International Journal of Mathematics
Vol. 24, No. 6 (2013) 1350046 (11 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0129167X13500468

Metadata, citation and similar pape

rsity Institutional Repository

SEPARATING INVARIANTS FOR THE KLEIN FOUR GROUP AND CYCLIC GROUPS

MARTIN KOHLS

Technische Universität München
Zentrum Mathematik-M11
Boltzmannstrasse 3, 85748 Garching, Germany
kohls@ma.tum.de

MÜFİT SEZER

Department of Mathematics, Bilkent University
Ankara 06800, Turkey
sezer@fen.bilkent.edu.tr

Received 5 August 2011
Accepted 3 May 2013
Published 11 June 2013

We consider indecomposable representations of the Klein four group over a field of characteristic 2 and of a cyclic group of order pm with p, m coprime over a field of characteristic p. For each representation, we explicitly describe a separating set in the corresponding ring of invariants. Our construction is recursive and the separating sets we obtain consist of almost entirely orbit sums and products.

Keywords: Separating invariants; Klein four group; cyclic groups.

Mathematics Subject Classification 2010: 13A50

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com
by BILKENT UNIVERSITY on 05/13/14. For personal use only.

1. Introduction

Let V be a finite-dimensional representation of a group G over an algebraically closed field F. In the sequel, we will also call V a G-module. There is an induced action on the symmetric algebra $F[V] := S(V^*)$ given by $\sigma(f) = f \circ \sigma^{-1}$ for $\sigma \in G$ and $f \in F[V]$ (we use σ^{-1} instead of σ to obtain a left action). We let $F[V]^G$ denote the subalgebra of invariant polynomials in $F[V]$. A subset $A \subseteq F[V]^G$ is said to be separating for V if for any pair of vectors $u, w \in V$, we have: If $f(u) = f(w)$ for all $f \in A$, then $f(u) = f(w)$ for all $f \in F[V]^G$. Goals in invariant theory include finding generators and studying properties of invariant rings. In the study of separating invariants the goal is rather to find and describe a subalgebra of the ring of invariants which separates the group orbits. Although separating invariants have been an object of study since the early times of invariant theory, they have regained particular attention following the influential textbook of Derksen and Kemper [5]. The invariant ring is often too complicated and it is difficult to describe explicit generators and relations. Meanwhile, there have been several papers within the last decade that demonstrate that one can construct separating subalgebras with nice properties that make them more accessible. For instance, Noether's (relative) bound holds for separating invariants independently of the characteristic of the field [5, Corollary 3.9.14]. For more results on separating algebras we direct the reader to [6–16].

If the order of the group is divisible by the characteristic of the field, then the degrees of the generators can become arbitrarily big. Therefore, computing the invariant ring in this case is particularly difficult. Even in the simplest situation of a cyclic group of prime order acting through Jordan blocks, explicit generating sets are known only for a handful of cases. This rather short list of cases consists of indecomposable representations up to dimension nine and decomposable ones whose indecomposable summands have dimension at most four. See [17] for a classical work and [18] for the most recent advances in this matter which also gives a good taste of the difficulty of the problem. On the other hand, separating invariants for these representations have a surprisingly simple theory. In [15, 16], it is observed that a separating set for an indecomposable representation of a cyclic p-group over a field of characteristic p can be obtained by adding some explicitly defined invariant polynomials to a separating set for a certain quotient representation. The main ingredient of the proofs of these results is the efficient use of the surjection of a representation to a quotient representation to establish a link between the respective separating sets that generating sets do not have. In this paper, we build on this technique to construct separating invariants for the indecomposable representations of the Klein four group over a field of characteristic 2 and of a cyclic group of order pm with p, m coprime over a field of characteristic p. Despite being the immediate follow ups of the cyclic p-groups, their invariant rings have not been computed yet. Therefore, these groups (and representations) appear to be the natural cases to consider. As in the case for cyclic p-groups, we describe a finite separating set recursively. We remark that in [5, Theorem 3.9.13], see also [12, Corollary 19], a way is given for calculating separating invariants explicitly for any finite group. This is done by presenting a large polynomial whose coefficients form a separating set. On the other hand, the separating sets we compute consist of invariant polynomials that are almost exclusively orbit sums and products. These are "basic" invariants which are easier to obtain. Additionally, our approach respects the inductive structure of the considered modules. Also, the size of the set we give for the cyclic group of order pm depends only on the dimension of the representation while the size in [5, Theorem 3.9.13] depends on the group order as well. Hence, for large p and m our separating set is much smaller for this group.

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com by BILKENT UNIVERSITY on 05/13/14. For personal use only.

The strategy of our construction is based on the following theorem.

Theorem 1.1. *Let V and W be G-modules, $\phi : V \to W$ a G-equivariant surjection, and $\phi^* : F[W] \hookrightarrow F[V]$ the corresponding inclusion. Let $S \subseteq F[W]^G$ be a separating set for W. Assume that $T \subseteq F[V]^G$ is a set of invariant polynomials with the following property: if $v_1, v_2 \in V$ are in different G-orbits and if $\phi(v_1) = \phi(v_2)$, then there is a polynomial $f \in T$ such that $f(v_1) \neq f(v_2)$. Then $\phi^*(S) \cup T$ is a separating set for V.*

Proof. Pick two vectors $v_1, v_2 \in V$ in different G-orbits. If $\phi(v_1)$ and $\phi(v_2)$ are in different G-orbits, then there exists a polynomial $f \in S$ that separates these vectors, so $\phi^*(f)$ separates v_1, v_2. So, we may assume that $\phi(v_1)$ and $\phi(v_2)$ are in the same G-orbit. Furthermore, by replacing v_2 with a suitable vector in its orbit we may take $\phi(v_1) = \phi(v_2)$. Hence, by construction, T contains an invariant that separates v_1 and v_2 as desired. □

Before we finish this section we recall the definitions of a transfer and a norm. For a subgroup $H \subseteq G$ and $f \in F[V]^H$, the relative transfer $\mathrm{Tr}_H^G(f)$ is defined to be $\sum_{\sigma \in G/H} \sigma(f)$. We also denote $\mathrm{Tr}_{\{\iota\}}^G(f) = \mathrm{Tr}^G(f)$, where ι is the identity element of G. Also for $f \in F[V]$, the norm $N_H(f)$ is defined to be the product $\prod_{\sigma \in H} \sigma(f)$.

2. The Klein Four Group

For the rest of this section, G denotes the Klein four group $\{\iota, \sigma_1, \sigma_2, \sigma_3\}$ ($\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \iota$ and $\sigma_1\sigma_3 = \sigma_2$). Over an algebraically closed field F of characteristic 2, the complete list of indecomposable G-modules is given in Benson [2, Theorem 4.3.3]. For each module in the list, we will explicitly construct a finite separating set. The modules in this list come in five "types". We use the same enumeration as in [2]. The first type (i) is just the regular representation FG of G. A minimal generating set consisting of six orbit sums of degree at most four is given in [4, Sec. 4.7], and the invariant ring can also easily be computed with Magma. In the following, we will thus concentrate on the remaining four types, where each type consists of an infinite series of indecomposable representations. Let I_n denote the identity matrix of $F^{n \times n}$, and J_λ denote an upper triangular Jordan block of size n with eigenvalue $\lambda \in F$. Let $H_i = \{\iota, \sigma_i\}$ for $i = 1, 2, 3$ be the three subgroups of order 2.

2.1. *Types* (ii) *and* (iii)

The even-dimensional indecomposable representations fall into two types. For $\lambda \in F$, we let $V_{2n,\lambda}$ denote the $2n$-dimensional module afforded by the representation given by $\sigma_1 \mapsto \left(\begin{smallmatrix} I_n & I_n \\ 0 & I_n \end{smallmatrix}\right)$ and $\sigma_3 \mapsto \left(\begin{smallmatrix} I_n & J_\lambda \\ 0 & I_n \end{smallmatrix}\right)$. The representations $V_{2n,\lambda}$ comprise those of type (ii). Meanwhile type (iii) representations are given by $\sigma_1 \mapsto \left(\begin{smallmatrix} I_n & J_0 \\ 0 & I_n \end{smallmatrix}\right)$ and $\sigma_3 \mapsto \left(\begin{smallmatrix} I_n & I_n \\ 0 & I_n \end{smallmatrix}\right)$ for $n \geq 1$. We denote these modules by W_{2n}. Notice that the matrix

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com by BILKENT UNIVERSITY on 05/13/14. For personal use only.

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com
by BILKENT UNIVERSITY on 05/13/14. For personal use only.

group associated with W_{2n} is the same as the matrix group associated with $V_{2n,0}$. Therefore, their invariant rings are equal, and a separating set for $V_{2n,0}$ is also a separating set for W_{2n}. We write $F[V_{2n,\lambda}] = F[x_1, \dots, x_{2n}]$. We then have

$$\begin{aligned}
\sigma_1 x_i &= x_i + x_{n+i} && \text{for } 1 \le i \le n,\\
\sigma_3 x_i &= x_i + \lambda x_{n+i} + x_{n+i+1} && \text{for } 1 \le i \le n-1,\\
\sigma_3 x_n &= x_n + \lambda x_{2n},\\
x_{n+i} &\in F[V_{2n,\lambda}]^G && \text{for } 1 \le i \le n.
\end{aligned}$$

We start by computing several transfers and norms modulo some subspaces of $F[V_{2n,\lambda}]$. Define $R := F[x_2, \dots, x_{2n}]$ and $S := F[x_1, \dots, x_{n-1}, x_{n+1}, \dots, x_{2n}]$. Note that S is a G-subalgebra of $F[V_{2n,\lambda}]$. We will need the first assertion of the following lemma for type (v) as well, so we mark this result with a star. Note that the given congruence particularly holds modulo R, as R contains $R \cap S$.

Lemma 2.1. *We have*

(a*) $\mathrm{Tr}^G(x_1 x_i x_j) \equiv x_1(x_{n+i}x_{n+j+1} + x_{n+i+1}x_{n+j}) \mod R \cap S$ *for* $2 \le i, j \le n-1$.
(b) $\mathrm{Tr}^G(x_1 x_{n-1} x_n) \equiv x_1 x_{2n}^2 \mod R$.

Proof. (a*) Since we work modulo the *subvectorspace* $R \cap S$ we only consider the terms containing x_1 or x_n. So

$$\begin{aligned}
\mathrm{Tr}^G(x_1 x_i x_j) &\equiv x_1 x_i x_j + x_1(x_i + x_{n+i})(x_j + x_{n+j})\\
&\quad + x_1(x_i + \lambda x_{n+i} + x_{n+i+1})(x_j + \lambda x_{n+j} + x_{n+j+1})\\
&\quad + x_1(x_i + (\lambda+1)x_{n+i} + x_{n+i+1})(x_j + (\lambda+1)x_{n+j} + x_{n+j+1})\\
&\equiv x_1 x_{n+i}x_{n+j+1} + x_1 x_{n+i+1}x_{n+j} \mod R \cap S.
\end{aligned}$$

(b) This part follows along the same lines as the first part. □

The invariant in (b) of the following lemma will also be needed for type (v).

Lemma 2.2. *For* $n \ge 3$, *we have*

(a) $\mathrm{Tr}^G(x_1 x_2^3) \equiv \lambda(\lambda+1)x_1 x_{n+2}^3 \mod (R + x_{n+3}F[V_{2n,\lambda}])$.
(b*) *The polynomial* $N_{H_2}(x_1 x_{n+2} + x_2 x_{n+1})$ *is in* $F[V_{2n,\lambda}]^G$. *Moreover, we have*

$$N_{H_2}(x_1 x_{n+2} + x_2 x_{n+1}) \equiv x_1^2 x_{n+2}^2 + x_1 x_{n+2}(x_{n+2}^2 + x_{n+1}x_{n+3}) \mod R \cap S.$$

Proof. (a) We only consider the terms containing x_1 and not x_{n+3}, so

$$\begin{aligned}
\mathrm{Tr}^G(x_1 x_2^3) &\equiv x_1 x_2^3 + x_1(x_2 + x_{n+2})^3 + x_1(x_2 + \lambda x_{n+2})^3\\
&\quad + x_1(x_2 + (\lambda+1)x_{n+2})^3\\
&\equiv \lambda(\lambda+1)x_1 x_{n+2}^3 \mod (R + x_{n+3}F[V_{2n,\lambda}]).
\end{aligned}$$

(b) Note that $x_1x_{n+2} + x_2x_{n+1}$ is H_1-invariant, so the H_2-orbit product of this polynomial is G-invariant. Second, we have

$$\begin{aligned}\sigma_2(x_1x_{n+2} + x_2x_{n+1}) = {} & (x_1 + (\lambda+1)x_{n+1} + x_{n+2})x_{n+2} \\ & + (x_2 + (\lambda+1)x_{n+2} + x_{n+3})x_{n+1}.\end{aligned}$$

Considering the monomials that are divisible by x_1 in the orbit product, a routine computation yields the desired equivalence. □

Let $(a_1, \ldots, a_n, a_{n+1}, \ldots, a_{2n}) \in F^{2n}$. We have a G-equivariant surjection $V_{2n,\lambda} \to V_{2n-2,\lambda}$ given by

$$\phi : (a_1, \ldots, a_n, a_{n+1}, \ldots, a_{2n}) \to (a_2, \ldots, a_n, a_{n+2}, \ldots, a_{2n}) \in F^{2n-2}.$$

Therefore, $F[V_{2n-2,\lambda}] = F[x_2, \ldots, x_n, x_{n+2}, \ldots, x_{2n}]$ is a G-subalgebra of $F[V_{2n,\lambda}] = F[x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n}]$.

Proposition 2.1. *Let $n \geq 3$ and $S \subseteq F[V_{2n-2,\lambda}]^G$ be a separating set for $V_{2n-2,\lambda}$. Then $\phi^*(S)$ together with the set T consisting of*

$$x_{n+1}, \quad N_G(x_1), \quad f_\lambda := \begin{cases} \mathrm{Tr}^G(x_1x_2^3) & \text{for } \lambda \neq 0, 1 \\ N_{H_2}(x_1x_{n+2} + x_2x_{n+1}) & \text{for } \lambda \in \{0, 1\}, \end{cases}$$

$$\mathrm{Tr}^G(x_1x_ix_{i+1}) \quad \text{for } 2 \leq i \leq n-1$$

is a separating set for $V_{2n,\lambda}$. Moreover, a separating set for $V_{2n,0}$ is a separating set for W_{2n}.

Proof. Let $v_1 = (a_1, \ldots, a_n, a_{n+1}, \ldots, a_{2n})$ and $v_2 = (b_1, \ldots, b_n, b_{n+1}, \ldots, b_{2n})$ be two vectors in V_{2n} with $\phi(v_1) = \phi(v_2)$, so $a_i = b_i$ for $i \in \{1, \ldots, 2n\} \backslash \{1, n+1\}$. To apply Theorem 1.1, we show that if all elements of T take the same values on v_1 and v_2, then v_1 and v_2 are in the same orbit. Since $x_{n+1} \in T$, we have $a_{n+1} = b_{n+1}$, hence we have $v_2 = (b_1, a_2, \ldots, a_n, a_{n+1}, \ldots, a_{2n})$. If $a_1 = b_1$ we are done, therefore we consider the case $a_1 \neq b_1$. Then Lemma 2.1(b) implies $a_{2n} = 0$. Since $\mathrm{Tr}^G(x_1x_ix_{i+1}) \equiv x_1(x_{n+i}x_{n+i+2} + x_{n+i+1}^2) \mod R$ for $2 \leq i \leq n-2$, we successively get $a_{2n-1} = a_{2n-2} = \cdots = a_{n+3} = 0$. If $\lambda \neq 0, 1$ we also have $a_{n+2} = 0$ by Lemma 2.2(a). If $\lambda \in \{0, 1\}$ and $a_{n+2} \neq 0$, $N_{H_2}(x_1x_{n+2} + x_2x_{n+1})$ taking the same value on v_1, v_2 implies $a_1 = b_1 + a_{n+2}$, hence $v_1 = \sigma_3v_2$ for $\lambda = 0$ and $v_1 = \sigma_2v_2$ for $\lambda = 1$ respectively, and we are done. So now assume $a_{n+2} = 0$. Then $N_G(x_1)(v_1) = N_G(x_1)(v_2)$ implies $a_1 + b_1 \in \{a_{n+1}, \lambda a_{n+1}, (\lambda+1)a_{n+1}\}$, hence $v_1 = \sigma_iv_2$ for some $i \in \{1, 2, 3\}$.

The final statement follows because the matrix group associated to $V_{2n,0}$ is the same as the group associated to W_{2n}, so their invariant rings are equal. □

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com
by BILKENT UNIVERSITY on 05/13/14. For personal use only.

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com
by BILKENT UNIVERSITY on 05/13/14. For personal use only.

We start the induction for $\lambda \neq 0, 1$ — the case $\lambda \in \{0, 1\}$ is left to the reader (or to Magma).

Lemma 2.3. *A separating set for $\lambda \neq 0, 1$ and $n = 2$ is given by the invariants*

$$g_1 := x_1x_4 + \frac{1}{\lambda(\lambda+1)}x_2^2 + x_2\left(x_3 + \frac{1}{\lambda(\lambda+1)}x_4\right),$$

$$N_G(x_1), \quad N_G(x_2), \quad x_3, \quad x_4.$$

Note that since G is not a reflection group, we need at least five separating invariants by [8, Theorem 1.1].

Proof of Lemma 2.3. We show that two points v_1, v_2 which cannot be separated by the invariants above are in the same orbit. The invariants x_3, x_4 imply that the two points have the form $v_1 = (a_1, a_2, a_3, a_4)$ and $v_2 = (b_1, b_2, a_3, a_4)$. As $N_G(x_2)(v_1) = N_G(x_2)(v_2)$, we have $a_2 + b_2 \in \{0, a_4, \lambda a_4, (\lambda + 1)a_4\}$, so after replacing v_2 by an element in its orbit we can assume $a_2 = b_2$. If $a_4 \neq 0$, then $g_1(v_1) = g_1(v_2)$ implies $a_1 = b_1$ and we are done. Therefore, we consider the case $a_4 = 0$. Then $N_G(x_1)(v_1) = N_G(x_1)(v_2)$ implies $a_1 + b_1 \in \{0, a_3, \lambda a_3, (\lambda + 1)a_3\}$, so v_1, v_2 are in the same orbit. □

2.2. *Type* (iv)

This type is afforded by the representation given by

$$\sigma_1 \mapsto \left(\begin{array}{c|c} I_n & \begin{array}{c} 0_{1\times(n-1)} \\ \hline I_{n-1} \end{array} \\ \hline 0 & I_{n-1} \end{array}\right) \quad \text{and} \quad \sigma_2 \mapsto \left(\begin{array}{c|c} I_n & \begin{array}{c} I_{n-1} \\ \hline 0_{1\times(n-1)} \end{array} \\ \hline 0 & I_{n-1} \end{array}\right)$$

for a positive integer n, where $0_{k\times l}$ denotes a $k \times l$ matrix whose entries are all zero. We let W_{2n-1} denote this representation. Notice that W_{2n-1} is isomorphic to the submodule of $V_{2n,1}$ spanned by $e_1, \ldots, e_n, e_{n+2}, \ldots, e_{2n}$, where $e_1, \ldots, e_{2n}$ are the standard basis vectors of F^{2n}. Dual to this inclusion, there is a restriction map $F[V_{2n,1}]^G \to F[W_{2n-1}]^G$, $f \mapsto f|_{W_{2n-1}}$ which sends separating sets to separating sets by [5, Theorem 2.3.16]. Therefore, in view of Proposition 2.1, we have the following.

Proposition 2.2. *Assume the notation of Proposition* 2.1. *Let $n \geq 3$ and $S \subseteq F[V_{2n-2,1}]^G$ be a separating set for $V_{2n-2,1}$. Let T denote the set of polynomials consisting of $\phi^*(S)$, $N_G(x_1)$, f_1 and $\mathrm{Tr}^G(x_1x_ix_{i+1})$ for $2 \leq i \leq n-1$. Then the polynomials in T restricted to W_{2n-1} form a separating set for W_{2n-1}.*

2.3. *Type* (v)

We consider the type (ii) module $V_{2n,1}$. Then $\langle e_n \rangle$ is a G-submodule, and we define $V_{2n-1} := V_{2n,1}/\langle e_n \rangle$ with basis $\tilde{e}_i := e_i + \langle e_n \rangle$, $i \in \{1, \ldots, 2n\}\backslash\{n\}$. The modules

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com
by BILKENT UNIVERSITY on 05/13/14. For personal use only.

V_{2n-1} comprise the type (v) representations and they are afforded by

$$\sigma_1 \mapsto \left(\begin{array}{c|c|c} I_{n-1} & I_{n-1} & 0_{(n-1)\times 1} \\ \hline 0 & \multicolumn{2}{c}{I_n} \end{array}\right) \quad \text{and} \quad \sigma_2 \mapsto \left(\begin{array}{c|c|c} I_{n-1} & 0_{(n-1)\times 1} & I_{n-1} \\ \hline 0 & \multicolumn{2}{c}{I_n} \end{array}\right).$$

We have a G-algebra inclusion $F[V_{2n-1}] = F[x_1, \dots, x_{n-1}, x_{n+1}, \dots, x_{2n}] \subset F[V_{2n,1}]$.

The action on the variables is given by

$$\sigma_1(x_i) = \begin{cases} x_i + x_{n+i} & \text{for } 1 \le i \le n-1, \\ x_i & \text{for } n+1 \le i \le 2n, \end{cases}$$

and

$$\sigma_2(x_i) = \begin{cases} x_i + x_{n+i+1} & \text{for } 1 \le i \le n-1, \\ x_i & \text{for } n+1 \le i \le 2n. \end{cases}$$

Let $(a_1, \dots, a_{n-1}, a_{n+1}, \dots, a_{2n}) \in F^{2n-1} \cong V_{2n-1}$. We have a G-equivariant surjection $V_{2n-1} \to V_{2n-3}$ given by

$$\phi : (a_1, \dots, a_{n-1}, a_{n+1}, \dots, a_{2n}) \to (a_2, \dots, a_{n-1}, a_{n+2}, \dots, a_{2n}) \in F^{2n-3}.$$

Therefore, $F[V_{2n-3}] = F[x_2, \dots, x_{n-1}, x_{n+2}, \dots, x_{2n}]$ is a G-subalgebra of $F[V_{2n-1}] = F[x_1, \dots, x_{n-1}, x_{n+1}, \dots, x_{2n}]$. Also, let $R := F[x_2, \dots, x_{n-1}, x_{n+1}, \dots, x_{2n}]$. We will make computations modulo R, considered as a subvectorspace of $F[V_{2n-1}]$, and we can reuse the equations of Lemmas 2.1(a*) and 2.2(b*).

Lemma 2.4. *Let $v_1, v_2 \in V_{2n-1}$ be two vectors in different orbits that agree everywhere except the first coordinate. Say, $v_1 = (a_1, \dots, a_{n-1}, a_{n+1}, \dots, a_{2n})$, $v_2 = (b_1, a_2, \dots, a_{n-1}, a_{n+1}, \dots, a_{2n})$. Assume further that one of the following holds*:

(a) *$a_{n+2} \ne 0$ and $a_i = 0$ for $n+3 \le i \le 2n$,*
(b) *$a_i = a_{2n} \ne 0$ for $n+2 \le i \le 2n-1$.*

Then the invariant

$$N_{H_2}(x_1 x_{n+2} + x_2 x_{n+1}) \equiv x_1^2 x_{n+2}^2 + x_1 x_{n+2}(x_{n+2}^2 + x_{n+1} x_{n+3}) \mod R$$

separates v_1 and v_2.

Proof. Note that $N_{H_2}(x_1 x_{n+2} + x_2 x_{n+1})$ was also used in the separating set for the even-dimensional representations, see Lemma 2.2(b*). We let f denote this polynomial. We have to show that if f does not separate v_1, v_2, then these two points are in the same orbit. By assumption, $a_1 \ne b_1$. First, assume (a) holds. Then $f(v_1) = f(v_2)$ implies $(a_1 + b_1)^2 a_{n+2}^2 = (a_1 + b_1) a_{n+2}^3$, hence $a_1 = b_1 + a_{n+2}$. Since $a_i = 0$ for $i \ge n+3$ this implies that $v_1 = \sigma_2 v_2$ and we are done. Next assume (b) holds. Then $f(v_1) = f(v_2)$ implies $(a_1 + b_1)^2 a_{n+2}^2 = (a_1 + b_1) a_{n+2}^2 (a_{n+1} + a_{n+2})$, hence $a_1 = b_1 + a_{n+1} + a_{n+2}$. Since $a_i = a_{2n}$ for $n+2 \le i \le 2n-1$, this implies that $v_1 = \sigma_3 v_2$. □

Lemma 2.5. *For $2 \leq i \leq n-1$, we have*

$$\operatorname{Tr}^G(x_1 x_i^3) \equiv x_1 x_{n+i} x_{n+i+1}(x_{n+i} + x_{n+i+1}) \mod R.$$

Proof.

$$\begin{aligned}\operatorname{Tr}^G(x_1 x_i^3) &\equiv x_1 x_i^3 + x_1(x_i + x_{n+i})^3 + x_1(x_i + x_{n+i+1})^3 \\ &\quad + x_1(x_i + x_{n+i} + x_{n+i+1})^3 \\ &\equiv x_1 x_{n+i} x_{n+i+1}(x_{n+i} + x_{n+i+1}) \mod R.\end{aligned}$$

□

Proposition 2.3. *Let $n \geq 3$ and $S \subseteq F[V_{2n-3}]^G$ be a separating set for V_{2n-3}. Then $\phi^*(S)$ together with the set T consisting of*

$$x_{n+1}, \quad N_G(x_1), \quad N_{H_2}(x_1 x_{n+2} + x_2 x_{n+1}), \quad \operatorname{Tr}^G(x_1 x_2 x_{n-1}),$$

$$\operatorname{Tr}^G(x_1 x_i x_{i+1}) \quad \textit{for } 2 \leq i \leq n-2, \quad \operatorname{Tr}^G(x_1 x_i^3) \quad \textit{for } 2 \leq i \leq n-1$$

is a separating set for V_{2n-1}.

Proof. Let

$$v_1 = (a_1, \ldots, a_{n-1}, a_{n+1}, \ldots, a_{2n}) \quad \text{and} \quad v_2 = (b_1, \ldots, b_{n-1}, b_{n+1}, \ldots, b_{2n})$$

be two vectors in V_{2n-1} with $\phi(v_1) = \phi(v_2)$, so $a_i = b_i$ for all $i \neq 1, n+1$. To apply Theorem 1.1, we show that if all elements of T take the same values on v_1 and v_2, then these two points are in the same orbit. Since $x_{n+1} \in T$, we have $a_{n+1} = b_{n+1}$, hence we have $v_2 = (b_1, a_2, \ldots, a_{n-1}, a_{n+1}, \ldots, a_{2n})$. If $a_1 = b_1$ we are done, so we consider the case $a_1 \neq b_1$.

We first assume $a_{n+i} \neq 0$ for all $2 \leq i \leq n$. Lemma 2.5 implies $a_{n+2} = a_{n+3} = \cdots = a_{2n} \neq 0$, and from Lemma 2.4(b) it follows v_1 and v_2 are in the same orbit, and we are done. Therefore, we now assume there is a $2 \leq i \leq n$ with $a_{n+i} = 0$, and let i be maximal with this property. Consider the invariants $f_j := \operatorname{Tr}^G(x_1 x_j x_{j+1}) \equiv x_1(x_{n+j} x_{n+j+2} + x_{n+j+1}^2) \mod R$ of T for $2 \leq j \leq n-2$ (see Lemma 2.1(a*)).

For $2 \leq j \leq n-2$, if $a_{n+j} = 0$, then $f_j(v_1) = f_j(v_2)$ implies $a_{n+j+1} = 0$. Therefore, $i \geq n-1$.

If $i = n-1$, then $a_{2n} \neq 0$, and $f_j(v_1) = f_j(v_2)$ for $j = n-3, n-4, \ldots, 2$ implies $a_{n+j} = 0$ for $3 \leq j \leq n-1$. As $\operatorname{Tr}^G(x_1 x_2 x_{n-1}) \equiv x_1(x_{n+2} x_{2n} + x_{n+3} x_{2n-1}) \mod R$ takes the same value on v_1, v_2, we also have $a_{n+2} = 0$. Now, $N_G(x_1)(v_1) = N_G(x_1)(v_2)$ implies $a_1 = b_1 + a_{n+1}$, thus $v_1 = \sigma_1 v_2$, and we are done.

If $i = n$, i.e. $a_{2n} = 0$, then since $f_j(v_1) = f_j(v_2)$ for $j = n-2, n-3, \ldots, 2$, we get $a_{n+j} = 0$ for $3 \leq j \leq 2n$. In case $a_{n+2} \neq 0$, we are done by Lemma 2.4(a). If $a_{n+2} = 0$, then $N_G(x_1)(v_1) = N_G(x_1)(v_2)$ implies as before $a_1 = b_1 + a_{n+1}$ and $v_1 = \sigma_1 v_2$. □

Remark 2.1. A separating set for V_3 is formed by $N_G(x_1), x_3, x_4$. In fact, these polynomials form a homogeneous system of parameters for $F[V_3]^G$. Since the product of their degrees is equal to four, it follows from [5, Theorem 3.7.5] that $F[V_3]^G = F[N_G(x_1), x_3, x_4]$.

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com
by BILKENT UNIVERSITY on 05/13/14. For personal use only.

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com
by BILKENT UNIVERSITY on 05/13/14. For personal use only.

3. Cyclic Groups

Let F be a field of positive characteristic p and $G = \boldsymbol{Z}_{p^r m}$ be the cyclic group of order $p^r m$, where r, m are non-negative integers with $(m, p) = 1$. Let H and M be the subgroups of G of order p^r and m, respectively. Let V_n be an indecomposable G-module of dimension n.

Lemma 3.1. *There exists a basis $e_1, e_2, \ldots, e_n$ of V_n such that $\sigma^{-1}(e_i) = e_i + e_{i+1}$ for $1 \leq i \leq n-1$ and $\sigma^{-1}(e_n) = e_n$ for a generator σ of H, and $\alpha(e_i) = \lambda e_i$ for $1 \leq i \leq n$ for a mth root of unity $\lambda \in F$ and α a generator of M.*

Proof. It is well known that $n \leq p^r$ and there is basis such that a generator ρ of G acts by a Jordan matrix $J_\mu = \mu I_n + N$ with μ a mth root of unity [1, p. 24]. Then ρ^{p^r} is a generator of M acting by $(\mu I_n + N)^{p^r} = \mu^{p^r} I_n$, and ρ^m is a generator of H acting by $(\mu I_n + N)^m = I_n + m\mu^{m-1}N + \binom{m}{2}\mu^{m-2}N^2 + \cdots$. This matrix has Jordan normal form $J_1 = I_n + N$, and the matrix representing ρ^{p^r} is fixed under change of basis, which proves the lemma. □

Since we want our representation to be faithful, we will assume that λ is a primitive mth root of unity from now on. We also restrict to the case $r = 1$. Let $x_1, x_2, \ldots, x_n$ be the corresponding basis elements in V_n^*. We have $\sigma(x_i) = x_i + x_{i-1}$ for $2 \leq i \leq n$, $\sigma(x_1) = x_1$ and $\alpha(x_i) = \lambda^{-1} x_i$ for $1 \leq i \leq n$. Since α acts by multiplication by a primitive mth root of unity, there exists a non-negative integer k such that $x_n x_{i+1}^{p-1} x_i^k \in F[V_n]^M$ for $1 \leq i \leq n-2$. We assume that k is the smallest such integer. Notice that k is the least integer satisfying $k \equiv -p \mod m$. Let I_i denote the ideal in $F[V_n]$ generated by $x_1, x_2, \ldots, x_i$. Set $f_i = x_n x_{i+1}^{p-1} x_i^k$ for $1 \leq i \leq n-2$.

Lemma 3.2. *Let a be a positive integer. Then $\sum_{0 \leq l \leq p-1} l^a \equiv -1 \mod p$ if $p-1$ divides a and $\sum_{0 \leq l \leq p-1} l^a \equiv 0 \mod p$, otherwise.*

Proof. See [3, 9.4] for a proof for this statement. □

Now set $R := F[x_1, x_2, \ldots, x_{n-1}]$.

Lemma 3.3. *Let $1 \leq i \leq n-2$. We have*

$$\mathrm{Tr}_M^G(f_i) \equiv -x_n x_i^{p+k-1} \mod (I_{i-1} + R).$$

Proof. We only consider the terms containing x_n but not $x_1, \ldots, x_{i-1}$, thus we have

$$\begin{aligned}\sigma^l(f_i) &= \left(x_n + l x_{n-1} + \binom{l}{2} x_{n-2} + \cdots\right)(x_{i+1} + l x_i + \cdots)^{p-1}(x_i + l x_{i-1} + \cdots)^k \\ &\equiv x_n (x_{i+1} + l x_i)^{p-1} x_i^k \mod (I_{i-1} + R).\end{aligned}$$

Thus it suffices to show that $\sum_{0 \leq l \leq p-1} (x_{i+1} + l x_i)^{p-1} = -x_i^{p-1}$. Let a and b be non-negative integers such that $a + b = p - 1$. Then the coefficient of $x_{i+1}^a x_i^b$ in

$(x_{i+1}+lx_i)^{p-1}$ is $\binom{p-1}{b}l^b$ and so the coefficient of $x_{i+1}^a x_i^b$ in $\sum_{0\le l\le p-1}(x_{i+1}+lx_i)^{p-1}$ is $\sum_{0\le l\le p-1}\binom{p-1}{b}l^b$. Hence, the result follows from the previous lemma. □

Let $(c_1, c_2, \ldots, c_n)$ be a vector in V_n. There is a G-equivariant surjection $\phi : V_n \to V_{n-1}$ given by $(c_1, c_2, \ldots, c_n) \to (c_1, c_2, \ldots, c_{n-1})$. Hence, $F[V_{n-1}] = F[x_1, \ldots, x_{n-1}]$ is a G-subalgebra of $F[V_n]$. Let l be the smallest non-negative integer such that $N_H(x_n)(N_H(x_{n-1}))^l \in F[V_n]^G$. In fact, α acts on the monomials in the polynomial $N_H(x_n)(N_H(x_{n-1}))^l$ by multiplication with $\lambda^{-(l+1)p}$. So the action of α on $N_H(x_n)(N_H(x_{n-1}))^l$ is trivial, if $p(l+1) \equiv 0 \mod m$. Since $(p, m) = 1$, we have $l = m - 1$.

Proposition 3.1. *Let $S \subseteq F[V_{n-1}]^G$ be a separating set for V_{n-1}. Then $\phi^*(S)$ together with the set T consisting of*

$$N_H(x_n)(N_H(x_{n-1}))^{m-1}, \quad N_G(x_n), \quad \mathrm{Tr}_M^G(f_i) \quad \textit{for } 1 \le i \le n-2$$

is a separating set for V_n.

Proof. Let $v_1 = (c_1, c_2, \ldots, c_n)$ and $v_2 = (d_1, d_2, \ldots, d_n)$ be two vectors in V_n with $\phi(v_1) = \phi(v_2)$, so $c_i = d_i$ for $1 \le i \le n-1$. To apply Theorem 1.1, we show that if all elements of T take the same values on v_1 and v_2, then v_1 and v_2 are in the same orbit. If $c_n = d_n$ we are done, so we consider the case $c_n \ne d_n$. Lemma 3.3 shows that $\mathrm{Tr}_M^G(f_i)$ taking the same value on v_1 and v_2 for $1 \le i \le n-2$ implies $c_1 = c_2 = \cdots = c_{n-2} = 0$. We consider two cases. First, assume that $c_{n-1} = 0$. Then $N_G(x_n)(v_1) = N_G(x_n)(v_2)$, i.e. $c_n^{pm} = d_n^{pm}$, implies that $c_n = \lambda^a d_n$ for some integer a and hence v_1 and v_2 are in the same orbit. If $c_{n-1} \ne 0$, we have $(N_H(x_{n-1}))^{m-1}(v_1) = (N_H(x_{n-1}))^{m-1}(v_2) \ne 0$, and therefore $N_H(x_n)(v_1) = N_H(x_n)(v_2)$. It follows $c_n^p - c_n c_{n-1}^{p-1} = d_n^p - d_n c_{n-1}^{p-1}$, which implies $c_n = d_n + jc_{n-1}$ for some $0 \le j \le p-1$, so v_1 and v_2 are in the same orbit. □

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com
by BILKENT UNIVERSITY on 05/13/14. For personal use only.

Acknowledgments

We thank the referee for carefully reading the manuscript and many useful remarks that improved the exposition. We also thank Gregor Kemper for funding a visit of the second author to TU München and Tübitak for funding a visit of the first author to Bilkent University. Second author is also partially supported by Tübitak-Tbag/112T113 and Tüba-Gebip/2010.

References

[1] J. L. Alperin, *Local Representation Theory: Modular Representations as an Introduction to the Local Representation Theory of Finite Groups*, Cambridge Studies in Advanced Mathematics, Vol. 11 (Cambridge University Press, Cambridge, 1986).

[2] D. J. Benson, *Representations and Cohomology. I, Basic Representation Theory of Finite Groups and Associative Algebras*, Cambridge Studies in Advanced Mathematics, 2nd edn., Vol. 30 (Cambridge University Press, Cambridge, second edition, 1998).

[3] H. E. A. Campbell, I. P. Hughes, R. J. Shank and D. L. Wehlau, Bases for rings of coinvariants, *Transform. Groups.* **1**(4) (1996) 307–336.

[4] H. E. A. E. Campbell and D. L. Wehlau, *Modular Invariant Theory.* Invariant Theory and Algebraic Transformation Groups, VIII, Encyclopaedia of Mathematical Sciences, Vol. 139 (Springer-Verlag, Berlin, 2011).

[5] H. Derksen and G. Kemper, *Computational Invariant Theory.* Invariant Theory and Algebraic Transformation Groups, I, Encyclopaedia of Mathematical Sciences, Vol. 130 (Springer-Verlag, Berlin, 2002).

[6] M. Domokos, Typical separating invariants, *Transform. Groups* **12**(1) (2007) 49–63.

[7] J. Draisma, G. Kemper and David Wehlau, Polarization of separating invariants, *Canad. J. Math.* **60**(3) (2008) 556–571.

[8] E. Dufresne, Separating invariants and finite reflection groups, *Adv. Math.* **221**(6) (2009) 1979–1989.

[9] E. Dufresne, J. Elmer and M. Kohls, The Cohen–Macaulay property of separating invariants of finite groups, *Transform. Groups* **14**(4) (2009) 771–785.

[10] E. Dufresne and M. Kohls, A finite separating set for Daigle and Freudenburg's counterexample to Hilbert's fourteenth problem, *Comm. Algebra* **38**(11) (2010) 3987–3992.

[11] H. Kadish, Polynomial bounds for invariant functions separating orbits, *J. Algebra* **359** (2012) 138–155.

[12] G. Kemper, Separating invariants, *J. Symbolic Comput.* **44** (2009) 1212–1222.

[13] M. Kohls and H. Kraft, Degree bounds for separating invariants, *Math. Res. Lett.* **17**(6) (2010) 1171–1182.

[14] M. D. Neusel and M. Sezer, Separating invariants for modular p-groups and groups acting diagonally, *Math. Res. Lett.* **16**(6) (2009) 1029–1036.

[15] M. Sezer, Constructing modular separating invariants, *J. Algebra* **322**(11) (2009) 4099–4104.

[16] M. Sezer, Explicit separating invariants for cyclic p-groups, *J. Combin. Theory Ser. A* **118**(2) (2011) 681–689.

[17] R. J. Shank, S.A.G.B.I. bases for rings of formal modular seminvariants [semi-invariants], *Comment. Math. Helv.* **73**(4) (1998) 548–565.

[18] D. L. Wehlau, Invariants for the modular cyclic group of prime order via classical invariant theory, *J. Eur. Math. Soc.* **15**(3) (2013) 775–803.

Int. J. Math. 2013.24. Downloaded from www.worldscientific.com
by BILKENT UNIVERSITY on 05/13/14. For personal use only.