FORMAL MODULAR SEMIN INVARIANTS

R. JAMES SHANK

December 13, 1996

Abstract. We 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 then 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 $2p - 2$.

Introduction

Let $k$ be a field and define a linear function $\sigma$ by $\sigma(x_1) = x_1$ and, for $i > 1$, $\sigma(x_i) = x_i + x_{i-1}$. Extend $\sigma$ to an algebra automorphism of the polynomial algebra $k[x_1, \ldots, x_n]$. If $f \in k[x_1, \ldots, x_n]$ and $\sigma(f) = f$, then $f$ will be called $\sigma$-invariant. Since $\sigma$ is a degree preserving map, any $\sigma$-invariant polynomial is a sum of homogeneous $\sigma$-invariant polynomials. Thus we will restrict our attention to homogeneous polynomials. Let $k[x_1, \ldots, x_n]^\sigma$ denote the ring of $\sigma$-invariant polynomials. Suppose that $p$ is a prime number and let $F_p$ denote the field with $p$ elements. If $k = F_p$ and $n \leq p$, then $\sigma$ generates a group isomorphic to $\mathbb{Z}/p$ and we denote $k[x_1, \ldots, x_n]^\sigma$ by $F_p[x_1, \ldots, x_n]^{\mathbb{Z}/p}$. The action of $\mathbb{Z}/p$ induced by $\sigma$ on the degree one polynomials of $F_p[x_1, \ldots, x_n]$ is the indecomposable modular representation of dimension $n$. The study of $F_p[x_1, \ldots, x_n]^{\mathbb{Z}/p}$ 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 $F_p[x_1, \ldots, x_n]^{\mathbb{Z}/p}$ are the formal modular semivariants of a binary $(n-1)$-form [5, III]. Dickson gave a complete description of $F_p[x_1, \ldots, x_n]^{\mathbb{Z}/p}$ 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 [10], constructed a generating set for $n = 4$, $p = 7$. 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 $k$ is zero, then $\sigma$ generates a group isomorphic to $\mathbb{Z}$. In this case we denote $k[x_1, \ldots, x_n]^\sigma$ by $k[x_1, \ldots, x_n]^\mathbb{Z}$. Let $\mathbb{Q}$ denote the rational num-

1991 Mathematics Subject Classification. 13A50.

Key words and phrases. Invariant theory, Indecomposable modular representation.
bers. For any element \( f \in \mathbb{Q}[x_1, \ldots, x_n] \mathbb{Z} \), a suitable scalar multiple of \( f \) lies in \( \mathbb{Z}[x_1, \ldots, x_n] \). By reducing coefficients modulo \( p \), an element of \( \mathbb{Z}[x_1, \ldots, x_n] \mathbb{Z} \) gives rise to an element of \( \mathbb{F}_p[x_1, \ldots, x_n] \mathbb{Z}/p \). We will call elements of \( \mathbb{F}_p[x_1, \ldots, x_n] \mathbb{Z}/p \) constructed in this fashion rational invariants. G. Almkvist has shown that, if \( f \in \mathbb{F}_p[x_1, \ldots, x_n] \mathbb{Z}/p \) and the degree of \( f \) is small compared to \( p \), then \( f \) is a rational invariant [1, 2.5]. Thus characteristic zero computations will provide us with some of our generators.

Two constructions are needed to provide us with the remaining generators. The first of these constructions is the transfer. The transfer is a homomorphism of \( \mathbb{F}_p[x_1, \ldots, x_n] \mathbb{Z}/p \)-modules from \( \mathbb{F}_p[x_1, \ldots, x_n] \mathbb{Z}/p \) to \( \mathbb{F}_p[x_1, \ldots, x_n] \mathbb{Z}/p \) defined by

\[
\text{Tr}(f) = \sum_{c=1}^{p} \sigma^c(f).
\]

The second construction is the norm. For an element, \( f \), of \( \mathbb{F}_p[x_1, \ldots, x_n] \) the norm of \( f \), denoted by \( \text{N}(f) \), is the product over the orbit of \( f \). We shall see that, at least for \( n = 4 \) and \( n = 5 \), \( \mathbb{F}_p[x_1, \ldots, x_n] \mathbb{Z}/p \) is generated by \( \text{N}(x_n) \), 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 [8], 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 \( \mathbb{Q}[V_{\infty}] \mathbb{Z} \) formed by taking the union over \( n \) of \( \mathbb{Q}[x_1, \ldots, x_n] \mathbb{Z} \). We are able to construct a vector space basis for \( \mathbb{Q}[V_{\infty}] \mathbb{Z} \). 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 \( \mathbb{F}_p[x_1, \ldots, x_4] \mathbb{Z}/p \) and Section 5 contains the analogous result for \( \mathbb{F}_p[x_1, \ldots, x_5] \mathbb{Z}/p \). Section 6 is devoted to conclusions and conjectures.

We recommend [9] 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 ([6],[7]). 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 coefficient. We extend the monomial order to a partial order on polynomials by comparing lead monomials.

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

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

**Proof.** See [8, 1.16]. □

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

$$P(M, t) = \sum_{d=0}^{\infty} \dim_k(M_d)t^d.$$  

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

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

Choose a basis for $A_d$. Every element of this basis can be written as a linear combination of monomials of degree $d$. Using the monomial order, write the coefficients of each basis element as a row vector. The row vectors corresponding to the basis elements can be used to construct a matrix with linearly independent rows. Using row operations put this matrix in echelon form. The rows of the echelon form are the coefficients of a new basis, say $B$, for $A_d$. Since the coefficient matrix corresponding to $B$ is in echelon form, the lead monomials of the elements of $B$ 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 $\sigma$–invariant.

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

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

Let $b_i$ be the exponent of $x_i$ in $\beta$ and let $e_i$ be the exponent of $x_i$ in $\gamma$. Let $j$ be the first position at which the exponent sequence of $\beta x_{m-1}$ differs from the exponent sequence of $\gamma$. Since $\beta x_{m-1}$ and $\gamma$ 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 $j = m - 1$. Therefore $b_{m-1} + 1 > e_{m-1} \geq b_{m-1}$ and $\gamma = \beta x_m$. □

**Theorem 2.2.** If $\beta$ is a monomial in $k[x_1, \ldots, x_{m-1}]$ then $\beta x_m$ is not the lead term of a $\sigma$–invariant.
Proof. Suppose that \( f \in \mathbb{k}[x_1, \ldots, x_n] \) for some \( n \) and that the lead term of \( f \) is \( \beta x_m \). Then \( f = \beta x_m + h \) for some polynomial \( h \) with \( \text{LM}(h) < \text{LM}(f) \). We will prove that \( \text{LM} \circ (\sigma - 1)(f) = \beta x_{m-1} \); hence \( f \) is not \( \sigma \)-invariant.

Evaluating \( \sigma(x_m) \) and rearranging terms gives
\[
(\sigma - 1)(f) = (x_m + x_{m-1})(\sigma - 1)(\beta) + \sigma(\beta)x_{m-1} + (\sigma - 1)(h).
\]

We extend the monomial order to a partial order on polynomials by comparing lead monomials. Note that, for any monomial \( \gamma \), \( (\sigma - 1)\gamma < \gamma \). Thus \( (\sigma - 1)(h) < h < \beta x_m \) and \( x_m(\sigma - 1)(\beta) < x_m\beta \). From Lemma 2.1, \( \beta x_m \) and \( \beta x_{m-1} \) are consecutive in the order. Thus \( (\sigma - 1)(h) < \beta x_{m-1} \) and \( \text{LM}(x_m(\sigma - 1)(\beta)) \leq \beta x_{m-1}. \) Since \( \beta x_{m-1} \) is in \( \mathbb{k}[x_1, \ldots, x_{m-1}] \) and \( \text{LM}(x_m(\sigma - 1)(\beta)) \) is not equal to \( \beta x_{m-1} \). Therefore \( \text{LM} \circ (\sigma - 1)(f) = \beta x_{m-1} \). \( \square \)

**Theorem 2.3.** If \( \beta \) is a monomial in \( \mathbb{k}[x_1, \ldots, x_{m-1}] \) and \( i \geq 2 \) then \( \beta x_m^i \) is the lead monomial of a \( \sigma \)-invariant in \( \mathbb{k}[x_1, \ldots, x_n] \) for sufficiently large \( n \).

**Proof.** We prove the theorem by introducing an algorithm for constructing a \( \sigma \)-invariant with lead monomial \( \beta x_m^i \).

Apply \( \sigma - 1 \) to \( \beta x_m^i \) and observe that the lead term of \( (\sigma - 1)(\beta x_m^i) \) is \( i\beta x_{m-1}^{i-1} \).

Define \( f_1 = \beta x_m^i - i\beta x_{m-1}^{i-2}x_{m+1} \). Note that \( \text{LM} \circ (\sigma - 1)(f_1) < \beta x_{m-1}^{i-1} \).

For \( j > 1 \), if \( \text{LM} \circ (\sigma - 1)(f_{j-1}) = 0 \) then \( f_{j-1} \) is \( \sigma \)-invariant, otherwise write the lead term of \( (\sigma - 1)(f_{j-1}) \) as \( \gamma x_r^k \) with \( \gamma \in \mathbb{k}[x_1, \ldots, x_{r-1}] \) and \( k > 0 \) and define \( f_j = f_{j-1} - \gamma x_r^{k-1}x_{r+1} \).

Observe that \( \text{LM}(f_j) < \text{LM}(f_{j-1}) \). Thus \( \text{LM}(f_j) \) is a decreasing sequence of monomials in a fixed degree.

To prove that the algorithm terminates it is sufficient to prove that the set of monomials in countably many variables is well ordered by the graded reverse lexicographic order. We will, however, take a slightly different approach; one that will provide us with an upper bound on the number of variables required. For a monomial \( \lambda = \prod_s x_s^{i_s} \), define the weight of \( \lambda \) by \( \text{wt}(\lambda) = \sum_s s_i \).

Note that that the monomials in \( (\sigma - 1)(\lambda) \) all have weight less than \( \text{wt}(\lambda) \). Furthermore \( \text{wt}(\gamma x_r^{k-1}x_{r+1}) = \text{wt}(\gamma x_r^k) - 1 \).

Hence any monomial appearing in \( f_j \) has weight less than or equal to \( \text{wt}(\beta x_m^i) \).

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 \( \beta x_m^i \) and define \( \ell = \text{wt}(\beta x_m^i) - d + 1 \), then \( x_\ell^{d-1}x_\ell \) is the smallest monomial of degree \( d \) and weight \( \text{wt}(\beta x_m^i) \), and \( f_j \in \mathbb{k}[x_1, \ldots, x_\ell] \).

If \( \gamma \) is a monomial satisfying the hypotheses of Theorem 2.3, then let \( \text{inv}(\gamma) \) be the invariant produced by the algorithm. For convenience we define \( \text{inv}(x_1^i) = x_1^i \).

**Corollary 2.4.** The set of admissible monomials equals \( \text{LM}(\mathbb{Q}[V_{\infty}]^\mathbb{Z}) \).

If \( \gamma \) is a monomial satisfying the hypotheses of Theorem 2.3, then let \( \text{inv}(\gamma) \) be the invariant produced by the algorithm. For convenience we define \( \text{inv}(x_1^i) = x_1^i \).
Remark 2.5. Reviewing the algorithm, we observe that γ is the only admissible monomial appearing in inv(γ). Furthermore, if ℓ = wt(γ) − degree(γ) + 1, then inv(γ) is in \( k[x_1, \ldots, x_\ell]^\sigma \).

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

**Theorem 2.6.** \( B \) is a basis for the vector space \( Q[V_\infty]^Z \).

**Proof.** Since the elements of \( B \) have distinct lead monomials the set is linearly independent. To see that \( B \) is a spanning set, consider a polynomial \( f \in Q[V_\infty]^Z \). Let \( \Gamma \) be the set of admissible monomials appearing in \( f \) and for \( \gamma \in \Gamma \) let \( c_\gamma \) denote the coefficient of \( \gamma \) in \( f \). Let

\[
\tilde{f} = \sum_{\gamma \in \Gamma} c_\gamma \text{inv}(\gamma).
\]

The lead monomial of the invariant \( f - \tilde{f} \) is not admissible and, therefore, from Corollary 2.4, \( f - \tilde{f} = 0 \). Thus \( B \) spans \( Q[V_\infty]^Z \) as required. \( \Box \)

Using the algorithm we see that \( \text{inv}(x_2^2) = x_2^2 - x_1(x_2 + 2x_3) \),

\[
\text{inv}(x_3^3) = x_3^3 - x_2(x_3 + 2x_4) + x_1(x_3 + 3x_4 + 2x_5),
\]

and \( \text{inv}(x_2^3) = x_2^3 + x_1^2(3x_4 - x_2) - 3x_1x_2x_3 \). Explicit calculation shows that, although \( \text{inv}(x_3^3) \) involves \( x_1 \) through \( x_7 \), if we define

\[
\overline{\text{inv}}(x_3^3) = 2\text{inv}(x_3^3) - 3\text{inv}(x_2x_3^2) + 9x_1\text{inv}(x_4^2),
\]

we get an element of \( k[x_1, \ldots, x_5]^\sigma \) with lead monomial \( x_3^3 \). Similarly define

\[
\overline{\text{inv}}(x_2^2x_3^3) = 3\text{inv}(x_2^2x_3^3) + x_1(6\text{inv}(x_2x_3^2) - 8\text{inv}(x_3^3)) - x_1^2(9\text{inv}(x_4^2) + 8\text{inv}(x_3^3)),
\]

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

3. Lead Monomials of Transfers

In this section we compute the lead monomial for various elements in the image of the transfer. We will use LM to denote the operation which takes a polynomial and produces its lead monomial. Observe that

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

Therefore

\[
\text{Tr} \left(x_m^i x_m^j\right) = \sum_{c \in F_p} \left( \sum_{k=0}^{m-2} \binom{c}{k} x_{m-1-k} \right)^i \left( \sum_{j=0}^{m-1} \binom{c}{j} x_{m-j} \right)^j.
\]
Note that \( \binom{c}{i} \) is a polynomial in \( c \) of degree \( i \). The following lemma is well-known.

**Lemma 3.1.** Suppose that \( \ell \) is a positive integer. Then

\[
\sum_{c \in \mathbb{F}_p} c^\ell = \begin{cases} 
-1, & \text{if } p - 1 \text{ divides } \ell; \\
0, & \text{if } p - 1 \text{ does not divide } \ell.
\end{cases}
\]

**Proof.** See, for example, [3, 9.4]. \( \square \)

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

\[
LM \circ \text{Tr}(x_m^i) = x_{m-2}^{p-1-i} x_{m-1}^{2i-(p-1)}.
\]

**Proof.** Referring to 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

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

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 \( \text{Tr}(x_m^i) \). \( \square \)

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

\[
LM \circ \text{Tr}(x_{m-1}^{i} x_{m-1}^p) = x_{m-1}^{i+p-1}.
\]

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

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

\[
LM \circ \text{Tr}(x_{m-1}^{i} x_{m-2}^p) = x_{m-2}^{i+p-3}.
\]

**Proof.** Using Equation 3.2 we see that the coefficient of \( x_{m-2}^{i+p-3} \) in \( \sigma^c(x_{m-1}^{i} x_{m-2}^p) \) is \( ic^{p-1} + (p-2)\binom{c}{2}c^{p-3} \). Thus, using Lemma 3.1, the coefficient of \( x_{m-2}^{i+p-3} \) in \( \text{Tr}(x_{m-1}^{i} x_{m-2}^p) \) is \( -i + 1 \). As long as \( i \neq 1 \), this coefficient is non-zero. All of the monomials appearing in \( \sigma^c(x_{m-1}^{i} x_{m-2}^p) \) which are greater than \( x_{m-2}^{i+p-3} \) 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 \( \text{Tr}(x_{m-1}^{i} x_{m-2}^p) \). \( \square \)
Theorem 3.5. If \((p - 1)/2 - 1 \leq i \leq p - 1\) then
\[
LM \circ \text{Tr}(x_{m-1}^2 x_m^i) = x_{m-2}^{p-1-i} x_m^{2i-p+3}.
\]

Proof. We use Equation 3.2 to compute the coefficient of \(x_{m-2}^{p-1-i} x_m^{2i-p+3}\) 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 \(c^2 x_{m-2}^2\) with the rest of the term coming from \(\sigma^c(x_m^i)\). Thus the coefficient of \(x_{m-2}^{p-1-i} x_m^{2i-p+3}\) in \(\sigma^c(x_{m-1}^2 x_m^i)\) is
\[
c^{2i-p+1} \left( \begin{array}{c} c \\ 2 \end{array} \right)^{p-1-i} \left( \begin{array}{c} i \\ p - 1 - i \end{array} \right) + 2c^{2i-p+3} \left( \begin{array}{c} c \\ 2 \end{array} \right)^{p-2-i} \left( \begin{array}{c} i \\ p - 2 - i \end{array} \right) + c^{2i-p+5} \left( \begin{array}{c} c \\ 2 \end{array} \right)^{p-3-i} \left( \begin{array}{c} i \\ p - 3 - i \end{array} \right).
\]

Thus, using Lemma 3.1, the coefficient of \(x_{m-2}^{p-1-i} x_m^{2i-p+3}\) in \(\text{Tr}(x_{m-1}^2 x_m^i)\) is
\[
- \left( \begin{array}{c} 1 \\ 2 \end{array} \right)^{p-1-i} \left( \begin{array}{c} i \\ p - 1 - i \end{array} \right) - 2 \left( \begin{array}{c} 1 \\ 2 \end{array} \right)^{p-2-i} \left( \begin{array}{c} i \\ p - 2 - i \end{array} \right) - \left( \begin{array}{c} 1 \\ 2 \end{array} \right)^{p-3-i} \left( \begin{array}{c} i \\ p - 3 - i \end{array} \right).
\]

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
\[
\frac{-1}{2(i + 2)} \left( \begin{array}{c} 1 \\ 2 \end{array} \right)^{p-3-i} \left( \begin{array}{c} i \\ p - 3 - i \end{array} \right).
\]

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 \(x_{m-2}^{p-1-i} x_m^{2i-p+3}\) 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 \(\text{Tr}(x_{m-1}^2 x_m^i)\). \(\square\)

Theorem 3.6. Suppose that \(LM \circ \text{Tr}(\beta) \in \mathbb{F}_p[x_m, \ldots, x_n]\). Then
\[
LM \circ \text{Tr}(x_m \beta) = x_m LM \circ \text{Tr}(\beta).
\]

Proof. Using Equation 3.1, we see that
\[
\text{Tr}(x_m \beta) = \sum_{\sigma \in \mathbb{F}_p} \sigma^c(x_m) \sigma^c(\beta)
\]
\[
= \sum_{\sigma \in \mathbb{F}_p} \left( \sum_{j=0}^{m-1} \binom{c}{j} x_{m-j} \right) \sigma^c(\beta)
\]
\[
= x_m \text{Tr}(\beta) + \sum_{\sigma \in \mathbb{F}_p} \left( \sum_{j=1}^{m-1} \binom{c}{j} x_{m-j} \right) \sigma^c(\beta).
\]

Thus \(\text{Tr}(x_m \beta)\) is congruent, modulo the ideal generated by \(x_1\) through \(x_{m-1}\), to \(x_m \text{Tr}(\beta)\). Since \(LM \circ \text{Tr}(\beta)\) is in \(\mathbb{F}_p[x_m, \ldots, x_n]\), the lead monomial of \(\text{Tr}(x_m \beta)\) comes from \(x_m \text{Tr}(\beta)\). Therefore \(LM \circ \text{Tr}(x_m \beta) = x_m LM \circ \text{Tr}(\beta)\). \(\square\)
4. The Four Dimensional Representation

In this section we construct a generating set for \( F_p[x_1, \ldots, x_4]^{\mathbb{Z}/p} \). 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.** \( F_p[x_1, \ldots, x_4]^{\mathbb{Z}/p} \) is generated by \( x_1, \text{inv}(x_2^3), \text{inv}(x_2^3), \text{inv}(x_2^3 x_3), N(x_4) \) and the following families:

(i) \( \text{Tr}(x_3^i x_4^{p-1}) \) for \( 0 \leq i \leq p - 2 \),
(ii) \( \text{Tr}(x_3^i x_4^{p-2}) \) for \( 3 \leq i \leq p - 2 \),
(iii) \( \text{Tr}(x_4^j) \) for \( q \leq j \leq p - 2 \) and
(iv) \( \text{Tr}(x_3^i x_4^{j}) \) for \( 2\ell - 1 \leq j \leq p - 2 \).

This rest of this section is devoted to the proof of Theorem 4.1. Let \( C \) denote the collection of invariants given in the statement of the preceding theorem. We prove the theorem by showing that \( C \) is a S.A.G.B.I. basis for \( F_p[x_1, \ldots, x_4]^{\mathbb{Z}/p} \), i.e., the lead monomials of the elements of \( C \) generate the lead term algebra of \( F_p[x_1, \ldots, x_4]^{\mathbb{Z}/p} \).

We do this by computing the Poincaré series of the algebra generated by the lead monomials of \( C \) and comparing the result with the Poincaré series of \( F_p[x_1, \ldots, x_4]^{\mathbb{Z}/p} \) 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 \( C \) generate the lead term algebra of \( F_p[x_1, \ldots, x_4]^{\mathbb{Z}/p} \). Therefore, by Proposition 1.1, \( C \) generates \( F_p[x_1, \ldots, x_4]^{\mathbb{Z}/p} \).

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

\[
\text{LM}\{x_1, \text{inv}(x_2^3), \text{Tr}(x_4^{p-1}), N(x_4)\} = \{x_1, x_2^2, x_3^{p-1}, x_4^p\}.
\]

Note that this set is algebraically independent. Let \( R \) denote the ring generated by \( \{x_1, x_2^2, x_3^{p-1}, x_4^p\} \). Using elementary properties of Poincaré series we see that

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

We will use the \( R \)-module structure of \( A \) to compute its Poincaré series. In order to understand the \( R \)-module structure we need to find module generators for \( A \). Let

\[
D = \{\text{Tr}(x_3 x_4^{p-1}), \text{Tr}(x_4^{p-2})\} \cup \{\text{inv}(x_2 x_3)^i, \text{inv}(x_2 x_3)^j | 1 \leq i \leq \ell/2 - 1\}
\]

and let \( M \) be the \( R \)-module generated by \( 1, \text{LM}(C) \) and \( \text{LM}(D) \). Observe that \( M \) is an \( R \)-submodule of \( A \). We will now compute the Poincaré series of \( M \). We shall see that the Poincaré series of \( M \) is equal to the Poincaré series of \( F_p[x_1, \ldots, x_4]^{\mathbb{Z}/p} \) and thus \( M = A = \text{LT}(F_p[x_1, \ldots, x_4]^{\mathbb{Z}/p}) \).

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

If $\beta$ and $\gamma$ are monomials in $F_p[x_1, \ldots, x_4]$ 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 $\beta$ and $\gamma$. In particular, an $R$-module generated by two monomials with the same multidegree has a single free relation.

Using the results of Section 3, we see that the $R$-module $M$ is generated by the following families of monomials:

(i) $1$ and $x_2x_3^{2p-3}$,
(ii) $(x_2x_3^2)^i, x_2^3(x_2x_3^2)^{i-1}$ for $1 \leq i \leq \ell/2$,
(iii) $x_3^{p-1+i}$ for $1 \leq i \leq p - 2$,
(iv) $x_2x_3^{p-3+i}$ for $3 \leq i \leq p - 2$,
(v) $x_2^{p-1-j}x_3^{2j-p+1}$ for $q \leq j \leq p - 2$ and
(vi) $x_2^{p-1-j}x_3^{2j-p+3}$ for $2\ell - 1 \leq j \leq p - 2$.

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 $M$ 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 $M$ as

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

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

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

We rewrite our expression for $g(t)$ by combining the second sum and the third sum and making minor adjustments to the range of the indices giving

$$g(t) = 1 - t^{2p-3} - t^p - t^{p-1} + \sum_{i=1}^{\ell/2} t^i + t^{i-1} + \sum_{i=1}^{p-1} (t^{p-1+i} + t^{p-2+i}) + \sum_{j=q}^{p-2} t^j + \sum_{j=2\ell-1}^{p-2} t^{j+2}.$$
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) \( \text{lcm}(x_2 x_3^{2i}, x_3^{2i+p-1}) = x_2^{2i} x_3^{2i+p-1} \) for \( 1 \leq i \leq \ell/2 \),
(ii) \( \text{lcm}(x_2^{2i+1} x_3^{2i-2}, x_2 x_3^{2i+p-3}) = x_2^{2i+1} x_3^{2i+p-3} \) for \( 1 \leq i \leq \ell/2 \),
(iii) \( \text{lcm}(x_2^{p-1-j} x_3^{2j-p-1}, x_2 x_3^{2j}) = x_2^{p-1-j} x_3^{2j} \) for \( q \leq j \leq p-3 \), and
(iv) \( \text{lcm}(x_2^{p-1-j} x_3^{2j+p+1}, x_2 x_3^{2j+2}) = x_2^{p-1-j} x_3^{2j+2} \) for \( 2\ell-1 \leq j \leq p-3 \).

Thus

\[
\begin{align*}
r(t) &= \sum_{i=1}^{\ell/2} (t^{4i+p-1} + t^{4i+p-2}) + \sum_{j=q}^{p-3} (t^{p-1+j} + \sum_{j=2\ell-1}^{p-3} t^{p+1+j}).
\end{align*}
\]

Now form the polynomial \( g(t) - r(t) \) collecting terms when possible to get

\[
\begin{align*}
g(t) - r(t) &= 1 - t^{2p-3} - t^p - t^{p-1} + \sum_{i=1}^{\ell/2} \left( (t^{4i} + t^{4i-1}) - (t^{4i+p-1} + t^{4i+p-2}) \right) \\
&\quad + t^{p-2} + \sum_{j=q}^{p-3} (t^j - t^{p-1+j}) + t^p + \sum_{j=2\ell-1}^{p-3} (t^{j+2} - t^{p+1+j}) \\
&\quad + \sum_{i=1}^{p-1} (t^{p-1+i} + t^{p-2+i}).
\end{align*}
\]

Factoring gives

\[
\begin{align*}
g(t) - r(t) &= 1 - t^{2p-2} - t^{p-1} + t^{p-2} + (1 - t^{p-1}) \left( t^3 + t^4 \right) \sum_{i=1}^{\ell/2} t^{4i-4} \\
&\quad + (1 - t^{p-1}) \sum_{j=q}^{p-3} t^j + (1 - t^{p-1}) \sum_{j=2\ell-1}^{p-3} t^{j+2} \\
&\quad + t^{p-1} (1 + t) \sum_{i=1}^{p-1} t^{i-1}.
\end{align*}
\]

Evaluate the various geometric series to get
Theorem 5.1. If \( p \equiv 1 \pmod{3} \), then 2\( \ell = q - 1 \) and
\[
P(\mathcal{M}, t) = \frac{1 + t^3 + 2tq + 2tq+1 + tq+2 + tq+3}{(1-t)(1-t^2)(1-t^4)(1-tp)}.
\]
If \( p \equiv -1 \pmod{3} \), then 2\( \ell = q + 1 \) and
\[
P(\mathcal{M}, t) = \frac{1 + t^3 + tq + tq+1 + 2tq+2 + 2tq+3}{(1-t)(1-t^2)(1-t^4)(1-tp)}.
\]
Comparing with [2, 3.1] we see that \( P(\mathcal{M}, t) = P(F_p[x_1, \ldots, x_4]^\mathbb{Z}/p, t) \) as required.

**Corollary 4.2.** \( F_p[x_1, \ldots, x_4]^\mathbb{Z}/p \) is generated in degrees less than or equal to 2\( p - 3 \).

5. The Five Dimensional Representation

**Theorem 5.1.** \( F_p[x_1, \ldots, x_5]^\mathbb{Z}/p \) is generated by \( x_1, \inv(x_2^2), \inv(x_3^2), \inv(x_4^3), \inv(x_5^3), \overline{\inv(x_5)}, N(x_5), Tr(x_2x_3x_5^{(p-1)/2}) \) and the following families:
(i) \( Tr(x_i^ix_5^{p-1}) \) and \( Tr(x_2x_3x_5^{(p-1)/2}) \) for \( 0 \leq i \leq p - 2 \).
(ii) \( Tr(x_4x_5^{p-2}) \) and \( Tr(x_2x_4x_5^{p-2}) \) for \( 3 \leq i \leq p - 2 \).
(iii) \( Tr(x_4^jx_5^i) \) and \( Tr(x_2x_4^jx_5^i) \) for \( (p-1)/2 \leq j \leq p - 2 \).
(iv) $\text{Tr}(x_j^p)$ for $(p+1)/2 \leq j \leq p-1$, and
(v) $\text{Tr}(x^p)$ for $(p-1)/2 \leq j \leq p-2$.

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

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

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

$$D' = \{\text{inv}(x_2^3)^i \cdot \text{inv}(x_3^3)^j : i, j \in \{0, 1\}, 0 \leq k \leq \ell/2 - 1 - j\},$$

and let

$$D = \{\text{Tr}(x_4), \text{Tr}(x_5^{p-2}), \text{Tr}(x_2x_4x_5^{p-1}), \text{Tr}(x_5^{p-2})\} \cup D'.$$

Let $\mathcal{M}$ be the $R$–module generated by $\text{LM}(\mathcal{C})$ and $\text{LM}(D)$. Note that $\mathcal{M}$ is a subset of $\mathcal{A}$. Impose a $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/(p-1)$–grading on $\mathbb{F}_p[x_1, \ldots, x_5]^{\mathbb{Z}/p}$. 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

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

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 $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/(p-1)$–grading.

Using the results of Section 3 we see that the $R$–module $\mathcal{M}$ is generated by the following families of monomials:

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

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

$$(x_3x_4^{2i+1})^{(i-1)}$$

(iii) $x_3^{p-3}$ for $1 \leq i \leq p-2$, $x_3^{p-3}$ for $0 \leq i \leq p-2$,

$$(x_3x_4^{p-3})^{i-1}$$

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

$$(x_3x_4^{p-1-i})^{2i-1}x_4^{2i-p+3}$$

$$(x_3^{p-1-i})^{2i-p+3}$$

$$(x_3^{p-1-i})^{2i-p+1}$$

$$(x_3^{p-1-i})^{2i-p+1}$$

for $(p-1)/2 + 1 \leq i \leq p-2$. 


Thus the Poincaré series of the generators is given by

\[ g(t) = 1 + (1 + t)t^{2p-2} + t^{3t-3} + \sum_{i=1}^{p-1} \left( 2t^{6i} + 2t^{6i-3} \right) \]

\[ + \sum_{i=0}^{p-2} t^{p-1+i} + \sum_{i=3}^{p-2} t^{p+i} + (1 + t) \sum_{i=3}^{p-2} t^{p-2+i} \]

\[ + \sum_{j=(p+1)/2}^{p-2} t^j + \sum_{j=(p-1)/2}^{p-2} t^j(t^2) + \sum_{j=(p-3)/2}^{p-2} t^{j+3}. \]

Evaluating the geometric series gives

\[ g(t) = 1 + (1 + t)t^{2p-2} + t^{3t-3} + 2t^3(1 + t^3) \left( \frac{1 - t^{3t-6}}{1 - t^6} \right) \]

\[ + \left( \frac{1}{1-t} \right) \left[ t^p(1 - t^{p-2}) + t^p(1 - t^{p-1}) + (1 + t)t^{p-2}(t^3 - t^{p-1}) \right. \]

\[ \left. + t^{(p+1)/2} - t^{p-1} + (t + t^2)(t^{p-1}/2 - t^{p-1}) + t^3(t^{p-1}/2 - 1 - t^{p-1}) \right] \]

Simplifying and collecting terms gives

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

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 the homogeneous components with three generators.

The free relations are given by:

(i) \( \text{lcm}(x_3^p, x_4^{p-1}) = x_3^p x_4^{p-1} \),
Thus\[(ii) \ \text{lcm}(x_3^{p-1-j}x_4^{2j-p+1}, x_3^{e(j)}x_4^{2j}) = x_3^{p-1-j}x_4^{2j} \text{ and}
\text{lcm}(x_2x_3^{p-1-j}x_4^{2j-p+1}, x_2x_3^{e(j)}x_4^{2j}) = x_2x_3^{p-1-j}x_4^{2j} \text{ for } 2\ell - 1 \leq j \leq p - 3,\]
\[(iii) \ \text{lcm}(x_3^{p-1-j}x_4^{2j-p+3}, x_3^{e(j)}x_4^{2j+2}) = x_3^{p-1-j}x_4^{2j+2} \text{ and}
\text{lcm}(x_2x_3^{p-1-j}x_4^{2j-p+3}, x_2x_3^{e(j)}x_4^{2j+2}) = x_2x_3^{p-1-j}x_4^{2j+2} \text{ for } q - 2 \leq j \leq p - 3.\]
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 now 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) \[
x_3^{p-1-j}x_4^{2j-p+1}, x_3^{e(j)}x_4^{2j}, x_3^{3e(j)}(x_2x_3x_4)^{2j-p+1}
\text{ for } (p+1)/2 \leq j \leq 2\ell - 2.
\]
(ii) \[
x_2x_3^{p-1-j}x_4^{2j-p+1}, x_2x_3^{e(j)}x_4^{2j}, x_2x_3^{3e(j)}(x_2x_3x_4)^{2j-p+1}
\text{ for } (p-1)/2 \leq j \leq 2\ell - 2.
\]
(iii) \[
x_3^{p-1-j}x_4^{2j-p+3}, x_3^{e(j)}x_4^{2j+2}, x_3^{3e(j)}(x_2x_3x_4)^{2j-p+3}
\text{ for } (p-1)/2 \leq j \leq q - 3.
\]
(iv) \[
x_2x_3^{p-1-j}x_4^{2j-p+3}, x_2x_3^{e(j)}x_4^{2j+2}, x_2x_3^{3e(j)}(x_2x_3x_4)^{2j-p+3}
\text{ for } (p-1)/2 - 1 \leq j \leq q - 3.
\]
Thus
\[s(t) = \sum_{j=(p+1)/2}^{2\ell-2} t^{3j} + \sum_{j=(p-1)/2}^{2\ell-2} t^{3j+3} + \sum_{j=(p-1)/2}^{q-3} t^{3j+4} + \sum_{j=(p-3)/2}^{q-3} t^{3j+7}.
\]
Evaluate the geometric series to get
\[s(t) = \left( \frac{1}{1 - t^3} \right) \left[ 2t^{3(p+1)/2} - t^{6\ell-3} - t^{6\ell} + 2t^{3(p+1)/2+1} - t^{3q-2} - t^{3q+1} \right].\]
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

\[
r_2(t) = \sum_{j=0}^{\ell/2-1} t^{6j + (p-1)} + \sum_{j=0}^{\ell/2-2} t^{6j + (p-1)+3} + \sum_{j=0}^{\ell/2-2} t^{6j + (p-1)+6}.
\]

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

\[
r_2(t) = \left( \frac{1}{1-t^3} \right) \left[ 2t^{(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} \right]

+ \left( \frac{1}{1-t^3} \right) \left[ 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} \right]

+ \sum_{i=1}^{\ell/2-1} t^{6j+(p-1)} + \sum_{i=0}^{\ell/2-2} 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}.
\]

Evaluate the geometric series in the last line and simplify to get

\[
r_2(t) = \left( \frac{1}{1-t} \right) \left[ 2t^{3(p-1)/2+1} (1 + t) - (1 + t)(t^{2\ell+p-2} + t^{q+p-1}) \right]

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

+ \left( \frac{1}{1-t^6} \right) t^{p-1} \left[ t^3 + 2t^6 + t^9 - t^{3\ell-3}(1 + 2t^3 + t^6) \right].
\]

Further simplification gives
\[ r_2(t) = \left( \frac{1}{1-t} \right) \left[ 2t^{3(p-1)/2+1}(1 + t) - (1 + t)(t^{2t^p-2} + t^{q+p-1}) \right] \\
+ \left( \frac{1}{1-t^3} \right) \left[ 2t^{(p-1)/2+3}(1 + t) - (1 + t^3)(t^{6t^p-2} + t^{3q-p-1}) \right] \\
+ \left( \frac{1 + t^3}{1 - t^3} \right)t^{p-1}(t^3 - t^{3t^3}). \]

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

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

Collecting terms with common factors gives

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

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

Using the fact that \(1/(1 - t) = (1 + t + t^2)/(1 - t^3)\) to simplify the expression gives

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

Further simplification gives

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

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

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

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

**Corollary 5.2.** \(F_p[x_1, \ldots, x_5]_{Z/p}\) is generated in degrees 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. In particular the problem of computing the rational invariants becomes significantly more difficult as \(n\) increases. Instead we suggest a more conceptual approach along the lines of the following conjecture.

**Conjecture 6.1.** \(F_p[x_1, \ldots, x_n]_{Z/p}\) is generated by rational invariants, the image of the transfer and \(N(x_n)\).
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 conclude with
the following theorem.

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

**Proof.** It is sufficient to find a homogeneous system of parameters for \( \mathbb{F}_p[x_1, \ldots, x_n] \)
inside \( \mathbb{F}_p[x_1, \ldots, x_n]^{\mathbb{Z}/p} \). Consider the set
\[
C = \{ \text{Tr}(x_2^{p-1}), \text{Tr}(x_3^{p-1}), \ldots, \text{Tr}(x_n^{p-1}), N(x_n) \}
\]
Using Theorem 3.2, \( \text{LM}(C) = \{ x_1^{p-1}, x_2^{p-1}, \ldots, x_n^{p-1}, x_n \} \). Since \( \text{LM}(C) \) is a homoge-
neous system of parameters and we are using the graded reverse lexicographic order,
\( C \) is a homogeneous system of parameters .

**References**

2. G. Almkvist and R. Fossum, *Decompositions of exterior and symmetric powers of indecomposable
5. L.E.J. Dickson, *On invariants and the theory of numbers*, The Madison Colloquium (1913)
A.M.S., reprinted by Dover, 1966.
6. G. Kemper, *Calculating invariant rings of finite groups over arbitrary fields*, J. Sym. Comp. 21
7. ______, *The INVAR Maple package*, Gregor.Kemper@iwr.uni-heidelberg.de.
Verlag, 1990.
10. W.L.G. Williams, *Fundamental systems of formal modular seminvariants of the binary cubic,
Trans. of the A.M.S. 22 (1921) 56–79.

**Department of Mathematics and Statistics, Queen’s University, Kingston, Ontario, Canada, K7L 3N6**

**E-mail address:** shank@mast.queensu.ca