Communications in Contemporary Mathematics
Vol. 19, No. 3 (2017) 1650023 (12 pages)

DOI: 10.1142/S0219199716500231

Degree of reductivity of a modular representation

Martin Kohls

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

Müfit Sezer

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

Received 14 June 2014
Accepted 30 January 2016
Published 15 March 2016

For a finite-dimensional representation V of a group G over a field F, the degree of reductivity $\delta(G, V)$ is the smallest degree d such that every nonzero fixed point $v \in V^G \backslash \{0\}$ can be separated from zero by a homogeneous invariant of degree at most d. We compute $\delta(G, V)$ explicitly for several classes of modular groups and representations. We also demonstrate that the maximal size of a cyclic subgroup is a sharp lower bound for this number in the case of modular abelian p-groups.

Keywords: Invariant theory; modular groups; reductive groups; degree bounds; Klein four group; separating invariants.

Mathematics Subject Classification 2010: 13A50

0. Introduction

Separating points from zero by invariants is a classical problem in invariant theory. While for infinite groups it is quite a problem to describe those points where this is (not) possible (leading to the definition of Hilbert's Nullcone), the finite group case is easier. We fix the setup before going into details. Unless otherwise stated, F denotes an algebraically closed field of characteristic $p > 0$. We consider a finite-dimensional representation V of a finite group G over F. We call V a G-module. The action of G on V induces an action of G on $F[V]$ via $\sigma(f) := f \circ \sigma^{-1}$ for $f \in F[V]$ and $\sigma \in G$. Any homogeneous system of parameters (hsop) $f_1, \dots, f_n$ of the invariant ring $F[V]^G$ has $\{0\}$ as its common zero set, hence every nonzero point can be separated from zero by one of the f_i. Moreover, Dade's algorithm [6, Sec. 3.3.1] produces an hsop in degree $|G|$, hence every nonzero point can be separated from zero by an invariant of degree at most $|G|$. Therefore, for a given nonzero point $v \in V\backslash\{0\}$, the number

$$\epsilon(G,v) := \min\{d > 0 \mid \text{there is an } f \in F[V]_d^G \text{ such that } f(v) \neq 0\}$$

is bounded above by the group order $|G|$, and hence so is the supremum $\gamma(G,V)$ of the $\epsilon(G,v)$ taken over all $v \in V\backslash\{0\}$. There has been a recent interest in this number, see [5, 7, 8]. In [7], another related number $\delta(G,V)$ is introduced, which is defined to be zero if $V^G = \{0\}$ and otherwise as the supremum of all $\epsilon(G,v)$ taken over all nonzero *fixed* points $v \in V^G\backslash\{0\}$. We propose the name *degree of reductivity* for $\delta(G,V)$. Note that a group G is called reductive, if for every V and every $v \in V^G\backslash\{0\}$, there exists a homogeneous positive degree invariant $f \in F[V]_+^G$ such that $f(v) \neq 0$, hence the suggested name. It was shown in [7], that $\delta(G)$, the supremum of the $\delta(G,V)$ taken over all V, equals the size of a Sylow-p subgroup of G. The goal of this paper is to give more precise information on $\delta(G,V)$ and compute it explicitly for several classes of modular groups (i.e. $|G|$ is divisible by p) and representations. In Sec. 1, we show that for a cyclic p-group G and every faithful G-module V, we have $\delta(G,V) = |G|$. In that situation we compute $\epsilon(G,v)$ for every $v \in V^G\backslash\{0\}$ as well. The most important stepstone that we lay to our main results is a restriction of the degrees of certain monomials that appear in invariant polynomials. We think that this restriction can also be useful for further studies targeting the generation of the invariant ring. In Sec. 2, we consider an abelian p-group G and show that the maximal size of a cyclic subgroup of G is a lower bound for $\delta(G,V)$ for every faithful G-module V. We also work out the Klein four group and compute the δ- and γ-values for all its representations. It turns out that our lower bound is sharp for a large number of these representations. In Sec. 3, we deal with groups whose order is divisible by p only once and put a squeeze on the δ-values of the representations of these groups.

For a general reference for invariant theory we refer the reader to [1, 4, 6, 13].

1. Modular Cyclic Groups

Let $G = Z_{p^r}$ be the cyclic group of order p^r. Fix a generator σ of G. It is well known that there are exactly p^r indecomposable G-modules $V_1, \ldots, V_{p^r}$ over F, and each indecomposable module V_i is afforded by σ^{-1} acting via a Jordan block of dimension i with ones on the diagonal. Let V be an arbitrary G-module over F. Write

$$V = \bigoplus_{j=1}^{k} V_{n_j} \quad (\text{with } 1 \leq n_j \leq p^r \text{ for all } j),$$

where each V_{n_j} is spanned as a vector space by $e_{1,j}, \ldots, e_{n_j,j}$. Then the action of σ^{-1} is given by $\sigma^{-1}(e_{i,j}) = e_{i,j} + e_{i+1,j}$ for $1 \leq i < n_j$ and $\sigma^{-1}(e_{n_j,j}) = e_{n_j,j}$. Note that the fixed point space V^G is F-linearly spanned by $e_{n_1,1}, \ldots, e_{n_k,k}$. The dual $V_{n_j}^*$ is isomorphic to V_{n_j}. Let $x_{1,j}, \ldots, x_{n_j,j}$ denote the corresponding dual basis, then we have

$$F[V] = F[x_{i,j} \,|\, 1 \leq i \leq n_j, 1 \leq j \leq k],$$

and the action of σ is given by $\sigma(x_{i,j}) = x_{i,j} + x_{i-1,j}$ for $1 < i \leq n_j$ and $\sigma(x_{1,j}) = x_{1,j}$ for $1 \leq j \leq k$. We call the $x_{n_j,j}$ for $1 \leq j \leq k$ *terminal variables*. Set $\Delta = \sigma - 1$. Notice that $\Delta(x_{i,j}) = x_{i-1,j}$ if $i \geq 2$ and $\Delta(x_{1,j}) = 0$. Since $\Delta(f) = 0$ for $f \in F[V]^G$, and Δ is an additive map, we have the following, see also the discussion in [12, before Lemma 1.4].

Lemma 1. *Let $f \in F[V]^G$ and M be a monomial that appears in f. If a monomial M' appears in $\Delta(M)$, then there is another monomial $M'' \neq M$ that appears in f such that M' appears in $\Delta(M'')$ as well.*

We say that a monomial M lies above M' if M' appears in $\Delta(M)$. We will use the well-known Lucas Theorem on binomial coefficients modulo a prime in our computations (see [9] for a short proof).

Lemma 2 (Lucas Theorem). *Let s, t be integers with base-p-expansions $t = c_m p^m + c_{m-1}p^{m-1} + \cdots + c_0$ and $s = d_m p^m + d_{m-1}p^{m-1} + \cdots + d_0$, where $0 \leq c_i$, $d_i \leq p-1$ for $0 \leq i \leq m$. Then $\binom{t}{s} \equiv \prod_{0 \leq i \leq m} \binom{c_i}{d_i}$ mod p.*

The following lemma is the main technical stepstone for the rest of the paper.

Lemma 3. *For $0 \leq s \leq r$, define*

$$J_s = \{j \in \{1, \ldots, k\} \,|\, n_j > p^{s-1}\}.$$

Let $M = \prod_{1 \leq j \leq k} x_{n_j,j}^{a_j}$ be a monomial consisting only of terminal variables that appears in an invariant polynomial with nonzero coefficient. Then p^s divides a_j for all $j \in J_s$.

Proof. As the case $s = 0$ is trivial, we will assume $s \geq 1$ from now. Let $f \in F[V]^G$ be an invariant polynomial in which M appears with a nonzero coefficient, and $j \in J_s$. Without loss of generality, we assume $j = 1$ and $a_1 \neq 0$. Set $M' = \prod_{2 \leq j \leq k} x_{n_j,j}^{a_j}$. For simplicity we denote a_1 with a. Then $M = x_{n_1,1}^a M'$, and the claim is $p^s \,|\, a$. We proceed by induction on s and at each step we verify the claim for all r such that $s \leq r$. Assume $s = 1$ and $r \geq 1 = s$. By way of contradiction, we assume $p \nmid a$. Then we can write $a = c_1 p + c_0$, where c_1 and c_0 are non-negative integers with $1 \leq c_0 < p$. We have $\sigma(M) = \sigma(x_{n_1,1}^a)\sigma(M')$ and $\sigma(x_{n_1,1}^a) = (x_{n_1,1} + x_{n_1-1,1})^a$. Since M' appears in $\sigma(M')$ with coefficient one, it follows that the coefficient of $x_{n_1-1,1}x_{n_1,1}^{a-1}M'$ in $\sigma(M)$ is $\binom{a}{1} = a \equiv c_0 \not\equiv 0 \mod p$. Therefore $x_{n_1-1,1}x_{n_1,1}^{a-1}M'$ appears in $\sigma(M) - M = \Delta(M)$. As $M = x_{n_1,1}^a M'$ only consists of terminal variables, it can be seen easily that it is the only monomial lying above $x_{n_1-1,1}x_{n_1,1}^{a-1}M'$, which is a contradiction by Lemma 1.

Next assume that $s > 1$ and let $r \geq s$ be arbitrary. Note that the induction hypothesis is that the assertion holds for every pair r', s' with $1 \leq s' \leq r'$ and

$s' < s$. Consider the base-p-expansion $a = c_l p^l + c_{l-1}p^{l-1} + \cdots + c_0 p^0$ of a where $0 \leq c_l, \ldots, c_0 \leq p-1$. Let t denote the smallest integer such that $c_t \neq 0$. We claim that $p^s \,|\, a$, which is equivalent to $t \geq s$. By way of contradiction assume $t < s$. Define $b = a - p^t$. Then the base-p-expansion of b is $c_l p^l + \cdots c_{t+1}p^{t+1} + (c_t - 1)p^t + 0 \cdot p^{t-1} + \cdots + 0 \cdot p^0$. As in the basis case, we see that the coefficient of $x_{n_1-1,1}^{p^t} x_{n_1,1}^{a-p^t} M'$ in $\sigma(M) = (x_{n_1,1} + x_{n_1-1,1})^a \sigma(M')$ is $\binom{a}{p^t}$. By the Lucas Theorem, $\binom{a}{p^t} \equiv \binom{c_t}{1} = c_t \not\equiv 0 \mod p$. So $x_{n_1-1,1}^{p^t} x_{n_1,1}^{a-p^t} M'$ appears in $\Delta(M)$. By Lemma 1 there exists another monomial M'' in f that lies above $x_{n_1-1,1}^{p^t} x_{n_1,1}^{a-p^t} M'$. We have $M'' = x_{n_1-1,1}^{d} x_{n_1,1}^{a-d} M'$ for some $1 \leq d < p^t$. Since $a - p^t < a - d < a$ and p^t divides a it follows that

$$p^t \text{ does not divide } a - d. \qquad (*)$$

Let H denote the subgroup of G generated by σ^p. Note that $H \cong Z_{p^{r-1}}$ and consider V_{n_1} as an H-module. From $\sigma^p - 1 = (\sigma - 1)^p$ it follows that V_{n_1} decomposes into p indecomposable H-modules such that $x_{n_1,1}, x_{n_1-1,1}, \ldots, x_{n_1-p+1,1}$ become terminal variables with respect to the H-action. Note that by assumption, $r \geq s \geq 2$ and as $1 = j \in J_s$, we have $n_1 > p^{s-1} \geq p$. Also the $H(\cong Z_{p^{r-1}})$-module generated by $x_{n_1,1}$ has dimension $\lceil \frac{n_1}{p} \rceil > p^{s-2}$. Therefore the monomial $M'' = x_{n_1,1}^{a-d} \cdot x_{n_1-1,1}^{d} M'$ appearing in $f \in F[V]^G \subseteq F[V]^H$ consists only of terminal variables with respect to the $H(\cong Z_{p^{r-1}})$-action and $x_{n_1,1}$ is a terminal variable whose index would appear in the set J'_{s-1} corresponding to the considered $H(\cong Z_{p^{r-1}})$-action. Therefore, the induction hypothesis (with $s' = s-1$ and $r' = r-1$) applied to M'' yields $p^{s-1} | a-d$. As we have assumed $t < s$, it follows that p^t divides $a - d$, which is a contradiction to $(*)$ above. $\square$

With this lemma we can precisely compute the degree required to separate a nonzero fixed point from zero.

Theorem 4. *Let $v = \sum_{1 \leq j \leq k} c_j e_{n_j,j} \in V^G \backslash \{0\}$ be a nonzero fixed point, where $c_1, \ldots, c_k \in F$. Let J denote the set of all $j \in \{1, \ldots, k\}$ such that $c_j \neq 0$, and s denote the maximal integer such that $p^{s-1} < n_j$ for all $j \in J$. Then $\epsilon(G, v) = p^s$.*

In particular, if V is a faithful G-module, then $\delta(G, V) = p^r$.

Proof. Any homogeneous invariant polynomial of positive degree that is nonzero on v must contain a monomial M with a nonzero coefficient in the variables of the set $\{x_{n_j,j} \,|\, j \in J\}$. With s as defined above, by the previous lemma the exponents of the $x_{n_j,j}$ in M are divisible by p^s for all $j \in J \subseteq J_s$. Hence $\epsilon(G, v) \geq p^s$, so it remains to prove the reverse inequality. The maximality condition on s implies the existence of a $j' \in J$ such that $p^{s-1} < n_{j'} \leq p^s$. Then the Jordan block representing the action of σ on $x_{1,j'}, \ldots, x_{n_{j'},j'}$ has order p^s, and so the orbit product $N = \prod_{m \in Gx_{n_{j'},j'}} m \in F[V]_+^G$ is an invariant homogeneous polynomial of degree p^s. Furthermore, for every $\sigma \in G$ and the corresponding element $m = \sigma(x_{n_{j'},j'}) \in Gx_{n_{j'},j'}$ in the orbit, we have $m(v) = (\sigma(x_{n_{j'},j'}))(v) = x_{n_{j'},j'}(\sigma^{-1}v) = x_{n_{j'},j'}(v) = c_{j'}$, where we used $v \in V^G$. Hence, $N(v) = c_{j'}^{p^s} \neq 0$, which shows $\epsilon(G,v) \leq p^s$.

For the final statement, note that if V is a faithful G-module, then there is a $j' \in \{1,\dots,k\}$ satisfying $p^{r-1} < n_{j'} \leq p^r$. Now for $v = e_{n_{j'},j'} \in V^G \backslash \{0\}$, in the notation above we have $J = \{j'\}$ and $s = r$, so the first part yields $\epsilon(G,v) = p^r = |G|$. It follows $\delta(G,V) = |G|$ as claimed. □

We now consider the general modular cyclic group $\tilde{G} = Z_{p^r m}$, where m is a non-negative integer with $(p,m) = 1$. Let G and N be the subgroups of $\tilde{G}$ of order p^r and m, respectively. Fix a generator σ of G and a generator α of N. For every $1 \leq n \leq p^r$ and an mth root of unity $\lambda \in F$, there is an n-dimensional $\tilde{G}$-module $W_{n,\lambda}$ with basis $e_1, e_2, \dots, e_n$ such that $\sigma^{-1}(e_i) = e_i + e_{i+1}$ for $1 \leq i \leq n-1$, $\sigma^{-1}(e_n) = e_n$ and $\alpha(e_i) = \lambda e_i$ for $1 \leq i \leq n$. It is well-known that the $W_{n,\lambda}$ form the complete list of indecomposable $\tilde{G}$-modules, see [10, Lemma 3.1] for a proof.

Notice that the indecomposable module $W_{n,\lambda}$ is faithful if and only if $p^{r-1} < n \leq p^r$ and λ is a primitive mth root of unity. Let $x_1, \dots, x_n$ denote the corresponding basis for $W_{n,\lambda}^*$. We have an isomorphism $W_{n,\lambda}^* \cong W_{n,\lambda^{-1}}$, where the action of σ on $x_1, \dots, x_n$ is given by an upper diagonal Jordan block. Note that if $\lambda \neq 1$, we have $W_{n,\lambda}^{\tilde{G}} = \{0\}$, and so $\delta(\tilde{G}, W_{n,\lambda}) = 0$.

Proposition 5. *Let $\tilde{G} = Z_{p^r m}$ and $W_{n,\lambda}$ be a faithful indecomposable $\tilde{G}$-module, i.e. $p^{r-1} < n \leq p^r$ and $\lambda \in F$ is a primitive mth root of unity. Then $\gamma(\tilde{G}, W_{n,\lambda}) = |\tilde{G}| = p^r m$.*

Proof. Let $f \in F[W_{n,\lambda}]_+^{\tilde{G}}$ be a homogeneous invariant of positive degree d such that $f(e_n) \neq 0$. Then f contains the monomial x_n^d with a nonzero coefficient. Considered as a G-module, $W_{n,\lambda}$ is isomorphic to the indecomposable G-module V_n. Since f is particularly G-invariant, we get from Lemma 3 that p^r divides d. As f is also α-invariant, and α acts just by multiplication with λ^{-1} on every variable, it follows that x_n^d is α-invariant, hence we have $\lambda^d = 1$. As λ is a primitive mth root of unity, it follows that m divides d. Since p^r and m are coprime we get that $p^r m$ divides d. Therefore $\gamma(\tilde{G}, W_{n,\lambda}) \geq \epsilon(\tilde{G}, e_n) \geq p^r m = |\tilde{G}|$. The reverse inequality always holds by Dade's hsop algorithm. □

Now let $1 \leq n \leq p^r$ be arbitrary and $\lambda \in F$ be an arbitrary mth root of unity. Define $0 \leq s \leq r$ such that $p^{s-1} < n \leq p^s$ and let m' denote the order of λ as an element of the multiplicative group $F^\times$ (then $m' \mid m$). Then $W_{n,\lambda}$ can be considered as a faithful $Z_{p^s m'}$-module, hence the result above yields $\gamma(\tilde{G}, W_{n,\lambda}) = |Z_{p^s m'}| = p^s m'$. As the γ-value of a direct sum of modules is the maximum of the γ-values of the summands (see for example [7, Proposition 3.3]), the proposition above allows to compute $\gamma(\tilde{G}, V)$ for every $\tilde{G}$-module. This precises the result of [7, Corollary 4.2], which states $\gamma(\tilde{G}) = |\tilde{G}|$. As an interesting example, take again λ a primitive mth root of unity and consider the $\tilde{G}$-module $V := W_{p^r,1} \oplus W_{1,\lambda}$. Note that though V

is a faithful $\tilde{G}$-module, we get from the above

$$\gamma(\tilde{G}, V) = \max\{\gamma(\tilde{G}, W_{p^r,1}), \gamma(\tilde{G}, W_{1,\lambda})\} = \max\{p^r, m\}$$

which is strictly smaller than $|\tilde{G}| = p^r m$ if $r > 0$ and $m > 1$.

2. Modular Abelian p-Groups

Before we focus on abelian p-groups, we start with a more general lemma.

Lemma 6. *Let $\tilde{G}$ be a p-group, V a faithful $\tilde{G}$-module and let $\sigma \in \tilde{G}$ be of order p^r such that $\sigma^{p^{r-1}} \in Z(\tilde{G})$ (the center of $\tilde{G}$). Then $\delta(\tilde{G}, V) \geq p^r$.*

Proof. Let G denote the subgroup of $\tilde{G}$ generated by σ. We follow the notation of the previous section and consider the decomposition $V = \bigoplus_{j=1}^{k} V_{n_j}$ of V as a G-module. Since V is also faithful as G-module, we have $J := J_r = \{j \in \{1, \ldots, k\} \,|\, n_j > p^{r-1}\} \neq \emptyset$. We can choose a suitable basis of V such that σ^{-1} acts on this basis via sums of Jordan blocks of dimensions $n_1, \ldots, n_k$. Set $\Gamma = \sigma^{-1} - 1$. Let W denote the image of the map $\Gamma^{p^{r-1}}$ on V. Since $\sigma^{p^{r-1}} \in Z(\tilde{G})$, we have that $\Gamma^{p^{r-1}}$ commutes with every $\tau \in \tilde{G}$, hence W is a $\tilde{G}$-module. We also have $W \subseteq \bigoplus_{j \in J} V_{n_j}$ because $\Gamma^{p^{r-1}} V_{n_j} = \{0\}$ if $n_j \leq p^{r-1}$. On the other hand, $\Gamma^{p^{r-1}} V_{n_j}$ is spanned by $e_{p^{r-1}+1,j}, e_{p^{r-1}+2,j}, \ldots, e_{n_j,j}$ for $n_j > p^{r-1}$. But $J \neq \emptyset$, so we get that $W \neq \{0\}$ and in particular $e_{n_j,j} \in W$ for $j \in J$. Hence W^G is spanned F-linearly by $\{e_{n_j,j} \,|\, j \in J\}$. Moreover, since every modular action of a p-group on a nonzero module has a non-trivial fixed point, we have

$$\{0\} \neq W^{\tilde{G}} \subseteq W^G = \langle \{e_{n_j,j} \,|\, j \in J\} \rangle.$$

Choose any nonzero vector $v \in W^{\tilde{G}} \subseteq V^{\tilde{G}}$. As v is in the span of $\{e_{n_j,j} \,|\, j \in J\}$, every homogeneous polynomial $f \in F[V]^{\tilde{G}} \subseteq F[V]^G$ of positive degree that is nonzero on v must contain a monomial with nonzero coefficient in the variables $\{x_{n_j,j} \,|\, j \in J\}$. Since f is also G-invariant, Lemma 3 applies and we get that the exponents of these variables in this monomial are all divisible by p^r. It follows $\delta(\tilde{G}, V) \geq \epsilon(\tilde{G}, v) \geq p^r$ as desired. $\square$

In the following two examples, F is an algebraically closed field of characteristic 2.

Example 7. Consider the dihedral group $D_{2^{r+1}} = \langle \sigma, \rho \rangle$ of order 2^{r+1} with relations $\mathrm{ord}(\sigma) = 2$, $\mathrm{ord}(\rho) = 2^r$ and $\sigma\rho\sigma^{-1} = \rho^{-1}$. Then $\rho^{2^{r-1}} \in Z(D_{2^{r+1}})$. Hence the lemma applies, and for every faithful $D_{2^{r+1}}$-module V we have $\delta(D_{2^{r+1}}, V) \geq 2^r$.

Example 8. Consider the quaternion group Q of order 8. There is an element $\sigma \in Q$ of order 4 such that $\sigma^2 \in Z(Q)$. From the lemma it follows that for every faithful Q-module V, we have $\delta(Q, V) \geq 4$.

Example 9. Consider the non-abelian group

$$T_p := \left\{ \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{0} & \overline{1} \end{pmatrix} \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^{2\times 2} \,\middle|\, a, b \in \mathbb{Z}, a \equiv 1 \bmod p \right\}$$

of order p^3 (where we write $\overline{a} := a + p^2\mathbb{Z}$). Note that $T_2 \cong D_8$. The element $\sigma := \left(\begin{smallmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{smallmatrix}\right) \in T_p$ is of order p^2, and it can be checked easily that $\sigma^p \in Z(T_p)$. From the lemma it follows that for every faithful T_p-module V, we have $\delta(T_p, V) \geq p^2$.

Recall that for a group $\tilde{G}$, the exponent $\exp(\tilde{G})$ of $\tilde{G}$ is the least common multiple of the orders of its elements. In particular for an abelian group, the exponent is the maximal order of an element. As a corollary of the above lemma, we get the following.

Theorem 10. *Let $\tilde{G}$ be a non-trivial p-group. Then for every faithful $\tilde{G}$-module V we have*

$$\delta(\tilde{G}, V) \geq \exp(Z(\tilde{G})) \geq p.$$

If $\tilde{G}$ is an abelian p-group, we particularly have

$$\delta(\tilde{G}, V) \geq \exp(\tilde{G}) \geq p.$$

Proof. First note that for p-groups, its center is non-trivial, so particularly we have $\exp(Z(\tilde{G})) \geq p$. Now chose an element $\sigma \in Z(\tilde{G})$ of maximal order $p^r = \exp(Z(\tilde{G}))$. Then Lemma 6 applies and yields $\delta(\tilde{G}, V) \geq p^r = \exp(Z(\tilde{G}))$. Finally, if $\tilde{G}$ is an abelian p-group, we have $\tilde{G} = Z(\tilde{G})$. □

For a recent related study of the invariants of abelian p-groups we refer the reader to [3]. We also remark that the inequality in Theorem 10 is sharp, see Theorem 15.

The Klein four group. Let $\tilde{G}$ denote the Klein four group with generators σ_1 and σ_2, and F an algebraically closed field of characteristic 2. The goal of this section is to compute the δ- and γ-value of every $\tilde{G}$-module (in all cases, both numbers are equal here). We first give the δ/γ-value for each indecomposable representation of the Klein four group. The complete list of indecomposable representations is for example given in [2, Theorem 4.3.3]. There, the indecomposable representations are classified in five types (i)–(v), and we will use the same enumeration. For the notation of the modules, we follow [10] but note that there types (iv) and (v) are interchanged. The first **type (i)** is just the regular representation $V_{\mathrm{reg}} := F\tilde{G}$, and here we have $\delta(\tilde{G}, V_{\mathrm{reg}}) = \gamma(\tilde{G}, V_{\mathrm{reg}}) = 4 = |\tilde{G}|$ by [7, Theorem 1.1 and Proposition 2.4].

The **type (ii)** representations $V_{2m,\lambda}$ are parameterized by a positive integer m and $\lambda \in F$. Then $V_{2m,\lambda}$ is defined as the $2m$-dimensional representation spanned by $e_1, \ldots, e_m$, $h_1, \ldots, h_m$ such that the action is given by $\sigma_i(e_j) = e_j$, $\sigma_1(h_j) = h_j + e_j$ for $i = 1, 2$ and $j = 1, \ldots, m$, $\sigma_2(h_j) = h_j + \lambda e_j + e_{j+1}$ for $1 \leq j < m$ and

$\sigma_2(h_m) = h_m + \lambda e_m$. Let $x_1, \ldots, x_m, y_1, \ldots, y_m$ be the elements of $V^*_{2m,\lambda}$ corresponding to $h_1, \ldots, h_m, e_1, \ldots, e_m$. Then we have $\sigma_i(x_j) = x_j$, $\sigma_1(y_j) = y_j + x_j$ for $i = 1, 2$ and $j = 1, \ldots, m$, $\sigma_2(y_1) = y_1 + \lambda x_1$ and $\sigma_2(y_j) = y_j + \lambda x_j + x_{j-1}$ for $1 < j \leq m$.

Lemma 11. *In the notation as above, we have that* $\delta(\tilde{G}, V_{2,\lambda}) = \gamma(\tilde{G}, V_{2,\lambda})$ *equals* 2 *if* $\lambda \in \{0, 1\}$, *and it equals* 4 *if* $\lambda \in F \backslash \{0, 1\}$.

Proof. If $\lambda \in \{0, 1\}$, the corresponding matrix group is of order 2, and the result follows easily. If $\lambda \in F \backslash \{0, 1\}$ it follows from [6, Theorem 3.7.5] that $F[V_{2,\lambda}]^{\tilde{G}}$ is generated by x_1 and the norm $N_{\tilde{G}}(y_1)$, as those two invariants form an hsop and the product of their degrees equals the group order 4. Now the claim follows easily. $\square$

Proposition 12. *In the notation as above, we have* $\delta(\tilde{G}, V_{2m,\lambda}) = \gamma(\tilde{G}, V_{2m,\lambda}) = 4$ *for all* $m \geq 2$ *and* $\lambda \in F$.

Proof. We have $\delta(\tilde{G}, V_{2m,\lambda}) \leq \gamma(\tilde{G}, V_{2m,\lambda}) \leq 4$, from Dade's hsop algorithm, hence it is enough to show $\delta(\tilde{G}, V_{2m,\lambda}) \geq 4$. Consider the point $e_m \in V^{\tilde{G}}_{2m,\lambda} \backslash \{0\}$. Any homogeneous invariant $f \in F[V_{2m,\lambda}]^{\tilde{G}}_d$ of positive degree d separating e_m from zero must contain y_m^d. Lemma 13 implies $d \geq 4$, so $\delta(\tilde{G}, V_{2m,\lambda}) \geq \epsilon(\tilde{G}, e_m) \geq 4$, finishing the proof. $\square$

Set $\Delta_i = \sigma_i - 1$ for $i = 1, 2$. Since $\Delta_i(f) = 0$ for every polynomial $f \in F[V]^{\tilde{G}}$, the assertion of Lemma 1 holds for $\Delta = \Delta_i$ for $i = 1, 2$. We say that a monomial M lies above the monomial M' with respect to Δ_i if M' appears in $\Delta_i(M)$.

Lemma 13. *Assume that* $V = V_{2m,\lambda}$ *with* $m \geq 2$. *Then* y_m^d *does not appear in a polynomial in* $F[V]^{\tilde{G}}$ *for* $1 \leq d \leq 3$.

Proof. Assume that y_m^d appears in $f \in F[V]^{\tilde{G}}$. Since $\{x_m, y_m\}$ spans a two-dimensional indecomposable summand as a $\langle \sigma_1 \rangle$-module, Lemma 3 applies and we get that d is divisible by 2. Assume on the contrary that $d = 2$. Then $\sigma_1(y_m^2) = y_m^2 + x_m^2$. So x_m^2 appears in $\Delta_1(y_m^2)$. Since $y_m x_m$ is the only other monomial in $F[V]$ that lies above x_m^2 with respect to Δ_1 we get that $y_m x_m$ appears in f as well. Moreover since the coefficient of x_m^2 in $\Delta_1(y_m^2)$ and $\Delta_1(y_m x_m)$ is one, it follows that the coefficients of y_m^2 and $y_m x_m$ in f are equal. Call this nonzero coefficient c. Then the coefficient of x_m^2 in $\Delta_2(c y_m^2 + c y_m x_m)$ is $c(\lambda^2 + \lambda)$. Since y_m^2 and $y_m x_m$ are the only monomials in $F[V]$ that lie above x_m^2 with respect to Δ_2, we get that $\Delta_2(f) \neq 0$ if $\lambda \neq 0, 1$, giving a contradiction. Next assume that $\lambda = 0$. Then, since $y_m x_m$ appears in f and $\sigma_2(y_m x_m) = (y_m + x_{m-1}) x_m$ we get that $x_{m-1} x_m$ appears in $\Delta_2(y_m x_m)$. This gives a contradiction by Lemma 1 again because $y_m x_m$ is the only monomial that lies above $x_{m-1} x_m$ with respect to Δ_2.

Finally, we note that the cases $\lambda = 1$ and $\lambda = 0$ correspond to the same matrix group and so their invariants are the same. $\square$

The **type (iii)** representations W_{2m} are $2m$-dimensional representations ($m \geq 1$) which are obtained from $V_{2m,0}$ just by interchanging the actions of σ_1 and σ_2. In particular, W_{2m} and $V_{2n,0}$ have the same invariant ring, so we get as a corollary from Lemma 11 and Proposition 12 that $\delta(\tilde{G}, W_2) = \gamma(\tilde{G}, W_2) = 2$ and $\delta(\tilde{G}, W_{2m}) = \gamma(\tilde{G}, W_{2m}) = 4$ for all $m \geq 2$.

The **type (iv)** representations V_{2m+1} for $m \geq 1$ are $(2m+1)$-dimensional representations. (Note that in [10], these representations are listed as type (v).) They are linearly spanned by $e_1, \ldots, e_m, h_1, \ldots, h_{m+1}$, where $\sigma_i(e_j) = e_j$ for $i = 1, 2$ and $1 \leq j \leq m$, $\sigma_1(h_i) = h_i + e_i$ for $1 \leq i \leq m$, $\sigma_1(h_{m+1}) = h_{m+1}$, $\sigma_2(h_1) = h_1$, and $\sigma_2(h_i) = h_i + e_{i-1}$ for $2 \leq i \leq m+1$. Let $x_1, \ldots, x_{m+1}, y_1, \ldots, y_m$ be the elements of V^*_{2m+1} corresponding to $h_1, \ldots, h_{m+1}, e_1, \ldots, e_m$. Then we have $\sigma_i(x_j) = x_j$ for $i = 1, 2$ and $1 \leq j \leq m+1$, $\sigma_1(y_j) = y_j + x_j$ and $\sigma_2(y_j) = y_j + x_{j+1}$ for $1 \leq j \leq m$.

Proposition 14. *We have $\delta(\tilde{G}, V_{2m+1}) = \gamma(\tilde{G}, V_{2m+1}) = 4$ for all $m \geq 1$.*

Proof. Again by Dade's hsop-algorithm, we have $\delta(\tilde{G}, V_{2m+1}) \leq \gamma(\tilde{G}, V_{2m+1}) \leq 4$. Consider the point $e_m \in V_{2m+1}^{\tilde{G}}$, and let $f \in F[V_{2m+1}]^{\tilde{G}}$ be homogeneous of minimal positive degree d such that $f(e_m) \neq 0$. Then y_m^d must appear in f with a nonzero coefficient. Since $\{x_m, y_m\}$ spans a two-dimensional indecomposable summand as a $\langle\sigma_1\rangle$-module and f is also $\langle\sigma_1\rangle$-invariant, Lemma 3 applies and we get that d is divisible by 2. By [12, Proposition 5.8.3], y_m^2 does not appear in a $\tilde{G}$-invariant polynomial. It follows $d \geq 4$, so we are done. $\square$

The **type (v)** representations W_{2m+1} for $m \geq 1$ are $(2m+1)$-dimensional representations. (Note that in [10], these representations are given as type (iv).) They are afforded by $\sigma_1 \mapsto \left(\begin{array}{c|c} I_{m+1} & \begin{array}{c} I_m \\ \hline 0_{1\times m} \end{array} \\ \hline 0 & I_m \end{array}\right)$ and $\sigma_2 \mapsto \left(\begin{array}{c|c} I_{m+1} & \begin{array}{c} 0_{1\times m} \\ \hline I_m \end{array} \\ \hline 0 & I_m \end{array}\right)$, where $0_{k\times l}$ denotes a $k \times l$ matrix whose entries are all zero. In [12, Sec. 4] (with notation $F[W_{2m+1}] =: F[y_1, \ldots, y_{m+1}, x_1, \ldots, x_m]$), an hsop consisting of invariants of degree at most 2 is given for $F[W_{2m+1}]^{\tilde{G}}$. As the δ-value is clearly not one, it follows $\delta(\tilde{G}, W_{2m+1}) = \gamma(\tilde{G}, W_{2m+1}) = 2$ for all $m \geq 1$.

Theorem 15. *Let V be a non-trivial representation of the Klein four group $\tilde{G}$ over an algebraically closed field of characteristic* 2, *and consider its decomposition into indecomposable summands. Then $\delta(\tilde{G}, V) = \gamma(\tilde{G}, V) = 2$ if and only if every non-trivial indecomposable summand is isomorphic to one of $V_{2,0}$, $V_{2,1}$, W_2 or W_{2m+1} $(m \geq 1)$. If another non-trivial indecomposable summand appears, then $\delta(\tilde{G}, V) = \gamma(\tilde{G}, V) = 4$.*

Proof. The δ/γ-value of a direct sum equals the maximal δ/γ-value of a summand (see [7, Proposition 2.2/Proposition 3.3]), so the theorem follows from the values for the indecomposable modules above. $\square$

3. Groups of Order with Simple Prime Factor p

In this section, we first note that $\delta(G, V)$ can only take the values 0, 1 or p if G is a group of order pm, where m is relatively prime to p. Then we demonstrate how the precise value is determined by the fixed point spaces of V and V^*.

Lemma 16. *Let G be a group of order $|G| = pm$ such that p, m are coprime. Then for a G-module V, we have $\delta(G, V) \in \{0, 1, p\}$.*

Proof. By [8, Corollary 2.2] (which is essentially a reformulation of a result of Nagata and Miyata [11]), $\delta(G, V)$ is 0, 1, or divisible by p. As $\delta(G)$ is the size of a sylow-p-subgroup of G by [7, Theorem 1.1], we also have $\delta(G, V) \leq \delta(G) = p$. It follows $\delta(G, V) \in \{0, 1, p\}$. □

For any G-module V, define

$$V_0 := \{v \in V \mid f(v) = 0 \text{ for all } f \in F[V]_1^G = (V^*)^G\} = \mathcal{V}((V^*)^G).$$

Clearly, V_0 is a G-submodule of V, because if $v \in V_0$, $\sigma \in G$ and $f \in F[V]_1^G$ we have $f(\sigma v) = f(v) = 0$, hence $\sigma v \in V_0$.

Lemma 17. *For a G-module V, we have*

$$\delta(G, V) = 1 \Leftrightarrow V^G \neq \{0\} \quad \textit{and} \quad V^G \cap V_0 = \{0\}.$$

Proof. Assume that $\delta(G, V) = 1$. Then clearly $V^G \neq \{0\}$, because otherwise $\delta(G, V) = 0$ by definition. Take $v \in V^G \cap V_0$. If $v \neq 0$, we would have $\epsilon(G, v) = 1$, hence there would be an $f \in F[V]_1^G$ such that $f(v) \neq 0$, a contradiction to $v \in V_0$. Hence $V^G \cap V_0 = \{0\}$.

Conversely, take a $v \in V^G \backslash \{0\}$. By assumption, $v \notin V_0$, hence there is an $f \in F[V]_1^G$ such that $f(v) \neq 0$. Therefore, $\epsilon(G, v) = 1$ for all $v \in V^G \backslash \{0\}$ and the claim follows. □

Proposition 18. *Let G be a group of order $|G| = pm$ such that p, m are coprime. Then for a G-module V, we have*

$$\delta(G, V) = \begin{cases} 0 & \textit{if } V^G = \{0\}, \\ 1 & \textit{if } V^G \neq \{0\} \textit{ and } V^G \cap V_0 = \{0\}, \\ p & \textit{otherwise.} \end{cases}$$

Proof. This is immediate from the previous couple of lemmas. □

The benefit of this proposition is that only V^G and $(V^*)^G$ need to be known in order to compute $\delta(G, V)$, but not generators of the full invariant ring $F[V]^G$.

Example 19. Let $G \subseteq S_p$ be any subgroup of order divisible by p. Then G contains an element of order p, i.e. a p-cycle. Consider the natural action of G on $V := F^p$.

Clearly, $V^G = \langle (1,1,\dots,1)\rangle \subseteq V_0 = \mathcal{V}(x_1+\cdots+x_p)$. The proposition implies that $\delta(G,V)=p$.

Example 20. Consider the group

$$G = \left\{ \sigma_{a,b} := \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \in \mathbb{F}_p^{2\times 2} \,\middle|\, a,b\in\mathbb{F}_p, b\neq 0 \right\}$$

of order $|G| = p(p-1)$. Then G acts naturally by left multiplication on the module $W := \langle X, Y\rangle := F^2$ with basis $\{X, Y\}$, i.e. $\sigma_{a,b}(X) = X$ and $\sigma_{a,b}(Y) = aX + bY$ for all $\sigma_{a,b}\in G$. Consider the nth symmetric power

$$V_n := S^n(W) = \langle e_0 := X^n, e_1 := X^{n-1}Y, \dots, e_n := Y^n\rangle$$

with basis $\{e_0,\dots,e_n\}$. From

$$\sigma_{a,b}(e_j) = \sigma_{a,b}(X^{n-j}Y^j) = X^{n-j}(aX+bY)^j = \sum_{i=0}^{j}\binom{j}{i}a^{j-i}b^iX^{n-i}Y^i$$

$$= \sum_{i=0}^{j}\binom{j}{i}a^{j-i}b^ie_i$$

we see that for $j=1,\dots,n$, the coefficient of e_{j-1} in $\sigma_{a,b}(e_j)$ is given by $\binom{j}{j-1}ab^{j-1} = jab^{j-1}$, which is nonzero if $a=b=1$ and $n<p$. It follows that $\mathrm{rank}(\sigma_{1,1}-\mathrm{id}_{V_n}) = n-1$ if $n<p$, and hence $V_n^{\sigma_{1,1}}$ is one-dimensional and spanned by X^n. As $V_n^G\subseteq V_n^{\sigma_{1,1}}$ and X^n is also G-invariant, it follows $V_n^G = \langle X^n\rangle = \langle e_0\rangle$. Write $F[V_n] = F[z_0,\dots,z_n]$, where $z_i(e_j) = \delta_{i,j}$ (the Kronecker symbol). A similar calculation shows that $(V_n^*)^{\sigma_{1,1}} = \langle z_n\rangle$ if $n<p$, and again we have $(V_n^*)^G\subseteq (V_n^*)^{\sigma_{1,1}}$. As $\sigma_{a,b}(z_n) = b^{-n}z_n$, we see for $1\le n<p$, that z_n is G-invariant only if $n=p-1$. Hence $(V_n^*)^G = \{0\}$ for $1\le n\le p-2$ and $(V_n^*)^G = \langle z_n\rangle$ if $n=p-1$. In both cases it follows $V_n^G\subseteq\mathcal{V}((V_n^*)^G)$ and hence the proposition above implies $\delta(G,V_n)=p$ for $1\le n<p$.

Acknowledgment

Second author is supported by a Grant from Tübitak: 112T113.

References

[1] D. J. Benson, *Polynomial Invariants of Finite Groups*, London Mathematical Society Lecture Note Series, Vol. 190 (Cambridge University Press, Cambridge, 1993).

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

[3] 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**(1) (2013) 1–22.

[4] H. E. A. Campbell and D. L. Wehlau, *Modular Invariant Theory*, Encyclopaedia of Mathematical Sciences, Vol. 139, Invariant Theory and Algebraic Transformation Groups, Vol. 8 (Springer-Verlag, Berlin, 2011).

[5] K. Cziszter and M. Domokos, On the generalized Davenport constant and the Noether number, *Cent. Eur. J. Math.* **11**(9) (2013) 1605–1615.

[6] H. Derksen and G. Kemper, *Computational Invariant Theory*, Encyclopaedia of Mathematical Sciences, Vol. 130, Invariant Theory and Algebraic Transformation Groups, Vol. 1 (Springer-Verlag, Berlin, 2002).

[7] J. Elmer and M. Kohls, Zero-separating invariants for finite groups, *J. Algebra* **411** (2014) 92–113.

[8] ———, Zero-separating invariants for infinite groups, preprint (2014); http://arXiv.org/abs/1402.6608.

[9] N. J. Fine, Binomial coefficients modulo a prime, *Amer. Math. Monthly* **54** (1947) 589–592.

[10] M. Kohls and M. Sezer, Separating invariants for the Klein four group and cyclic groups, *Internat. J. Math.* **24**(6) (2013), Article ID: 1350046, 11 pp.

[11] M. Nagata and T. Miyata, Note on semi-reductive groups, *J. Math. Kyoto Univ.* **3** (1963/1964) 379–382.

[12] M. Sezer and R. J. Shank, Rings of invariants for modular representations of the Klein four group, preprint (2013); http://arXiv.org/abs/1309.7812.

[13] L. Smith, *Polynomial Invariants of Finite Groups*, Research Notes in Mathematics, Vol. 6 (A. K. Peters, Wellesley, MA, 1995).