RINGS OF INVARIANTS FOR MODULAR REPRESENTATIONS
OF THE KLEIN FOUR GROUP

MÜFIT SEZER AND R. JAMES SHANK

ABSTRACT. We study the rings of invariants for the indecomposable modular representations of the Klein four group. For each such representation we compute the Noether number and give minimal generating sets for the Hilbert ideal and the field of fractions. We observe that, with the exception of the regular representation, the Hilbert ideal for each of these representations is a complete intersection.

INTRODUCTION

The modular representation theory of the Klein four group has long attracted attention. The group algebra of Klein four over an infinite field of characteristic 2 is one of the relatively rare examples of a group algebra with domestic representation type (see, for example, [2, §4.4]). If we work over an algebraically closed field, then for each even dimension there is a one parameter family of indecomposable representations and a finite number of exceptional indecomposable representations. For each odd dimension (greater than 1) there are only two indecomposable representations. In this paper we investigate the rings of invariants of the indecomposable representations of the Klein four group over fields of characteristic 2. For each such representation we compute the Noether number and give minimal generating sets for the Hilbert ideal and the field of fractions (definitions are given below). For an indecomposable representation of the Klein four group, say $V$, our results show that the Noether number is at most $2 \dim(V) + 1$ (detailed formulae are given later in this introduction) and, with the exception of the regular representation, the Hilbert ideal is generated by a homogeneous system of parameters. We note that the Hilbert ideals are generated by polynomials of degree at most 4, confirming Conjecture 3.8.6(b) of [9] for these representations.

We start with a few definitions and some notation. Suppose that $V$ is a finite dimensional representation of a finite group $G$ over a field $F$. The induced action on the dual space $V^*$ extends to the symmetric algebra $S(V^*)$ of polynomial functions on $V$ which we denote by $F[V]$. The action of $g \in G$ on $f \in F[V]$ is given by $(gf)(v) = f(g^{-1}v)$ for $v \in V$. The ring of invariant polynomials

$$F[V]^G = \{ f \in F[V] \mid g(f) = f \ \forall g \in G \}$$

Received by the editors October 1, 2013 and, in revised form, July 16, 2014.

2010 Mathematics Subject Classification. Primary 13A50.

The first author was partially supported by a grant from TÜBİTAK: 112T113.
is a graded, finitely generated subalgebra of $\mathbf{F}[V]$. The maximal degree of a polynomial in a minimal homogeneous generating set for $\mathbf{F}[V]^G$ is known as the Noether number of $V$. The ideal in $\mathbf{F}[V]$ generated by the homogeneous invariants of positive degree is the Hilbert ideal of $V$. If the characteristic of $\mathbf{F}$ divides $|G|$, then $V$ is called a modular representation. Rings of invariants for non-modular representations are reasonably well behaved. For instance, it is well known that if $V$ is non-modular, then $\mathbf{F}[V]^G$ is always Cohen-Macaulay and the Noether number is less than or equal to $|G|$ (see, for example, [9, §3.4, §3.8]). Both of these properties can fail in the modular case. Rings of invariants for modular representations are rarely Cohen-Macaulay, and there is no bound on the degrees of a generating set which depends only on the group order. Computing rings of invariants for modular representations can be difficult even in basic cases. Consider a representation of a cyclic $p$-group $\mathbf{Z}/p^r$ over a field of characteristic $p$. The action is easy to describe: up to a change of basis, a generator of the group acts by a sum of Jordan blocks each with eigenvalue 1 and size at most $p^r$. Despite this, even when $r = 1$, although the Noether numbers are known [12], an explicit generating set has been constructed for only a limited number of cases; see [23] for a summary and recent advances. For $r > 1$, much less is known; see [20] for the study of a specific case and [17] for some partial results on degree bounds. This paper is a part of a programme, initiated in [8], to understand the rings of invariants of modular representations of elementary abelian $p$-groups. In [8], the rings of invariants of all two dimensional representations and all three dimensional representations for groups of rank at most three were computed; in all cases the rings were shown to be complete intersections. The results in section 2 apply to an arbitrary group $G$, but for the rest of the paper $G := \langle \sigma_1, \sigma_2 \rangle \cong \mathbf{Z}/2 \times \mathbf{Z}/2$ denotes the Klein four group. For $\mathbf{F}$ an algebraically closed field of characteristic 2, the indecomposable representations of the Klein four group over $\mathbf{F}$ are the following:

- the trivial representation $\mathbf{F}$;
- the regular representation $V_{\text{reg}}$;
- a representation of dimension $2m$ for each $\lambda \in \mathbf{F} \cup \{\infty\}$, which we denote by $V_{m,\lambda}$;
- the representations $\Omega^m(\mathbf{F})$ and $\Omega^{-m}(\mathbf{F})$ of dimension $2m + 1$, where $\Omega$ denotes the Heller operator.

See [2, §4.4] for a detailed discussion of this classification. Note that $V_{m,0}$, $V_{m,1}$ and $V_{m,\infty}$, while not equivalent representations, are linked by group automorphisms. Therefore the invariants can be computed using the same matrix group and $\mathbf{F}[V_{m,0}]^G \cong \mathbf{F}[V_{m,1}]^G \cong \mathbf{F}[V_{m,\infty}]^G$. In [10], the depth of $\mathbf{F}[V]^G$ was computed for each of the indecomposable modular representations of the Klein four group. The only indecomposable representations for which the ring of invariants is Cohen-Macaulay are the the trivial representation, the regular representation, $V_{1,\lambda}$, $V_{2,\lambda}$, $\Omega^{-1}(\mathbf{F})$, $\Omega^{-2}(\mathbf{F})$ and $\Omega^1(\mathbf{F})$. Note that, for each of these representations, $\mathbf{F}[V]^G$ is a complete intersection. In [15] separating sets of invariants are given for the indecomposable modular representations of the Klein four group.

We identify $\mathbf{F}[V]$ with the polynomial algebra on the variables $x_i$ and $y_j$. We use the graded reverse lexicographic order (grevlex) with $x_i < y_j$, $x_i < x_{i+1}$ and $y_j < y_{j+1}$. We adopt the convention that a monomial is a product of variables and a term is a monomial multiplied by a coefficient. For a polynomial $f \in \mathbf{F}[V]$, we denote the leading monomial by $\text{LM}(f)$ and the leading term by $\text{LT}(f)$. We
make occasional use of SAGBI bases, the Subalgebra Analog of a Gröbner Basis for Ideals. For a subset $B = \{h_1, \ldots, h_\ell\}$ of a subalgebra $A \subset F[V]$ and a sequence $I = (i_1, \ldots, i_\ell)$ of non-negative integers, denote $\prod_{j=1}^\ell h_{i_j}^j$ by $h^I$. A tête-a-tète for $B$ is a pair $(h^I, h^J)$ with $\text{LM}(h^I) = \text{LM}(h^J)$; we say that a tête-a-tète is non-trivial if the support of $I$ is disjoint from the support of $J$. The reduction of an S-polynomial is a fundamental calculation in the theory of Gröbner bases. The analogous calculation for SAGBI bases is the subduction of a tête-a-tète. $B$ is a SAGBI basis for $A$ if every non-trivial tête-a-tète subductions to zero. A SAGBI basis is a particularly useful generating set for the subalgebra. For background material on SAGBI bases, see [21, §11] or [19, §3]. For $f \in F[V]$, we define the transfer of $f$ by $\text{Tr}(f) := \sum_{\sigma \in G} \sigma(f)$ and the norm of $f$, which we denote by $N_G(f)$, to be the product over the $G$-orbit of $f$. If the coefficient of a monomial $M$ in a polynomial $f$ is non-zero, we say that $M$ appears in $f$.

We conclude the introduction with a summary of the paper. Section 1 contains preliminary results on the invariant theory of $Z/2$. In section 2, we introduce the concept of a block hsop, a particularly nice homogeneous system of parameters, and prove a theorem which we use to compute Noether numbers. A recent result of Peter Symonds [22, Corollary 0.3] is a key ingredient in our proof. The results of this section are valid for any modular representation of a finite group.

In section 3, we consider the even dimensional representations. We include an explicit description of the group actions. We show that for $m > 1$, the Noether number for $\Omega^{-m}(F)$ is $m + 1$ (Corollary 4.2), the Noether number for $\Omega^m(F)$ is $3m$ for $m > 1$ (Corollary 5.2), and in that all cases the Hilbert ideal is generated by a block hsop. We give generating sets for the rings of invariants and for the other cases we give explicit input sets for the SAGBI/Divide-by-$x$ algorithm introduced in [8, §1].

The odd dimensional representations are considered in sections 4 and 5. We show that the Noether number for $\Omega^{-m}(F)$ is $m + 1$ (Corollary 4.2), the Noether number for $\Omega^m(F)$ is $3m$ for $m > 1$ (Corollary 5.2), and in that all cases the Hilbert ideal is generated by a block hsop. We give generating sets for $F[\Omega^{-m}(F)]^G[x_1^{-1}]$ and for $F[\Omega^m(F)]^G[(x_1x_2(x_1 + x_2))^{-1}]$. We also give explicit input sets for the SAGBI/Divide-by-$x$ algorithm.

1. Preliminaries

Let $F$ denote a field of characteristic 2. Suppose $\langle \sigma \rangle \cong Z/2$ acts on $S := F[x_1, \ldots, x_m, y_1, \ldots, y_m]$ by $\sigma(x_j) = x_j$, $\sigma(y_j) = y_j + x_j$. Define $\Delta := \sigma = 1$ and $n_i := y_i^2 + x_i y_i$. We will often write $S^\sigma$ as shorthand for $S^{(\sigma)}$.

Proposition 1.1 ([16], [5], [7]). $S^\sigma$ is generated by
$$\{n_1, \ldots, n_m\} \cup \{\Delta(\beta) \mid \beta \text{ divides } y_1 \cdots y_m\}.$$  

Corollary 1.2. $\Delta S = ((x_1, \ldots, x_m) S)^\sigma$ and $S^\sigma/\Delta S \cong F[n_1, \ldots, n_m]$.

Proof. It is clear from the definition of $\Delta$ that $\Delta S \subseteq (x_1, \ldots, x_m) S$. Since $\Delta^2 = 0$, we have $\Delta S \subseteq ((x_1, \ldots, x_m) S)^\sigma$. The result then follows from the definition of $n_i$ and the generating set for $S^\sigma$ given above. \hfill \Box

Proposition 1.1 and Corollary 1.2 give the following.
Lemma 1.3. Suppose \( a_1, \ldots, a_m \) are non-negative integers. Let \( f \in S^\sigma \).

(i) If \( y_1^{a_1} \cdots y_m^{a_m} \) appears in \( f \), then \( a_i \) is even for \( i \in \{1, \ldots, m\} \).

(ii) If \( y_1^{a_1} \cdots y_{m-1}^{a_{m-1}} y_m x_m \) appears in \( f \), then \( a_i \) is even for \( i \in \{1, \ldots, m-1\} \).

A simple calculation shows that for \( a, b \in S \),
\[
\Delta(a \cdot b) = \Delta(a)b + a\Delta(b) + \Delta(a)\Delta(b)
\]
and \( \Delta(a^2) = \Delta(a)^2 \). Therefore, if \( M = y_1^{a_1} \cdots y_m^{a_m} \) with \( a_i > 0 \), then the monomial \( x_i M/\gamma_i \) appears in \( \Delta(M) \) with coefficient 1 if \( a_i \) is odd and coefficient 0 if \( a_i \) is even. Note that if a monomial \( M \) appears (with non-zero coefficient) in \( f \in S^\sigma \) and a monomial \( M' \) appears in \( \Delta(M) \), then there is at least one further monomial, say \( M'' \), with \( M \neq M'' \), such that \( M'' \) appears in \( f \) and \( M' \) appears in \( \Delta M'' \).

Lemma 1.4. Suppose \( M' \) is a monomial in \( \{y_1, \ldots, y_m\} \) and \( M = M'x_i y_j \) for some \( i, j \in \{1, \ldots, m\} \) with \( i \neq j \). Assume further that the degree of \( y_j \) in \( M' \) is even. If \( M \) appears in a polynomial \( f \in S^\sigma \), then the degree of \( y_i \) in \( M' \) is even and \( M'x_j y_i \) also appears in \( f \). Moreover, the coefficients in \( f \) of these monomials are the same.

Proof. Since the degree of \( y_j \) in \( M \) is odd, \( M'x_ix_j \) appears in \( \Delta(M) \) with coefficient 1. Note that if the degree of \( y_i \) in \( M' \) is odd, then there is no other monomial in \( S \) that produces \( M'x_ix_j \) after applying \( \Delta \). Therefore, we may assume that the degree of \( y_i \) in \( M' \) is even. In this case, \( M'x_ix_j \) appears in \( \Delta(M'y_i x_j) \) and in \( \Delta(M'y_j x_j) \). However, the degree of \( y_j \) in the monomial \( M'y_i y_j \) is odd, so it follows from Lemma 1.3 that \( M'y_j x_i \) does not appear in \( f \). Therefore \( M'y_i y_j \) appears in \( f \). Since the coefficient of \( M'x_i x_j \) in both \( \Delta(M'y_i x_j) \) and \( \Delta(M'y_j x_i) \) is 1, the coefficients of \( M'y_i x_j \) and \( M'y_j x_i \) in \( f \) must be equal. \( \square \)

Lemma 1.5. Suppose that \( M' \) is a monomial in \( \{y_1, \ldots, y_m\} \setminus \{y_j\} \) for some \( j \in \{1, \ldots, m\} \) and \( M = M'y_j x_j \). For \( f \in S^\sigma \), \( M \) appears in \( f \) if and only if \( M'y_j^2 \) appears in \( f \). Moreover, the coefficients in \( f \) of these monomials are the same. Finally, \( M'y_j^2 x_j \) does not appear in any polynomial in \( S^\sigma \).

Proof. Note that \( M'y_j^2 \) appears in both \( \Delta(M) \) and \( \Delta(M'y_j^2) \) with coefficient 1. Since these are the only monomials in \( S \) that produce \( M'y_j^2 x_j \) after applying \( \Delta \), the result follows. The final statement follows from the fact that \( M'y_j^2 x_j \) is the only monomial in \( S \) that produces \( M'y_j^2 x_j \) after applying \( \Delta \). \( \square \)

2. Block HSOPs

In this section, \( G \) is an arbitrary finite group, \( F \) is a field of characteristic \( p \) for some prime number \( p \) dividing the order of \( G \) and \( V \) is a finite dimensional \( FG \)-module. Suppose we have a homogeneous system of parameters \( S = \{h_1, \ldots, h_n\} \) for \( F[V]^G \). Let \( A \) denote the algebra generated by \( S \) and let \( I \) denote the ideal \( (h_1, \ldots, h_n)F[V] \). Further suppose that there exists a term order for which \( S \) is a Gröbner basis for \( I \) and the reduced monomials are the monomial factors of a given monomial, say \( \beta \). Then the monomial factors of \( \beta \) are a basis for \( F[V] \) as a free \( A \)-module; in the language of [3], we have a block basis for \( F[V] \) over \( A \). In this situation, we will refer to \( S \) as a block hsop and \( \beta \) as the top class. Note that if the elements of \( \{LM(h_1), \ldots, LM(h_n)\} \) are pair-wise relatively prime, then \( S \) is a block hsop and the top class is the unique maximal reduced monomial.
**Theorem 2.1.** Suppose \( S = \{h_1, \ldots, h_n\} \) is a block hsp with top class \( \beta \). If \( \text{Tr}(\beta) \) is indecomposable in \( F[V]^G \), then

(a) the Noether number for \( V \) is \( \deg(\beta) \);
(b) the Hilbert ideal of \( V \) is generated by \( S \).

**Proof.** Proof of (a): The indecomposability of \( \text{Tr}(\beta) \) gives a lower bound on the Noether number. The fact that \( \deg(\beta) \) is also an upper bound follows from [22 Corollary 0.3].

Proof of (b): Denote the Hilbert ideal of \( V \) by \( h \). Since \( S \subset F[V]^G \), we have \( I \subseteq h \). Suppose, by way of contradiction, that there exists \( f \in h \setminus I \). We may assume that \( f \) is homogeneous and that \( \text{LM}(f) \) is reduced with respect to \( I \) using the chosen term order. Therefore \( \text{LM}(f) \) divides \( \beta \). Reducing \( \beta \) with respect to \( S \cup \{f\} \) produces a polynomial of degree \( d := \deg(\beta) \) with lead term less than \( \beta \). However, \( F[V]/I \) in degree \( d \) has dimension one. Thus \( \beta \in (h_1, \ldots, h_n, f)F[V] \subseteq h \). Let \( C \) be the reduced monomials with respect to \( h \) using the chosen term order. Observe that the elements of \( C \) are monomial factors of \( \beta \) with degree less than \( d \). Since \( C \) generates \( F[V] \) as an \( F[V]^G \)-module, the transfer ideal, \( \text{Tr}(F[V]) \), is generated by \( \{\text{Tr}(\gamma) \mid \gamma \in C\} \) as an \( F[V]^G \)-module. Therefore,

\[
\text{Tr}(\beta) = \sum_{\gamma \in C} c_\gamma \text{Tr}(\gamma)
\]

for some \( c_\gamma \in F[V]^G \). Since the representation is modular, \( \text{Tr}(1) = 0 \). Furthermore \( \deg(\text{Tr}(\gamma)) < d \). Therefore, the equation above gives a decomposition of \( \text{Tr}(\beta) \) in terms of invariants of degree less than \( d \), contradicting the indecomposability of \( \text{Tr}(\beta) \). \( \square \)

### 3. Even dimensional representations

In this section we consider the even dimensional representations \( V_{m,\lambda} \). For completeness, we also include a brief discussion of the regular representation in subsection 3.1. For \( \lambda \in F \), the action of \( G = \langle \sigma_1, \sigma_2 \rangle \) on \( S := F[V_{m,\lambda}] = F[x_1, \ldots, x_m, y_1, \ldots, y_m] \) is given by \( \sigma_1(x_j) = x_j, \sigma_1(y_j) = y_j + x_j, \sigma_2(y_j) = y_j + \lambda x_j \) and \( \sigma_2(y_j) = y_j + \lambda x_j + x_{j-1} \) for \( j > 1 \). Define \( n_i := y_i^2 + x_i y_i \) and \( u_{ij} := x_i y_j + x_j y_i \). Then \( n_i, u_{ij} \in S^{G_1} \). A simple calculation gives \( \Delta_2(n_i) = (\lambda^2 + \lambda)x_i^2 + x_{i-1}^2 + x_i x_{i-1} \) and \( \Delta_2(u_{ij}) = x_i x_{j-1} + x_{i-1} x_j \) (using the convention that \( x_0 = 0 \)).

Define \( \ell := \lceil m/2 \rceil \). An explicit calculation, exploiting the fact that \( \Delta_2(u_{1j}) = x_1 x_{j-1}, \) gives \( \Delta_2(N_i) = 0 \). Therefore \( N_i \in S^G \). Define

\[
H := \{x_1, \ldots, x_m \cup \{N_i \mid 1 \leq i \leq \ell/2\} \cup \{N_G(y_j) \mid m/2 < j \leq m\}\}.
\]

**Theorem 3.1.** \( H \) is a block hsp with top class \( y_1 \cdots y_\ell y_{\ell+1} \cdots y_m \).

**Proof.** This follows from the fact that \( \text{LT}(N_i) = y_i^2 \) and \( \text{LT}(N_G(y_j)) = y_j^4 \). \( \square \)

**Corollary 3.2.** The image of the transfer, \( \text{Tr}(S) \), is the ideal in \( S^G \) generated by

\[
\{\text{Tr}(\beta) \mid \beta \text{ divides } y_1 \cdots y_\ell(y_{\ell+1} \cdots y_m)^3\}.
\]
Theorem 3.3. For $\lambda \not\in \mathbb{F}_2$ and $m \geq 3$, $\text{Tr}(y_1 \cdots y_{i+1}^3 \cdots y_m^3)$ is indecomposable.

See subsection 3.13 for the proof of Theorem 3.3. Combining Theorem 3.3 with Theorem 2.1 gives the following.

Corollary 3.4. If $\lambda \not\in \mathbb{F}_2$ and $m \geq 3$, then the Noether number for $V_{m,\lambda}$ is $3m - 2\lfloor m/2 \rfloor$ and the Hilbert ideal is generated by $\mathcal{H}$.

Descriptions of $S^G$ for $m \leq 3$ are given in subsection 3.14. The formula given above for the Noether number is valid for $m > 1$.

For $j > 1$, an explicit calculation gives

\[
\text{Tr}(y_1 y_2 y_j) = y_1(x_2 x_{j-1} + x_1 x_j) + y_2 x_1 x_{j-1} + y_j x_1^2
\]
\[
+ x_1 x_2((\lambda^2 + \lambda)x_j + x_{j-1}) + x_1^2(x_j + x_{j-1})
\]
\[
= u_{12} x_{j-1} + u_{1j} x_1 + \text{Tr}(y_1 y_3) ((\lambda^2 + \lambda)x_j + x_{j-1})
\]
\[
+ \text{Tr}(y_1 y_2)(x_j + x_{j-1}).
\]

Therefore $t_j := u_{12} x_{j-1} + u_{1j} x_1 \in \text{Tr}(S)$.

Theorem 3.5. For $m > 3$ and $\lambda \not\in \mathbb{F}_2$,

\[
F[V_{m,\lambda}]^G[x_1^{-1}] = F[x_1, \ldots, x_m, N_1, N_2, t_3, \ldots, t_m][x_1^{-1}].
\]

Proof. We use [4, Theorem 2.4]. $F[x_1, \ldots, x_m, y_1]^G$ is the polynomial algebra generated by $\{x_1, \ldots, x_m, N_G(y_1)\}$. Since $N_1 = y_1^2 + x_1 y_1 + (\lambda^2 + \lambda)(x_1 y_2 + x_2 y_1)$, we see that $N_1 \in F[x_1, x_2, y_1, y_2]$ is degree 1 in $y_2$ with coefficient $(\lambda^2 + \lambda)x_1$. Using the equation above, $t_j \in F[x_1, \ldots, x_m, y_1, y_2, y_j]$ is degree 1 in $y_j$ with coefficient $x_1^2$. Thus $S^G[x_1^{-1}] = F[x_1, \ldots, x_m, N_G(y_1), N_1, t_3, \ldots, t_m][x_1^{-1}]$. To complete the proof, we need only rewrite $N_G(y_1)$ in terms of $N_2$ and the other generators. An explicit calculation gives

\[
N_G(y_1) = y_1^4 + x_1^2 y_1^2(\lambda^2 + \lambda + 1) + x_1^3 y_1(\lambda^2 + \lambda).
\]

Define $c := \lambda^2 + \lambda$. Subduction gives

\[
N_G(y_1) = N_1^2 + ((cx_2)^2 + cx_1^2)N_1 + (cx_1)^2 N_2 + (c^3 x_2 + c^2 x_1) t_3 + c^3 x_4 t_4,
\]

as required. \hfill \Box

Remark 3.6. For $m > 3$ and $\lambda \not\in \mathbb{F}_2$, it follows from Theorem 3.5 and Theorem 3.1 that $S^G$ is the normalisation of the algebra generated by $B := \mathcal{H} \cup \{t_3, \ldots, t_m\}$. Furthermore, applying the SAGBI/Divide-by-$x$ algorithm of [8] with $x = x_1$ to $B$ computes a SAGBI basis for $S^G$.

Using the familiar formula for the group cohomology of a cyclic group, we have

\[
H^1(\langle \sigma_2 \rangle, \Delta_1 S) \cong (\Delta_1 S)^{\sigma_2} / \Delta_2 \Delta_1 S = (\Delta_1 S)^{\sigma_2} / \text{Tr} S
\]

and

\[
H^1(\langle \sigma_1 \rangle, \Delta_2 S) \cong (\Delta_2 S)^{\sigma_1} / \text{Tr} S.
\]

Note that $H^1(\langle \sigma_1 \rangle, \Delta_2 S)$ and $H^1(\langle \sigma_2 \rangle, \Delta_1 S)$ are both finitely generated $S^G$-modules and, therefore, are also finitely generated over the algebra generated by $\mathcal{H}$. In the following $\sqrt{\text{Tr} S}$ denotes the radical of the image of the transfer.

Proposition 3.7. For $\lambda \not\in \mathbb{F}_2$, $(\Delta_2 S)^{\sigma_1} = (\Delta_1 S)^{\sigma_2} = (x_1, \ldots, x_m, S)^G = \sqrt{\text{Tr} S}$ and

\[
\sqrt{\text{Tr} S} / \text{Tr} S \cong H^1(\langle \sigma_2 \rangle, \Delta_1 S) \cong H^1(\langle \sigma_1 \rangle, \Delta_2 S).
\]

Furthermore $S^G / \sqrt{\text{Tr} S} \cong F[N_1, \ldots, N_\ell, N_G(y_{\ell+1}), \ldots, N_G(y_m)]$. \hfill \Box
Proof. For $\lambda \not\in \mathbb{F}_2$,
\[
\Delta_1 V^*_{m,\lambda} = \Delta_2 V^*_{m,\lambda} = (\sigma_1 \sigma_2 + 1) V^*_{m,\lambda} = \text{Span}_F \{ x_1, \ldots, x_m \}.
\]
Using [18] Theorem 2.4 (see also [11] Theorem 2.4), $\sqrt{\text{Tr} S} = ((x_1, \ldots, x_m)S)^G$. Applying Proposition [1.1] with $\sigma = \sigma_1$ gives $\Delta_1 S = ((x_1, \ldots, x_m)S)^{\sigma_1}$. Thus $(\Delta_1 S)^{\sigma_2} = ((x_1, \ldots, x_m)S)^G$. Applying Proposition [1.1] with $\sigma = \sigma_2$ gives $(\Delta_2 S)^{\sigma_1} = ((x_1, \ldots, x_m)S)^G$.

To prove the final statement, first observe that
\[
N := \{ N_1, \ldots, N_\ell, N_G(y_{\ell+1}), \ldots, N_G(y_m) \}
\]
is algebraically independent modulo $\sqrt{\text{Tr} S}$. Therefore, there is a subalgebra of $S^G/\sqrt{\text{Tr} S}$ isomorphic to $A := \mathbb{F}[N_1, \ldots, N_\ell, N_G(y_{\ell+1}), \ldots, N_G(y_m)]$. We will show that for every $f \in S^G$, there exists $F \in A$ with $f - F \in \sqrt{\text{Tr} S}$. We proceed with a minimal counterexample. Without loss of generality, we may assume $f$ is homogeneous of positive degree. Since $\text{LM}(g(y_i)) = y_i$ for all $g \in G$, using [19] Theorem 3.2, there exists a finite SAGBI basis for $S^G$ and therefore a finite SAGBI-Gröbner basis for the ideal $\sqrt{\text{Tr} S}$. We may assume that $f$ is reduced, i.e., equal to its normal form. Therefore $\text{LM}(f) = \prod_{i=1}^m y_i^{a_i}$. Using Lemma [1,3] each $a_i$ is even. It follows from Proposition [3.15,2] that $\text{LM}(f)$ does not divide $\prod_{i=1}^m y_i^{2}$.

Since $\text{LT}(N_i) = y_i^2$ and $\text{LT}(N_G(y_j)) = y_j^4$, there exits $N \in N$ with $\text{LT}(N) = y_k^{b_k}$ dividing $\text{LM}(f)$. Note that $N = y_k^{b_k} + \bar{N}$ for some $\bar{N} \in (x_1, \ldots, x_m)S$. Since $N$ is monic as a polynomial in $y_k$, we can divide $f$ by $N$ to get $f = qN + r$ for unique $q, r \in S$ with $\deg_{y_k}(r) < \deg_{y_k}(N) = b_k$. Furthermore, since we are using grevlex with $x_i < y_k$, we have $\text{LM}(r) < \text{LM}(f)$. Applying $g \in G$ gives $f = g(f) = g(q)N + g(r)$. However, $\deg_{y_k}(g(r)) \leq \deg_{y_k}(r)$. Therefore, by the uniqueness of the remainder, $g(r) = r$ and $g(q) = q$. Thus $q, r \in S^G$ with $q < f$ and $r < f$. By the minimality of $f$, there exists $F_1, F_2 \in A$ with $q - F_1, r - F_2 \in \sqrt{\text{Tr} S}$. Therefore $F := NF_1 - F_2 \in A$ and $f - F \in \sqrt{\text{Tr} S}$, giving the required contradiction. 

While $V_{m,0}$ and $V_{m,1}$ are not equivalent representations, the automorphism of $G$ which fixes $\sigma_1$ and exchanges $\sigma_2$ and $\sigma_1 \sigma_2$, takes $V_{m,0}$ to $V_{m,1}$. Therefore $\mathbb{F}[V_{m,0}]^G \cong \mathbb{F}[V_{m,1}]^G$. Hence, to compute $\mathbb{F}[V_{m,\lambda}]^G$ with $\lambda \in \mathbb{F}_2$, it is sufficient to take $\lambda = 0$.

Substituting $\lambda = 0$ into the expression for $N_i$ given above gives an element in $\mathbb{F}[V_{m,0}]^G$ with lead term $y_i^2$ for $i \leq [m/2]$. Define $\ell' := [m/2]$ and
\[
\mathcal{H}' := \{ x_1, \ldots, x_m \} \cup \{ N_i \mid 1 \leq i \leq (m + 1)/2 \} \cup \{ N_G(y_j) \mid (m + 1)/2 < j \leq m \}.
\]
Looking at lead terms gives the following.

**Theorem 3.8.** For $\lambda \in \mathbb{F}_2$, $\mathcal{H}'$ is a block hsop with top class $y_1 \cdots y_{\ell'} y_{\ell'+1}^3 \cdots y_m^3$.

**Theorem 3.9.** For $\lambda \in \mathbb{F}_2$ and $m > 3$, $\text{Tr}(y_1 \cdots y_{\ell'} y_{\ell'+1}^3 \cdots y_m^3)$ is indecomposable.

See subsection 3.11 for the proof of Theorem 3.9 Combining Theorem 3.9 with Theorem 2.10 gives the following.

**Corollary 3.10.** For $m > 3$, the Noether number for $V_{m,0}$ is $3m - 2[m/2]$ and the Hilbert ideal is generated by $\mathcal{H}'$.

Descriptions of $\mathbb{F}[V_{m,\lambda}]^G$ for $m \leq 3$ are given in subsection 3.14. The above formula for the Noether number is valid for $m > 1$.
Theorem 3.11. For $m > 2$,
\[ F[V_{m,0}]^G[x_1^{-1}] = F[x_1, \ldots, x_m, N_1, N_2, t_3, \ldots, t_m][x_1^{-1}] \]

Proof. We construct the field of fractions for an upper-triangular action as in [11] or [14]. From Remark 3.14.3, we see that $F[x_1, x_2, y_1, y_2]^G[x_1^{-1}] = F[x_1, x_2, N_1, \tilde{w}]^G[x_1^{-1}]$, where $\tilde{w} := (x_1 + x_2)u_1 + x_1 n_2$. Since $t_j \in F[x_1, \ldots, x_m, y_1, \ldots, y_j]^G$ has degree one as a polynomial in $y_j$ with coefficient $x_1^2$, we have
\[ F[V_{m,0}]^G[x_1^{-1}] = F[x_1, \ldots, x_m, N_1, \tilde{w}, t_3, \ldots, t_m][x_1^{-1}] \]

The result then follows from the relation $\tilde{w} = x_1 N_2 + t_3$. □

Remark 3.12. For $m > 2$ it follows from Theorem 3.11 and Theorem 3.8 that $F[V_{m,0}]^G$ is the normalisation of the algebra generated by $\mathcal{B}' := \mathcal{H}' \cup \{t_3, \ldots, t_m\}$. Furthermore, applying the SAGBI/Divide-by-Algorithm of [8] with $x = x_1$ to $\mathcal{B}'$ computes a SAGBI basis for $F[V_{m,0}]^G$.

Proposition 3.13. For $\lambda = 0$:
\[
\sqrt{\text{Tr} S} = \left( (x_1, \ldots, x_{m-1}) S \right)^G, \\
H^1(\langle \sigma_1 \rangle, \Delta_2 S) \cong \left( (x_1, \ldots, x_{m-1}) S \right)^G / \text{Tr} S, \\
H^1(\langle \sigma_2 \rangle, \Delta_1 S) \cong \left( (x_1, \ldots, x_m) S \right)^G / \text{Tr} S, \\
S^G / \langle (x_1, \ldots, x_m) S \rangle^G \cong F[N_1, \ldots, N_{r'}, N_G(y_{r'+1}), \ldots, N_G(y_m)].
\]

Proof. Direct calculation gives $\Delta_1 V_{m,0}^* = (\sigma_1 \sigma_2 + 1)V_{m,0}^* = \text{Span}_F \{x_1, \ldots, x_m\}$ and $\Delta_2 V_{m,0}^* = \text{Span}_F \{x_1, \ldots, x_{m-1}\}$. Using [13, Theorem 2.4],
\[ \sqrt{\text{Tr} S} = \bigcap_{g \in G, \|g\| = 2} \left( (g - 1)V_{m,0}^* \right)^G = ((x_1, \ldots, x_{m-1}) S)^G. \]

The rest of the proof is analogous to the proof of Proposition 3.7. □

3.14. Even dimensional examples.

Remark 3.14.1. It follows from [9, Theorem 3.75] that $F[V_{1,\lambda}]^G$ is the polynomial ring generated by $x_1$ and $N_G(y_1)$.

Define $w := \Delta_2(n_2)u_1 + x_1^2 n_2$. Note that $N_G(y_2) = n_2^2 + n_2 \Delta_2(n_2)$ and recall that $\Delta_2(n_2) = (\lambda^2 + \lambda)x_2^2 + x_1 x_2 + x_1^2$. A simple calculation shows that $\text{LT}(w) = (\lambda^2 + \lambda) y_1 x_2^2$. Subduction gives
\[
(3.1) \quad w^2 = \Delta_2(n_2)^2 x_2^2 N_1 + x_1^4 N_G(y_2) + w \Delta_2(n_2) \left( \Delta_2(n_2) + x_1^2 \right).
\]

Theorem 3.14.2. If $\lambda \notin F$, then $F[V_{2,\lambda}]^G$ is the hypersurface generated by $x_1$, $x_2$, $N_1$, $w$, and $N_G(y_2)$, subject to the above relation.

Proof. Since $N_2$ has degree 1 in $y_2$ with coefficient $(\lambda^2 + \lambda)x_1^2$, using [11, Theorem 2.4], we have $F[V_{2,\lambda}]^G[x_1^{-1}] = F[x_1, x_2, N_G(y_1), N_1][x_1^{-1}]$. Subduction gives
\[ N_G(y_1) = N_1^2 + (\lambda^3 + \lambda^2) x_2^2 N_1 + w + x_1^2 (w^2 + w) N_1. \]

Therefore $F[V_{2,\lambda}]^G[x_1^{-1}] = F[x_1, x_2, N_1, w][x_1^{-1}]$. Furthermore $\{x_1, x_2, N_1, N_G(y_2)\}$ is a block hsop. Taking $\mathcal{B} := \{x_1, x_2, N_1, w, N_G(y_2)\}$, we see that there is a single non-trivial tête-a-tête, which subducts to 0 using equation (3.1). Therefore, using [8, Theorem 1.1], $\mathcal{B}$ is a SAGBI basis for $F[V_{2,\lambda}]^G$.

It follows from Theorem 3.14.2 that the Noether number for $V_{2,\lambda}$ is 4 and the Hilbert ideal is generated by $\{x_1, x_2, N_1, N_G(y_2)\}$. □
Remark 3.14.3. A Magma [3] calculation shows that $F[V_{2,0}]^G$ is a hypersurface with generators $x_1, x_2, n_1, \tilde{w} := (x_1 + x_2)u_{12} + x_1n_2, \tilde{N}_2 := n_2^2 + n_2(x_1^2 + x_1x_2)$ and relation $\tilde{w}^2 + x_1^2(x_2 + x_1)^2n_1 + x_1x_2(x_1 + x_2)\tilde{w} = x_1^2\tilde{N}_2$. Therefore the Noether number for $V_{2,0}$ is 4 and the Hilbert ideal is generated by $x_1, x_2, n_1, \tilde{N}_2$. Using the relation to eliminate $\tilde{N}_2$ gives $F[V_{2,0}]^{G}[x_1^{-1}] = F[x_1, x_2, n_1, \tilde{w}][x_1^{-1}]$. Define $u_{123} := x_1(n_2 + u_{12} + u_{13}) + (\lambda^2 + \lambda)x_2u_{13}$. Simple calculations give LM$(u_{123}) = y_1x_2x_3$ and $\Delta_2(u_{123}) = 0$.

Theorem 3.14.4. If $\lambda \notin F_2$, then $F[V_{3,\lambda}]^{G}[x_1^{-1}] = F[x_1, x_2, x_3, N_1, u_{123}, t_3][x_1^{-1}]$.

Proof. From the proof of Theorem 3.14.2 $F[V_{2,\lambda}]^{G}[x_1^{-1}] = F[x_1, x_2, N_1, w][x_1^{-1}]$. Since $t_3$ is degree 1 in $y_3$ with coefficient $x_1^2$, using [4] Theorem 2.4, we have $F[V_{3,\lambda}]^{G}[x_1^{-1}] = F[x_1, x_2, x_3, N_1, w, t_3][x_1^{-1}]$. An explicit calculation gives $w = (\lambda^2 + \lambda)x_2t_3 + x_1u_{123} + x_1t_3$, and the result follows. 

With $c := \lambda^2 + \lambda$, define

$$n_{23} := (n_2 + u_{12} + u_{13}) (cx_3 + x_2 + x_1) + c(x_1n_3 + x_2u_{23} + cx_3u_{23}),$$

$$u_{133} := x_1^{-1}(cx_3t_3 + x_2u_{23}),$$

$$u_{233} := x_1^{-1}((cx_3 + x_2)n_{222} + n_{23}x_2^2 + x_2(u_{123} + t_3))$$

and $n_{222} = x_1^{-2}(t_3^2 + N_1(x_3^2 + x_2^2) + (c(x_3^2 + x_1x_2x_3) + x_1x_2^2))$.

A straightforward calculation gives $n_{23}, u_{133}, n_{222}, u_{233} \in F[V_{3,\lambda}]^G$ and LT$(n_{23}) = cy_2^2x_3, LT(u_{133}) = cy_3^2, LT(n_{222}) = y_2^2x_2, LT(u_{233}) = c^2y_2^3x_3$. Define $B_{3,\lambda} := \{x_1, x_2, x_3, N_1, t_3, u_{123}, u_{133}, n_{23}, n_{222}, u_{233}, N_G(y_2), N_G(y_3)\}$

$$\cup \{\text{Tr}(y_1y_2y_3^3), \text{Tr}(y_1y_2^2y_3), \text{Tr}(y_2^3y_3), \text{Tr}(y_1y_2y_3^3)\}.$$ 

Further calculation gives LT$(\text{Tr}(y_1y_2y_3^3)) = cy_2^2y_1x_3^3, LT(\text{Tr}(y_1y_2^2y_3)) = y_2^2y_1x_2^2, LT(\text{Tr}(y_2^3y_3)) = cy_3^2x_3^3, LT(\text{Tr}(y_1y_2y_3^3)) = cy_1y_2^2x_3^3$.

Remark 3.14.5. Suppose $\lambda \notin F_2$, i.e., $c \neq 0$. Applying the SAGBI/Divide-by-$x$ algorithm to $\{x_1, x_2, x_3, N_1, u_{123}, t_3, N_G(y_2), N_G(y_3)\}$ produces a SAGBI basis for $F[V_{3,\lambda}]^G$. A Magma calculation over the rational function field $F_2(\lambda)$ shows that for generic $\lambda$, $B_{3,\lambda}$ is a SAGBI basis for $F_2(\lambda)[V_{3,\lambda}]^G$. Since the lead coefficients of the elements of $B_{3,\lambda}$ lie in $\{1, c, c^2\}$, the calculations could have been performed over $F_2[\lambda, c^{-1}]$. Therefore $B_{3,\lambda}$ is a SAGBI basis for $F[V_{3,\lambda}]^G$, as long as $c \neq 0$. It follows from this that, for $\lambda \notin F_2$, the Hilbert ideal is generated by $x_1, x_2, x_3, N_1, N_G(y_2), N_G(y_3)$. Although a SAGBI basis need not be a minimal generating set, running a SAGBI basis test on $B_{3,\lambda} \setminus \{\text{Tr}(y_1y_2y_3^3)\}$ shows that $\text{Tr}(y_1y_2y_3^3)$ is indecomposable and hence the Noether number is 7.

Remark 3.14.6. A Magma calculation shows that $F[V_{3,0}]^G$ is generated by $\{x_1, x_2, x_3, n_1, n_2 + u_{13} + u_{12}, t_3, (x_3 + x_2)u_{13} + n_3x_1, N_G(y_3), \text{Tr}(y_2y_3^3), \text{Tr}(y_1y_2y_3^3)\}$. Furthermore, this is a SAGBI basis and Tr$(y_1y_2y_3^3)$ is indecomposable. Therefore the Hilbert ideal is generated by $\{x_1, x_2, x_3, n_1, n_2 + u_{13} + u_{12}, N_G(y_3)\}$ and the Noether number is 5.

The ring of invariants for the regular representation was computed in [10 Corollary 1.8] and [11 Lemma 5.2]. We include an alternate calculation here for completeness. Choose a basis $\{x, y_1, y_2, z^2\}$ for $V_{reg}^{*}$ so that $\Delta_i(z) = y_i$ and Tr$(z) = x$. Define $u := y_1y_2 + xz$ and $h := (u^2 + N_G(y_1)N_G(y_2))/x = y_1^2y_2 + y_2^2y_1 + x(z^2 + y_1y_2)$.
Theorem 3.14.7. \( F[V_{\text{reg}}]^G \) is the complete intersection generated by 
\[ N_G(y_1), N_G(y_2), h, N_G(z) \]
subject to the relations 
\[ u^2 = N_G(y_1)N_G(y_2) + xh \]
and 
\[ h^2 = N_G(y_1)^2N_G(y_2) + N_G(y_1)N_G(y_2)^2 + x(hN_G(y_1) + uh + hN_G(y_2) + xN_G(z)). \]

Proof. It follows from \[9, Theorem 3.75\] that \( F[x, y_1, y_2]^G \) is the polynomial ring generated by \( x, N_G(y_1) \) and \( N_G(y_2) \). Since \( u \) is degree 1 in \( z \) with coefficient \( x \), using \[4, Theorem 2.4\] we have \( F[V_{\text{reg}}]^G[x^{-1}] = F[x, N_G(y_1), N_G(y_2), u][x^{-1}] \). Using the graded reverse lexicographic order with \( z > y_1 > y_2 > x \), there are two non-trivial tete-a-tete situations among the elements of \( C \). These two tete-a-tetes subduct to zero using the given relations. Therefore \( C \) is a SAGBI basis for the subalgebra it generates. Since \( \{ x, N_G(y_1), N_G(y_2), N_G(z) \} \) is a block hso, applying \[8, Theorem 1.1\] shows that \( C \) is a SAGBI basis for \( F[V_{\text{reg}}]^G \). Since all relations come from subducting tete-a-tetes, the ring of invariants is the given complete intersection. \( \square \)

It follows from the above theorem that for \( V_{\text{reg}} \) the Noether number is 4 and the Hilbert ideal is generated by \( \{ x, u, N_G(y_1), N_G(y_2), N_G(z) \} \). We note that \( V_{\text{reg}} \) is the only indecomposable modular representation of \( G \) whose Hilbert ideal is not generated by a block hso.

3.15. The proof of Theorem 3.3. Suppose, by way of contradiction, that \( \text{Tr}(y_1 \cdots y_i y_{i+1} \cdots y_m) \) is decomposable. Working modulo the \( G \)-stable ideal \( (x_1, \ldots, x_{m-1})S \), it is easy to see that 
\[ \text{LT}(\text{Tr}(y_1 \cdots y_i y_{i+1} \cdots y_m)) = (\lambda^2 + \lambda) y_1 \cdots y_i y_{i+1} \cdots y_{m-1} x_m. \]
Thus there are two monomials of positive degree, say \( M_1 \) and \( M_2 \), such that \( M_1M_2 = y_1 \cdots y_i y_{i+1} \cdots y_{m-1} x_m \), and both \( M_1 \) and \( M_2 \) appear in \( G \)-invariant polynomials. We use the following results to rule out possible factorisations.

Lemma 3.15.1. Suppose \( f \in S^G \), \( M' \) is a monomial in \( y_1, \ldots, y_m \), and \( i > 1 \). If the degree of \( y_i \) in \( M' \) is even, then \( M'y_i x_m \) does not appear in \( f \). Further suppose \( j < m \). Then the degree of \( y_i \) in \( M' \) is even and \( M'y_i x_j \) appears in \( f \) if and only if the degree of \( y_j \) in \( M' \) is even and \( M'y_j x_{j-1} \) appears in \( f \).

Proof. We list the monomials in \( S \) that produce \( M'x_{i-1}x_j \) after applying \( \Delta_2 \):
1. \( M'y_i x_j \) if the degree of \( y_i \) in \( M' \) is even;
2. \( M'x_{i-1}y_j+1 \) if \( j < m \) and the degree of \( y_j+1 \) in \( M' \) is even;
3. \( M'x_{i-1}y_j \) if the degree of \( y_j \) in \( M' \) is even and \( \lambda \neq 0 \);
4. \( M'y_{i-1}x_j \) if the degree of \( y_{i-1} \) in \( M' \) is even and \( \lambda \neq 0 \);
5. \( M'y_{i-1}y_j \) if the degree of \( y_{i-1} \) and \( y_j \) in \( M' \) is even and \( \lambda \neq 0 \);
6. \( M'y_{i-1}y_{j+1} \) if \( j < m \) and the degree of \( y_{i-1} \) and \( y_{j+1} \) in \( M' \) is even and \( \lambda \neq 0 \);
7. \( M'y_i y_j+1 \) if \( j < m \) and the degree of \( y_i \) and \( y_{j+1} \) in \( M' \) is even;
8. \( M'y_i y_j \) if \( i \neq j \) and the degree of \( y_i \) and \( y_j \) in \( M' \) is even and \( \lambda \neq 0 \).
Note that the monomials in (5)–(8) do not appear in \( f \) by Lemma 1.3 because the degree of either \( y_i \) or \( y_{i-1} \) is odd. On the other hand, by Lemma 1.4, the monomials in (3) and (4) appear in \( f \) with the same coefficient (which is possibly zero). Call this coefficient \( \alpha \). Then the coefficient of \( M'x_{i-1}x_j \) in \( \Delta_2(\alpha M'x_{i-1}y_j+\alpha M'y_{i-1}x_j) \)
is $2\lambda \alpha = 0$. It follows that the monomial in (1) appears in $f$ if and only if the monomial in (2) appears in $f$.

**Proposition 3.15.2.** Let $M = \prod_{i \in I} y_i^2$ for some non-empty subset $I \subseteq \{1, \ldots, m\}$ and assume that $M$ appears in a polynomial $f \in S^G$. Let $j$ denote the maximum integer in $I$. Then $2j \leq m + 1$. Furthermore, if $\lambda \in F \setminus F_2$, then $2j \leq m$.

**Proof.** If $j = 1$, then $2j \leq m + 1$ implies $m \geq 1$ and $2j \leq m$ gives $m > 1$. For $m = 1$, we have $S^G = F[x_1, N_G(y)]$ and, if $\lambda \in F \setminus F_2$, then $LT(N_G(y_1)) = y_1^2$. Thus the assertion holds for $j = 1$.

Suppose $j > 1$ and assume that $M$ is maximal among all such monomials that appear in $f$. Let $M'$ denote the monomial $\prod_{i \in I \setminus \{j\}} y_i^2$. Using Lemma 3.15.1 (with $\sigma = \sigma_1$), we see that $M'x_jy_j$ appears in $f$. Since $j > 1$, by Lemma 3.15.1, $j < m$ and $M'x_{j-1}y_{j+1}$ appears in $f$. Applying Lemma 3.15.1 shows that $M'x_{j-1}y_{j-1}$ appears in $f$. If $j = 1$, then, again using Lemma 3.15.1, we have $j + 1 < m$ and $M'x_{j-2}y_{j+2}$ appears in $f$. In this case, by applying Lemma 3.15.1, we see that $M'x_{j-2}y_{j-2}$ appears in $f$. Continue alternating Lemma 3.15.1 and Lemma 1.4 until $j - k = 1$. This shows that $M'y_{j-k}x_{j+k} = M'y_1x_{j+1}$ appears in $f$. Thus $2j - 1 \leq m$, as required.

Suppose that $\lambda \in F \setminus F_2$. Note that $M'x_{j}^2$ appears in $\Delta_2(M + M'x_{j}y_{j})$ with coefficient $\lambda + \lambda^2 \neq 0$. Since $\Delta_2(f) = 0$, there must be other monomials in $f$ that produce $M'x_{j}^2$ after applying $\Delta_2$. The monomials $M'y_{j}y_{j+1}, M'x_{j}y_{j+1}$ and $M'y_{j+1}^2$ are the only such monomials. However, $M'y_{j}y_{j+1}$ does not appear in $f$ by Lemma 3.15.1, and the maximality of $j$ implies that $M'y_{j+1}^2$ does not appear in $f$ either. It follows that $M'x_{j}y_{j+1}$ appears in $f$. Applying Lemma 3.15.1 and Lemma 3.15.2 repeatedly we see that $M'x_{1}y_{2}$ appears in $f$. Hence $2j \leq m$.

Write $M_1 = y_1^{a_1} \cdots y_{m-1}^{a_{m-1}} x_m^{a_m}$ and $M_2 = y_1^{b_1} \cdots y_{m-1}^{b_{m-1}} x_m^{b_m}$, where $a_i$ and $b_i$ are non-negative integers. We have $a_i + b_i = 1$ for $i \leq \ell$ and $a_i + b_i = 3$ for $i > \ell$.

Suppose $a_m = 0$. Then, using Lemma 3.15.1 (with $\sigma = \sigma_1$), $a_i$ is even for all $i$. Thus $a_i = 0$ for $i \leq \ell$. Hence Proposition 3.15.2 applies, forcing $a_i = 0$ for $i > \ell \geq m/2$. Therefore, if $a_m = 0$, we have $M_1 = 1$ and the factorisation is trivial. Hence $a_m = 0$. Similarly, $b_m > 0$. Without loss of generality, we assume $a_m = 1$ and $b_m = 2$.

**Lemma 3.15.3.** If $m \geq 3$, then $a_{m-1}$ is even. If $m \geq 4$, then $a_{m-2}$ is even.

**Proof.** Both statements follow from Lemma 3.15.1.

**Lemma 3.15.4.** If $m \geq 3$, then $b_{m-1}$ and $b_{m-2}$ are not both odd.

**Proof.** Assume on the contrary that both $b_{m-1}$ and $b_{m-2}$ are odd and that $M_2$ appears in $f_2 \in S^G$. Define $M = y_1^{b_1} \cdots y_{m-3}^{b_{m-3}} y_{m-2}^{b_{m-2}-1} y_{m-1}^{b_{m-1}-1}$ so that $M_2 = M y_{m-2} y_{m-1} x_m^2$. Then $M x_{m-2} y_{m-1} x_m^2$ appears in $\Delta_1(M y_{m-2} y_{m-1} x_m^2)$. Since $\Delta_1(f_2) = 0$, there must be other monomials in $f_2$ that produce $M x_{m-2} y_{m-1} x_m^2$ after applying $\Delta_1$. The only monomials with this property are $M y_{m-2} y_{m-1} x_m^2, M y_{m-2} y_{m-1} y_m^2, M y_{m-2} y_{m-1} x_m y_m, M y_{m-2} y_{m-1} y_m^2$ and $M x_{m-2} y_{m-1} x_m y_m$. However $M y_{m-2} y_{m-1} y_m^2$ does not appear in $f_2$ by Lemma 3.15.1 because the degree of $y_{m-1}$ in this monomial is odd. Also, $M y_{m-2} y_{m-1} x_m y_m$ does not appear in $f_2$ by Lemma 3.15.1. If $M x_{m-2} y_{m-1} y_m^2$ appears in $f_2$, then, since the degree of $y_{m-2}$ in this monomial is odd, $M x_{m-2} y_{m-1} y_m^2$ appears in $\Delta_2(M x_{m-2} y_{m-1} y_m^2)$. So there must be another monomial in $f_2$ that produces $M x_{m-2} y_{m-1} y_m^2$ after applying $\Delta_2$. The only monomials in $S$ with this property are $M y_{m-2} y_{m-1} y_m^2$ if $b_{m-1} = 1, M y_{m-2} y_{m-1} y_m^2$ if $b_{m-2} = 1,
Lemma 3.15.3, appears in Proposition 3.15.2. On the other hand \( Mx_{m-2}y_{m} \) does not appear in \( f_{2} \) if \( b_{m-2} = 3 \) by Lemma 3.15.1. If \( b_{m-2} = 1 \), then \( Mx_{m-2}y_{m} \) appears in \( f_{2} \) if and only if \( M_{y_{m}}y_{m} \) appears in \( f_{2} \). However the latter monomial does not appear in \( f_{2} \) by Lemma 1.3 and Proposition 3.15.2. Therefore \( Mx_{m-2}y_{m} \) does not appear in \( f_{2} \).

We finish the proof by showing that \( Mx_{m-2}y_{m} \) does not appear in \( f_{2} \). Note that \( Mx_{m-2}y_{m} \) appears in \( \Delta_{2}(Mx_{m-2}y_{m}) \). The other monomials that produce \( Mx_{m-2}y_{m} \) after applying \( \Delta_{2} \) are \( M_{y_{m}}y_{m} \) if \( b_{m-1} = 1 \), \( M_{y_{m}}y_{m} \) if \( b_{m-2} = 1 \), \( M_{y_{m}}y_{m} \) and \( Mx_{m-2}y_{m} \). The first two monomials appear in \( f_{2} \) if and only if \( M_{y_{m}}y_{m} \) and \( M_{y_{m}}y_{m} \) appear in \( f_{2} \), respectively, by Lemma 1.5. However neither of the latter monomials appear in \( f_{2} \) by Lemma 3.15.1 and Proposition 3.15.2. The third monomial does not appear in \( f_{2} \) by Lemma 3.15.1. Finally, \( Mx_{m-2}y_{m} \) appears in \( f_{2} \) if and only if \( M_{y_{m}}y_{m} \) appears in \( f_{2} \) because these are the only monomials in \( S \) that produce \( Mx_{m-2}y_{m} \) after applying \( \Delta_{1} \). However \( M_{y_{m}}y_{m} \) appears in \( f_{2} \) if and only if \( M_{y_{m}}y_{m} \) appears in \( f_{2} \) by Lemma 1.5 and the latter monomial does not appear in \( f_{2} \) by Proposition 3.15.2.

Returning to the proof of Theorem 3.3, first assume that \( m \geq 4 \). Then by Lemma 3.15.3 \( a_{m-2} \) and \( a_{m-1} \) are both even. Therefore \( b_{m-2} \) and \( b_{m-1} \) are both odd, contradicting Lemma 3.15.3.

Suppose \( m = 3 \) and \( M_{1} \) appears in \( f_{1} \in S^{G} \). By Lemma 3.15.3 \( a_{2} \) is even. Thus \( b_{2} \) is odd and, by Lemma 3.15.1 \( b_{1} \) is even. Therefore \( b_{1} = 0 \), \( a_{1} = 1 \) and \( M_{1} = y_{1}y_{2}^{a_{2}}x_{3} \). By Lemma 1.4 \( x_{1}y_{2}^{a_{2}}y_{3} \) also appears in \( f_{1} \). Thus \( y_{2}^{a_{2}+1}x_{2} \) appears in \( f_{1} \) as well by Lemma 3.15.1. This contradicts Lemma 1.5 if \( a_{2} = 2 \) and Proposition 3.15.2 if \( a_{2} = 0 \).

3.16. The proof of Theorem 3.9 Suppose, by way of contradiction, that \( \text{Tr}(y_{1} \cdots y_{i} y_{i+1}^{3} \cdots y_{m}^{3}) \) is decomposable. Working modulo the \( G \)-stable ideal \((x_{1}, \ldots, x_{m-2}, x_{m-1})S \), a straightforward calculation gives

\[
\text{LT}(\text{Tr}(y_{1} \cdots y_{i} y_{i+1}^{3} \cdots y_{m}^{3})) = y_{1} \cdots y_{i} y_{i+1}^{3} \cdots y_{m-1} x_{m-1}^{2}.
\]

Thus there are two monomials of positive degree, say \( M_{1} \) and \( M_{2} \), such that \( M_{1}M_{2} = y_{1} \cdots y_{i} y_{i+1}^{3} \cdots y_{m-1} x_{m-1}^{2} \), and both \( M_{1} \) and \( M_{2} \) appear in \( G \)-invariant polynomials, say \( f_{1} \) and \( f_{2} \). Without loss of generality, we may assume \( M_{1} = y_{1}^{a_{1}} \cdots y_{m-1}^{a_{m-1}} x_{m-1} \) and \( M_{2} = y_{1}^{b_{1}} \cdots y_{m-1}^{b_{m-1}} x_{m-1} \). It follows from Lemma 1.3 and Proposition 3.15.2 that \( b_{m} > 0 \).

Lemma 3.16.1. If \( m > i > 1 \), then \( b_{i} \) is even and \( a_{i} \) is odd.

Proof. Note that \( V_{m,0}^{1} \) and \((m-1)V_{2} \oplus V_{1} \) are isomorphic \( \sigma_{2} \)-modules, where the two copies of \( V_{1} \) are generated by \( x_{m} \) and \( y_{1} \) and where each pair \( x_{i-1}, y_{i} \) for \( 2 \leq i \leq m \) generate a copy of \( V_{2} \). Therefore we have \( S^{\sigma_{2}} \cong F[x_{1}, \ldots, x_{m-1}, y_{2}, \ldots, y_{m}]^{\sigma_{2}} \otimes F[x_{m}, y_{1}] \). Hence the fact that \( b_{i} \) is even follows from Lemma 1.3 (with \( \sigma = \sigma_{2} \)). Since \( b_{i} \) is even and \( a_{i} + b_{i} \) is odd, \( a_{i} \) is odd.

We have \( b_{m} > 0 \) and \( a_{m} + b_{m} = 2 \). Therefore, there are two cases, \( a_{m} = 0 \) and \( a_{m} = 1 \). First assume that \( a_{m} = 0 \). If \( a_{m-1} = 3 \), then \( M_{1} \) does not appear in \( f_{1} \) by Lemma 1.5. On the other hand, if \( a_{m-1} = 1 \), then by Lemma 1.5 \( y_{1}^{a_{1}} \cdots y_{m-1}^{a_{m-1}+1} \) appears in \( f_{1} \), contradicting Lemma 1.3 because \( a_{m-2} \) is odd.
Suppose that \( a_m = 1 \). Set \( M = y_1^{a_1} \cdots y_{m-1}^{a_{m-1}} \) so that \( M_1 = My_{m-1}x_{m-1}x_m \). Then \( Mx_m - 2x_{m-1}x_m \) appears in \( \Delta_2(M_1) \). The only other monomials in \( S \) that produce \( Mx_m - 2x_{m-1}x_m \) after applying \( \Delta_2 \) are \( My_{m-2}x_m \) and \( Mx_m - 2y_{m-1}x_m \). However by Lemma 4.3 \( My_{m-2}x_m \) appears in \( f_1 \) if and only if \( My_{m-2}y_m^2 \) does, but the latter monomial does not appear in \( f_1 \) by Lemma 4.3 and Proposition 3.15.2. Finally, if \( Mx_m - 2y_{m-1}x_m \) appears in \( f_1 \), there must be another monomial in \( f_1 \) that produces \( Mx_m - 2x_m^2 \) after applying \( \Delta_1 \). Since \( a_{m-2} = 3 \), odd, \( Mx_m - 2y_m^2 \) is the only such monomial. However if \( a_{m-2} = 3 \), then \( Mx_m - 2y_m^2 \) does not appear in \( f_1 \). If \( a_{m-2} = 1 \), then again by Lemma 4.3 \( My_{m-2}y_m^2 \) also appears in \( f_1 \), contradicting Proposition 3.15.2.

### 4. The Easy Odd Case

In this section we consider the odd dimensional representations \( \Omega^{-m}(F) \). The action of \( G \) on \( S := F[\Omega^{-m}(F)] = F[x_1, \ldots, x_m, y_1, \ldots, y_{m+1}] \) is given by \( \sigma_i(x_j) = x_j, \sigma_j(y_j) = y_j + x_j - 1 \), using the convention that \( x_0 = 0 \) and \( x_{m+1} = 0 \). As in section 3 define \( n_i := y_i^2 + x_iy_i \) and \( u_{ij} = x_iy_j + x_jy_i \). Then \( n_i, u_{ij} \in S^{G} \). A simple calculation gives \( \Delta_2(u_{ij}) = x_{i+1}x_{j+1}x_{i+1}x_{j+1} \). For \( i \in \{1, \ldots, m + 1\} \) define

\[
N_i := n_i + \sum_{j=1}^{i-1} (u_{i-j, i+j} + u_{i-j, i+j+1})
\]

so that \( N_1 = n_1 \) and \( N_2 = n_2 + u_{12} + u_{13} \). An explicit calculation, exploiting the fact that \( \Delta_2(u_{ij}) = x_{i+1}x_{j+1} \), gives \( \Delta_2(N_i) = 0 \). Therefore \( N_i \in S^{G} \). Define \( H_{-m} := \{ x_1, \ldots, x_m, N_1, \ldots, N_{m+1} \} \). Since \( LM(N_i) = y_i^2 \), \( H_{-m} \) is a block hop with top class \( y_1 \cdots y_{m+1} \), and the image of the transfer is generated by \( \text{Tr}(\beta) \) for \( \beta \) dividing \( y_1 \cdots y_{m+1} \).

**Theorem 4.1.** For \( m > 3 \), \( \text{Tr}(y_1 \cdots y_{m+1}) \) is indecomposable.

See subsection 4.8 for the proof of Theorem 4.1. Combining Theorem 4.1 with Theorem 2.1 gives the following.

**Corollary 4.2.** If \( m > 3 \), then the Noether number for \( \Omega^{-m}(F) \) is \( m + 1 \) and the Hilbert ideal is generated by \( H_{-m} \).

Remarks 4.3 and 4.6 show that the above formula for the Noether number is valid for \( m \geq 1 \).

As in section 3 define \( t_j := u_{12}x_{j-1} + u_{1j}x_1 \).

**Theorem 4.3.** For \( m > 2 \),

\[
F[\Omega^{-m}(F)]^{G}[x_1^{-1}] = F[x_1, \ldots, x_m, N_1, N_2, t_3, \ldots, t_{m+1}][x_1^{-1}].
\]

**Proof.** We construct the field of fractions for an upper-triangular action as in 4 or 14. The restriction of the action of \( G \) to the span of \( \{ x_1, x_2, y_1, y_2 \} \) is \( V_{2,0}^* \). Therefore, using Remark 3.14.3, \( F[x_1, x_2, y_1, y_2]^{G}[x_1^{-1}] = F[x_1, x_2, n_1, \bar{w}]^{G}[x_1^{-1}] \). Since \( t_j \in F[x_1, \ldots, x_m, y_1, \ldots, y_j]^{G} \) has degree one as a polynomial in \( y_j \) with coefficient \( x_j^2 \), we have \( F[\Omega^{-m}(F)]^{G}[x_1^{-1}] = F[x_1, \ldots, x_m, n_1, \bar{w}, t_3, \ldots, t_{m+1}][x_1^{-1}] \). The result then follows from the fact that \( \bar{w} = x_1N_2 + t_3 \) and \( N_1 = n_1 \). \( \square \)
Assume on the contrary that \( f \neq 0 \) is a \( \mathbb{F} \)-linear combination of \( D_1, D_2, D_3 \) with \( \beta_1 \neq 0 \) or \( \beta_2 \neq 0 \).

Remark 4.4. It is easy to see that \( \mathbf{F}[\Omega^{-1}(\mathbf{F})]^G = \mathbf{F}[x_1, n_1, y_2^2 + x_1 y_3] \). A Magma calculation shows that \( \mathbf{F}[\Omega^{-2}(\mathbf{F})]^G \) is the hypersurface with generators \( x_1, x_2, N_1, N_2, N_3, t_3 \) and relation \( t_3^2 + x_1^2 N_1 + x_1 x_2 (x_1 + x_2) t_3 + x_1^2 x_2^2 N_2 = x_1^3 N_3 \). Therefore, the Noether number for this representation is \( m + 1 = 3 \).

Remark 4.5. It follows from Theorem 4.3 that applying the SAGBI/Divide-by-\( x \) algorithm of \([8]\) with \( x = x_1 \) to
\[
\{ x_1, \ldots, x_m, N_1, N_2, \ldots, N_{m+1}, t_3, \ldots, t_{m+1} \}
\]
produces a SAGBI basis for \( \mathbf{F}[\Omega^{-m}(\mathbf{F})]^G \).

Remark 4.6. A Magma calculation shows that \( \mathbf{F}[\Omega^{-3}(\mathbf{F})]^G \) is generated by
\[
\{ x_1, x_2, x_3, n_1, N_2, N_3, n_4, t_4, u_{233}, u_{133}, \text{Tr}(y_1 y_2 y_3 y_4) \},
\]
where \( u_{133} := x_3 u_{13} + x_1 u_{24} \) and \( u_{233} := x_3 u_{23} + x_2 u_{24} + x_3 u_{14} \). Furthermore, this set is a SAGBI basis, and running a SAGBI test with \( \text{Tr}(y_1 y_2 y_3 y_4) \) omitted shows that \( \text{Tr}(y_1 y_2 y_3 y_4) \) is indecomposable. Therefore the Noether number for this representation is \( m + 1 = 4 \) and the Hilbert ideal is generated by the block hsp \( x_1, x_2, x_3, n_1, N_2, N_3, n_4 \). From \([10]\), we know \( \text{depth}(\mathbf{F}[\Omega^{-3}(\mathbf{F})]^G) = 6 \). The relation \( x_2 t_4 + x_3 t_3 + x_1 u_{133} = 0 \) shows that the partial hsp \( \{ x_1, x_2, x_3 \} \) is not a regular sequence, giving an alternate proof of the fact that the ring is not Cohen-Macaulay.

**Proposition 4.7.** For \( S = \mathbf{F}[\Omega^{-m}] \), \( \langle \Delta_2 S \rangle_{\sigma_1} = \langle \Delta_1 S \rangle_{\sigma_2} = \langle (x_1, \ldots, x_m) S \rangle^G = \sqrt{\text{Tr} S} \) and
\[
\sqrt{\text{Tr} S} / \text{Tr} S \cong H^1(\langle \sigma_2 \rangle, \Delta_1 S) = H^1(\langle \sigma_1 \rangle, \Delta_2 S).
\]
Furthermore \( S^G / \sqrt{\text{Tr} S} \cong \mathbf{F}[N_1, \ldots, N_m] \).

**Proof.** The proof is analogous to the proof of Proposition 3.7 (Note that LT(\( N_i \)) = \( y_i^2 \) and so an analogue of Proposition 3.15.2 is unnecessary.) \( \square \)

4.8. **Proof of Theorem 4.1** Suppose by way of contradiction that \( \text{Tr}(y_1 \cdots y_{m+1}) \) is decomposable. Working modulo the \( G \)-stable ideal \( \langle x_1, \ldots, x_{m-1} \rangle S \), it is easy to see that
\[
\text{LT}(\text{Tr}(y_1 \cdots y_{m+1})) = y_1 \cdots y_{m-1} x_m^2.
\]
Thus there are two monomials, say \( M_1 \) and \( M_2 \), such that \( M_1 M_2 = y_1 \cdots y_{m-1} x_m^2 \), \( \text{deg}(M_2) \leq \text{deg}(M_1) < m + 1 \) and both \( M_1 \) and \( M_2 \) appear in \( G \)-invariant polynomials. Since a \( G \)-invariant is also a \( \sigma_i \)-invariant, it follows from Lemma 1.3 that both \( M_1 \) and \( M_2 \) are divisible by \( x_m \). Since \( m + 1 \geq 5 \), we have \( \text{deg}(M_1) \geq 3 \). The required contradiction is then a consequence of the following lemma.

**Lemma 4.8.1.** Let \( M = \langle \prod_{j \in J} y_j \rangle x_k \) for some \( k \leq m \) and set \( J \subseteq \{1, \ldots, k-1\} \) with \( |J| > 1 \). Then \( M \) does not appear with a non-zero coefficient in a \( G \)-invariant polynomial.

**Proof.** Let \( d \) denote the maximum integer in \( J \). We proceed by induction on \( k - d \). Assume on the contrary that \( M \) appears in a \( G \)-invariant polynomial \( f \). Set \( M' = \prod_{j \in J, j \neq d} y_j \). Then we have \( M = M' y_d x_k \). From Lemma 1.4 we get that \( M' x_d y_k \) also appears in \( f \). Furthermore, since \( M' x_d x_{k-1} \) appears in \( \Delta_2(M' x_d y_k) \), there must be another monomial in \( f \) that produces \( M' x_d x_{k-1} \) after applying \( \Delta_2 \). If \( k - d = 1 \), then the only other monomial that produces \( M' x_d x_{k-1} = M' x_k^2 \) after applying \( \Delta_2 \) is \( M' y_k^2 \). However, this monomial cannot appear in \( f \) by Lemma 1.3. This establishes the basis case for the induction. If \( k - d > 1 \), the only monomials...
(other than $M'x_d y_k$) that produce $M'x_d x_{k-1}$ after applying $\Delta_2$ are $M'y_{d+1}y_k$ and $M'y_{d+1}x_{k-1}$. Again by Lemma 1.3, $M'y_{d+1}y_k$ cannot appear in $f$. Moreover, if $d + 1 < k - 1$, then $M'y_{d+1}x_{k-1}$ does not appear in $f$ by induction. On the other hand, if $d + 1 = k - 1$, then $M'y_{d+1}x_{k-1}$ does not appear in $f$ by Lemma 1.3. 

5. THE HARD ODD CASE

In this section we consider the odd dimensional representations $\Omega^m(F)$. The action of $G$ on $S := F[\Omega^m(F)] = F[x_1, \ldots, x_{m+1}, y_1, \ldots, y_m]$ is given by $\sigma_i(x_j) = x_j$, $\sigma_i(y_j) = y_j + x_j$ and $\sigma_2(y_j) = y_j + x_{j+1}$.

Define

$$\mathcal{H}_m := \{x_1, \ldots, x_{m+1}, N_G(y_1), \ldots, N_G(y_m)\}.$$ 

Since $\text{LM}(N_G(y_i)) = y_i^3$, $\mathcal{H}_m$ is a block isop with top class $(y_1 \ldots y_m)^3$ and the image of the transfer is generated by $\text{Tr}(\beta)$ for $\beta$ dividing $(y_1 \ldots y_m)^3$.

**Theorem 5.1.** For $m > 2$, $\text{Tr}(y_1^3 \ldots y_m^3)$ is indecomposable.

See subsection 5.8 for the proof of Theorem 5.1. Combining Theorem 5.1 with Theorem 2.1 gives the following.

**Corollary 5.2.** If $m > 2$, then the Noether number for $\Omega^m(F)$ is $3m$ and the Hilbert ideal is generated by $\mathcal{H}_m$.

From Remark 5.4, the Noether number for $\Omega^2(F)$ is 6.

For $j > 1$, define $v_j := u_{1j}(x_2^2 + x_1x_2) + n_1(x_1x_2 + x_1x_{j+1})$.

**Theorem 5.3.** For $m > 1$,

$$F[\Omega^m(G)] = F[x_1, \ldots, x_{m+1}, N_G(y_1), v_2, \ldots, v_m]((x_1x_2 + x_1x_2)^{-1}).$$

**Proof.** We use [4] Theorem 2.4. $F[x_1, \ldots, x_n, y_1]G$ is the polynomial algebra generated by $\{x_1, \ldots, x_n, N_G(y_1)\}$. The invariant $v_j \in F[x_1, x_2, x_3]$ has degree one as a polynomial in $y_j$ and the coefficient of $y_j$ is $x_1x_2(x_1 + x_2)$. 

It is easy to see that $F[\Omega^2(F)]G = F[x_1, x_2, N_G(y_1)]$, and, therefore, the Noether number is 4.

**Remark 5.4.** A Magma calculation shows that $F[\Omega^2(F)]G$ is generated by

$$B_2 := \{x_1, x_2, x_3, N_G(y_1), N_G(y_2), v_2, n_{13}, u_{1233}, \text{Tr}(y_1^2y_2^2)\},$$

where $n_{13} = x_3n_1 + x_3u_{12} + x_1n_2$ and $u_{1233} = (x_3^2 + x_2x_3)u_{12} + (x_2^2 + x_1x_3)n_2$. Therefore the Hilbert ideal for $\Omega^2(F)$ is generated by $x_1, x_2, x_3, N_G(y_1), N_G(y_2)$. In fact, $B_2$ is a SAGBI basis using grevlex with $y_2 > y_1 > x_3 > x_2 > x_1$. Although a SAGBI basis need not be a minimal generating set, running a SAGBI basis test on $B_2 \setminus \{\text{Tr}(y_1^2y_2^2)\}$ shows that $\text{Tr}(y_1^2y_2^2)$ is indecomposable and hence the Noether number is 6. From [10], we know depth$(F[\Omega^2(F)]G) = 4$. The relation $x_3x_2 + (x_2^2 + x_1x_3)n_{13} + x_1u_{1233} = 0$ shows that the partial isop $\{x_1, x_2, x_3\}$ is not a regular sequence, giving an alternate proof of the fact that the ring is not Cohen-Macaulay.

**Remark 5.5.** We have been unable to find “polynomial generators” for the ring $F[\Omega^m(F)]G[x_1^{-1}]$. We note that $x_1$ is not in the radical of the image of the transfer for these representations but that $x_1x_2(x_1 + x_2)$ is. Furthermore, $x_1$ is in the radical of the image of the transfer for $\Omega^{-m}(F)$ and $V_{m, \lambda}$. Hence $F[\Omega^{-m}]G[x_1^{-1}]$ and $F[V_{m, \lambda}]G[x_1^{-1}]$ are “trace-surjective” in the sense of [13].
Proposition 5.6. For $S = \mathbf{F}[\Omega^m(\mathbf{F})]$ and $m \geq 3$,
\[
\sqrt{\text{Tr}} S = ((x_2 x_{m+1} + x_2 x_1, x_1 x_{m+1} + x_1 x_2, x_2^2 + x_2 x_2, x_3^2 + x_2 x_3, \ldots, x_m + x_2, S)^G).
\]

Proof. Direct calculation gives $\Delta_1(\Omega^m(\mathbf{F})^*) = \text{Span}_\mathbf{F}\{x_1, \ldots, x_m\}$, $\Delta_2(\Omega^m(\mathbf{F})^*) = \text{Span}_\mathbf{F}\{x_2, \ldots, x_{m+1}\}$, and $(\sigma_1 \sigma_2 + 1)(\Omega^m(\mathbf{F})^*) = \text{Span}_\mathbf{F}\{x_1 + x_2, \ldots, x_m + x_{m+1}\}$.

Using [18, Theorem 2.4] and computing intersections of ideals gives
\[
\sqrt{\text{Tr}} S = \bigcap_{g \in G, |g| = 2} (\{(g - 1)(\Omega^m(\mathbf{F})^*)S\})^G = \{(x_2 x_{m+1} + x_2 x_1, x_1 x_{m+1} + x_1 x_2, x_2^2 + x_2 x_1, x_3^2 + x_2 x_3, \ldots, x_m + x_2, S)^G\).
\]

Remark 5.7. The above shows that for $m \geq 3$, we have $x_2 + x_3 \in \sqrt{\text{Tr}} S$. In fact, for
\[
\alpha := (x_1 + x_2 + x_3)y_2 y_3 + (x_2 + x_2 + x_3 + x_4)y_1 y_3 + (x_2 + x_2 + x_3 + x_4)y_1 y_2 + y_1^2 y_3 + y_1 y_3^2,
\]

\[
\text{Tr}(\alpha) = (x_2 + x_3)^3.
\]

Define $x := x_2 + x_3$ and use the variables $x < x_1 < x_3 < x_4 < \cdots < x_{m+1} < y_1 < \cdots < y_m$ with the grevlex order. Define $\rho : \mathbf{F}[\Omega^m(\mathbf{F})][x^{-1}] \to \mathbf{F}[\Omega^m(\mathbf{F})]^G[x^{-1}]$ by $\rho(f) = x^{-3}\text{Tr}(f\alpha)$. Then $\rho$ restricts to the identity on $\mathbf{F}[\Omega^m(\mathbf{F})]^G$ and $\mathbf{F}[\Omega^m(\mathbf{F})]^G[x^{-1}]$ is “trace-surjective”. Define
\[
B_m := H_m \cup \{\text{Tr}(\beta) | \beta \text{ divides } (y_1 \cdots y_m)^3\}.
\]

Since $\{\beta \mid \beta \text{ divides } (y_1 \cdots y_m)^3\}$ generates $\mathbf{F}[\Omega^m(\mathbf{F})][x^{-1}]$ as a module over the ring $\mathbf{F}[H_m][x^{-1}]$ and $\rho$ is surjective, we see that $B_m \cup \{x^{-1}\}$ generates $\mathbf{F}[\Omega^m(\mathbf{F})]^G[x^{-1}]$. Thus, since $H_m$ is an hsodp, applying the SAGBI/Divide-by-$x$ algorithm to $B_m$ produces a generating set, in fact a SAGBI basis, for $\mathbf{F}[\Omega^m(\mathbf{F})]^G$.

5.8. Proof of Theorem 5.1

Suppose, by way of contradiction, that $\text{Tr}(y_1^3 \cdots y_m^3)$ is decomposable. Working modulo the $G$-stable ideal $(x_1, \ldots, x_{m-1})S$, it is not difficult to see that
\[
\text{LT}(\text{Tr}(y_1^3 \cdots y_m^3)) = y_1^3 \cdots y_{m-1}^3 x_{m+1}^2 x_m^2.
\]

Write $y_1^3 \cdots y_{m-1}^3 x_m^2 x_{m+1}^2 = M_1 M_2$, where $M_1$ and $M_2$ are monomials of positive degree which appear in $G$-invariant polynomials. We use the following results to eliminate possible factorisations.

Lemma 5.8.1. Suppose $1 \leq i \leq m$, $2 \leq k \leq m + 1$, $k \neq i + 1$ and $M$ is a monomial in $y_1, \ldots, y_m$. Further suppose that the degree of $y_i$ in $M$ is even and $y_i x_k M$ appears in a $G$-invariant polynomial $f$. Then the degree of $y_{k-1}$ in $M$ is even and $x_{i+1} y_{k-1} M$ appears in $f$.

Proof. Since the degree of $y_i$ in $M$ is even, $x_{i+1} x_k M$ appears in $\Delta_2(y_i x_k M)$. Since $\Delta_2(f) = 0$, $f$ must contain another monomial that produces $x_{i+1} x_k M$ after applying $\Delta_2$. If the degree of $y_{k-1}$ in $M$ is odd, then there is no such monomial. Thus the degree of $y_{k-1}$ in $M$ is even and applying $\Delta_2$ to either $y_i y_{k-1} M$ or $x_{i+1} y_{k-1} M$ produces $x_{i+1} x_k M$. However, by Lemma 1.3, $y_i y_{k-1} M$ does not appear in $f$. Thus $x_{i+1} y_{k-1} M$ appears in $f$. \hfill \square

Proposition 5.8.2. Suppose $M = y_1^e \cdots y_m^e$. If $k$ is a positive integer and $M x_k^k$ or $M x_{m+1}^k$ appears in a $G$-invariant polynomial, then $e_j$ is even for $1 \leq j \leq m$. \hfill \square
Proof. Note that $S'^{σ_1} \cong F[x_i, y_i \mid i \leq m]^{σ_1} \otimes F[x_{m+1}]$ and $S'^{σ_2} \cong F[x_i, y_i \mid i \leq m]^{σ_2} \otimes F[x_{1}]$. If $Mx_{m+1}^k$ appears in a $G$-invariant polynomial, then $M$ appears in a $σ_1$-invariant polynomial, and the result follows from applying Lemma 1.3 with $σ = σ_1$. If $Mx_{1}^k$ appears in a $G$-invariant polynomial, then $M$ appears in a $σ_2$-invariant polynomial, and the result follows from applying Lemma 1.3 with $σ = σ_2$. □

Proposition 5.8.3. Suppose $M = \prod_{j \in J} y_j^2$ for a non-empty index set $J \subseteq \{1, \ldots, m\}$. Then $M$ does not appear in a $G$-invariant polynomial.

Proof. Suppose, by way of contradiction, that $M$ appears in a $G$-invariant polynomial $f$. Let $ℓ$ denote the largest integer in $J$ and set $M' = M/y_ℓ^2$. Note that $M'x_ℓ^{2}+1$ appears in $Δ_2(M)$, and since $Δ_2(f) = 0$, there must be another monomial in $f$ that produces $M'y_ℓx_{ℓ+1}$ after applying $Δ_2$. The only other monomial in $S$ with this property is $M'y_ℓx_{ℓ+1}$. Therefore, this monomial also appears in $f$. If $ℓ = m$, then the degree of $y_m$ in $M'y_ℓx_{ℓ+1} = M'y_mx_{m+1}$ is odd, and we have a contradiction by Proposition 5.8.2. Otherwise, using Lemma 1.4, $M'y_ℓx_{ℓ+1}$ appears in $f$. If $ℓ = 1$, this also gives a contradiction using Proposition 5.8.2. Otherwise, we apply Lemma 5.8.1 and conclude that $M'y_{ℓ−1}x_{ℓ+2}$ appears in $f$. This gives a contradiction if $ℓ + 1 = m$. Continuing in this fashion, the process terminates with either $M'y_{2ℓ−m}x_{m+1}$ or $M'y_{2ℓ}x_1$ appearing in $f$, again contradicting Proposition 5.8.2.

Returning to the proof of Theorem 5.1, first suppose that $M_1$ is a factor of $y_1^3 \cdots y_{m−1}^3$. Since $M_1$ appears in a $σ_1$-invariant, we have from Lemma 1.3 that the degree of each $y_i$ in $M_1$ is even. However, since these degrees are at most two, we get a contradiction using Proposition 5.8.3. Similarly, $M_2$ is a not factor of $y_1^3 \cdots y_{m−1}^3$. Therefore we may assume $x_m$ divides $M_1$ and $x_{m+1}$ divides $M_2$. By Proposition 5.8.2 the degrees of the variables $y_1, \ldots, y_{m−1}$ in $M_2$ are even. Hence the degrees of these variables in $M_1$ are odd. Therefore we have either $M_1 = y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_m$ or $M_1 = y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_mx_{m+1}$, where $a_1, \ldots, a_{m−1}$ are odd. Let $f$ denote the $G$-invariant polynomial in which $M_1$ appears. Suppose that $M_1 = y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_m$. Since $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_m^{2}M_2$ appears in $Δ_2(M_1)$ and $Δ_2(f) = 0$, there must be another monomial in $f$ that produces $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_m^{2}M_2$ after applying $Δ_2$. However, $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_m^{2}$ is the only other monomial in $S$ with this property. Since $f$ is also $σ_1$-invariant and $a_1$ is odd, we get a contradiction by Lemma 1.3. Therefore, we may assume that $M_1 = y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_mx_{m+1}$. Then $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_m^{2}M_2$ appears in $Δ_2(M_1)$. Since $Δ_2(f) = 0$, there must be another monomial in $f$ that produces $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_m^{2}M_2$ after applying $Δ_2$. The monomials in $S$ with this property are $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_my_m$, $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_{m+1}$. The first two monomials do not appear in $f$ by Lemma 1.3 because the degree of $y_1$ is odd. For the same reason the third monomial does not appear in $f$ by Proposition 5.8.2. Finally, if $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_m^{2}M_2$ appears in $f$, then there must be another monomial in $f$ that produces $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}x_{m+1}$ after applying $Δ_1$. However, $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}y_m$ and $y_1^{a_1} \cdots y_{m−1}^{a_{m−1}}y_m$ are the only monomials in $S$ with this property. Since neither of these monomials can appear in $f$, by Lemma 1.3 and Proposition 5.8.2 respectively, we have ruled out all possible factorisations, proving Theorem 5.1.
ACKNOWLEDGEMENTS

The authors thank the reviewer for comments that improved the exposition.

REFERENCES

[1] Alejandro Adem and R. James Milgram, Cohomology of finite groups, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 309, Springer-Verlag, Berlin, 1994. MR1317096 (96f:20082)

[2] D. J. Benson, Representations and cohomology. I. Basic representation theory of finite groups and associative algebras. Cambridge Studies in Advanced Mathematics, vol. 30, Cambridge University Press, Cambridge, 1991. MR1105811 (92m:20005)

[3] Web Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). J. Symbolic Comput. 24 (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. MR1484478

[4] H. E. A. Campbell and J. Chuai, Invariant fields and localized invariant rings of \( p \)-groups, Q. J. Math. 58 (2007), no. 2, 151–157, DOI 10.1093/qmath/ham011. MR2334559 (2008f:13007)

[5] H. E. A. Campbell and I. P. Hughes, Vector invariants of \( U_2(F_p) \): a proof of a conjecture of Richman, Adv. Math. 126 (1997), no. 1, 1–20, DOI 10.1006/aima.1996.1590. MR1440251 (98c:13007)

[6] H. E. A. Campbell, I. P. Hughes, R. J. Shank, and D. L. Wehlau, Bases for rings of coinvariants, Transform. Groups 1 (1996), no. 4, 307–336, DOI 10.1007/BF02549211. MR1424447 (98a:13011)

[7] H. E. A. Campbell, R. J. Shank, and D. L. Wehlau, Rings of invariants for modular representations of elementary abelian \( p \)-groups, Transform. Groups 18 (2013), no. 1, 1–22, DOI 10.1007/s00031-013-9207-z. MR3022756

[8] H. E. A. Campbell, R. J. Shank, and D. L. Wehlau, Vector invariants for the two-dimensional modular representation of a cyclic group of prime order, Adv. Math. 225 (2010), no. 2, 1069–1094, DOI 10.1016/j.aim.2009.12.001. MR2562623 (2011a:13008)

[9] Harm Derksen and Gregor Kemper, Computational invariant theory, Invariant Theory and Algebraic Transformation Groups I, Encyclopaedia of Mathematical Sciences, 130. Springer-Verlag, Berlin, 2002. MR1918599 (2003g:13004)

[10] Jonathan Elmer and Peter Fleischmann, On the depth of modular invariant rings for the groups \( C_p \times C_p \), Symmetry and spaces, Progr. Math., vol. 278, Birkhäuser Boston, Inc., Boston, MA, 2010, pp. 45–61, DOI 10.1007/978-0-8176-4875-6. MR2562623 (2011a:13008)

[11] Ming-chang Kang, Fixed fields of triangular matrix groups, J. Algebra 302 (2006), no. 2, 845–847, DOI 10.1016/j.jalgebra.2006.03.037. MR2293785 (2007m:13006)

[12] Martin Kohls and Müfit Sezer, Separating invariants for the Klein four group and cyclic groups, Internat. J. Math. 24 (2013), no. 6, 1350046, 11, DOI 10.1142/S0129167X13500468. MR3078070

[13] David R. Richman, On vector invariants over finite fields, Adv. Math. 81 (1990), no. 1, 30–65, DOI 10.1016/0001-8708(90)90003-6. MR1051222 (91g:15020)

[14] R. James Shank and David L. Wehlau, The transfer in modular invariant theory, J. Pure Appl. Algebra 142 (1999), no. 1, 63–77, DOI 10.1016/S0022-4049(98)00036-X. MR1716047 (2000b:13010)

[15] R. James Shank and David L. Wehlau, Computing modular invariants of \( p \)-groups, J. Symbolic Comput. 34 (2002), no. 5, 307–327, DOI 10.1006/jsco.2002.0558. MR1937464 (2003j:13006)
[20] R. James Shank and David L. Wehlau, *Decomposing symmetric powers of certain modular representations of cyclic groups*, Symmetry and spaces, Progr. Math., vol. 278, Birkhäuser Boston, Inc., Boston, MA, 2010, pp. 169–196, DOI 10.1007/978-0-8176-4875-6_9. MR2562628 (2010j:13015)

[21] Bernd Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996. MR1363949 (97b:13034)

[22] Peter Symonds, *On the Castelnuovo-Mumford regularity of rings of polynomial invariants*, Ann. of Math. (2) 174 (2011), no. 1, 499–517, DOI 10.4007/annals.2011.174.1.14. MR2811606 (2012j:13006)

[23] David L. Wehlau, *Invariants for the modular cyclic group of prime order via classical invariant theory*, J. Eur. Math. Soc. (JEMS) 15 (2013), no. 3, 775–803, DOI 10.4171/JEMS/376. MR3085091

Department of Mathematics, Bilkent University, 06800 Ankara, Turkey

E-mail address: sezer@fen.bilkent.edu.tr

School of Mathematics, Statistics and Actuarial Science, University of Kent, Canterbury, CT2 7NF, United Kingdom

E-mail address: R.J.Shank@kent.ac.uk