{Tr}(x_3^{p-1}),\ldots,\mathrm{Tr}(x_n^{p-1}),\mathrm{N}(x_n)\}$$

Using Theorem 3.2, $\mathrm{LM}(\mathcal{C})=\{x_1^{p-1},x_2^{p-1},\ldots,x_{n-1}^{p-1},x_n^p\}$. Since $\mathrm{LM}(\mathcal{C})$ is a homogeneous system of parameters and we are using the graded reverse lexicographic order, $\mathcal{C}$ is a homogeneous system of parameters . □

Remark 6.3. The image of the transfer is an ideal in $\mathbf{F}_p[x_1,\ldots,x_n]^{\mathbf{Z}/p}$. The radical of this ideal is the intersection of the ideal generated by $x_1,\ldots,x_{n-1}$ in $\mathbf{F}_p[x_1,\ldots,x_n]$ with $\mathbf{F}_p[x_1,\ldots,x_n]^{\mathbf{Z}/p}$ (see [11, Remark 2.5]). It is not hard to show that $\mathbf{F}_p[x_1,\ldots,x_n]^{\mathbf{Z}/p}$ is generated by $\mathrm{N}(x_n)$ and the radical of the image of the transfer.

References

[1] G. Almkvist, Invariants, mostly old, *Pacific J. Math.* **86** (1980), 1–13.

[2] G. Almkvist and R. Fossum, *Decompositions of exterior and symmetric powers of indecomposable* $\mathbf{Z}/p\mathbf{Z}$*–modules in characteristic* p, Lecture Notes in Math. **641**, pp. 1–114, Springer–Verlag, 1978.

[3] 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.

[4] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Springer–Verlag, 1992.

[5] L.E.J. Dickson, *On invariants and the theory of numbers*, The Madison Colloquium (1913) A.M.S., reprinted by Dover, 1966.

[6] D. Hilbert, *Theory of algebraic invariants*, Cambridge University Press, 1993.

[7] G. Kemper, Calculating invariant rings of finite groups over arbitrary fields, *J. Sym. Comp.* **21** (1996), 351–366.

[8] G. Kemper, The INVAR Maple package, Gregor.Kemper@iwr.uni-heidelberg.de.

[9] L. Robbiano and M. Sweedler, *Subalgebra bases*, Lecture Notes in Math. **1430**, pp. 61–87, Springer–Verlag, 1990.

[10] L. Smith, *Polynomial invariants of finite groups*, A.K. Peters, Wellesley MA USA, 1995.

[11] R.J. Shank and D.L. Wehlau, The transfer in modular invariant theory, *J. of Pure and Applied Algebra*, to appear.

[12] K. Stråhlén, *On the invariants and their relations for the binary cubic modulo* 7, Masters Thesis, Lund Institute of Technology (1993).

[13] J.J. Sylvester, A synoptical table of the irreducible invariants and covariants to a binary quintic, with a scholium on a theorem in conditional hyperdeterminants, *American J. of Math.* **1** (1878), 370–378.

[14] W.L.G. Williams, Fundamental systems of formal modular seminvariants of the binary cubic, *Trans. of the A.M.S.* **22** (1921), 56–79.

R. James Shank
Department of Mathematics and Statistics
Queen's University
Kingston, Ontario K7L 3N6, Canada
e-mail: shank@mast.queensu.ca

(Received: January 22, 1997)