Journal of Mathematical Research with Applications
Mar., 2024, Vol. 44, No. 2, pp. 161–169
DOI:10.3770/j.issn:2095-2651.2024.02.003
Http://jmre.dlut.edu.cn

The Noether Numbers for Cyclic Groups of pq Order in the Modular Case

Haixian CHEN
School of Mathematical Sciences, Shanxi University, Shanxi 030006*, P. R. China*

Abstract Let G be a cyclic group of order pq, where $q|p-1, q, p$ are prime numbers and let F be a field of characteristic p. Let V be a finite-dimensional G-module over F. We refer to the maximal degree of indecomposable polynomials in the invariant algebra $F[V]^G$ as the Noether number of the invariant algebra $F[V]^G$, denoted $\beta(F[V]^G)$. In this paper, we determine the Noether number of the invariant algebra $F[V]^G$. Furthermore, we prove that for such a cyclic group of order pq, Wehlau's conjecture holds.

Keywords Noether number; invariant algebra; cyclic group; modular case

MR(2020) Subject Classification 13A50

1. Introduction

Let G be a finite group and F be a field. Let V be the n-dimensional representation space of G over F. Let $x_1, x_2, \ldots, x_n$ be a basis of the dual space V^* of V. Then the action of G on V can be induced to the dual space V^* and also to the polynomial algebra $F[V] = F[x_1, x_2, \ldots, x_n]$. The set consisting of polynomials that are fixed under the action of G is the main object of study in invariant theory. This set is called the algebra of invariants, denoted as $F[V]^G$. It is the graded subalgebra of the polynomial algebra. According to Noether's classical theorem, if G is a finite group, then the invariant algebra $F[V]^G$ is finitely generated. Let the minimal generating set of the invariant algebra $F[V]^G$ be $f_1, f_2, \ldots, f_s$, thus the maximal degree of polynomials in the minimal generating set is called the Noether number of the invariant algebra $F[V]^G$, denoted by $\beta(F[V]^G)$. We call $\beta(G):=\max_V \beta(F[V]^G)$ for any finite dimensional representation V of a finite group G as the Noether number of G. Firstly, Noether proved that if the characteristic of F is zero, then $\beta(G) \leq |G|$ in [1]. Secondly, this was generalized to the case of coprime characteristic by Fleischmann [2] and Fogarty [3]. In the non-modular case, i.e., the characteristic of the field is 0 or does not divide $|G|$, mathematicians proved that the Noether number of any finite group is less than or equal to the order of the group. But in the modular case, i.e., the characteristic of the field divides $|G|$, in 1990 Richman [4] found an example to show that the Noether number is related to the dimension of the representation space and the order of the group. In 2006, Fleischmann, Sezer, Shank and Woodcock computed the Noether number for an arbitrary representation of

Received June 6, 2023; Accepted August 15, 2023
Supported by the Natural Science Foundation for Young Scientists of China (Grant No. 12101375) and the Foundation for Young Scientists of Shanxi Province (Grant No. 201901D211184).
E-mail address: hxchen@sxu.edu.cn

a cyclic group of prime order [5]. Subsequently, using the Castelnuovo-Mumford regularity and projective resolution, Symonds [6] determined an upper bound on the Noether number of a finite-dimensional nontrivial representation of a nontrivial group. It is still an open question as to whether this upper bound can be reached. Mathematicians turned to describe the relation of the Noether number between the module of a group and its submodule, and Wehlau proposed the following conjecture:

Conjecture 1.1 ([7]) If U is a G-submodule of a G-module V, then $\beta(F[U]^G) \leq \beta(F[V]^G)$.

Shank and the proposer of the conjecture proved that the conjecture holds for cyclic groups of order p (see [8]). For other finite groups, no relevant conclusions have been given.

In this paper, we determine the Noether number of any finite dimensional representation of a cyclic group of order pq and prove that Wehlau's conjecture holds for cyclic groups of order pq, where p, q are prime and $q|p-1$. For the remainder of the paper, let G be a cyclic group of order pq and a be a generating element of G, where p, q are prime and $q|p-1$. Let $P = \langle a^q \rangle$ be the Sylow p subgroup of G and $H = \langle a^p \rangle$ be the subgroup of order q of G. It is known that the group P has exactly p non-isomorphic indecomposable representations over a field of characteristic p, with the dimension of the representations being $1, 2, \ldots, p$, respectively, see [9]. Denote these indecomposable representations by $V_n, n = 1, \ldots, p$, respectively. Let $e_1, \ldots, e_n$ be a basis of V_n, then

$$a^q(e_i) = e_i + \sum_{j=1}^{n-i} (-1)^j e_{i+j}, \quad i = 1, \ldots, n-1, a^q(e_n) = e_n.$$

Suppose that $x_1, \ldots, x_n$ is a dual basis of dual space V_n^* of V_n. Then

$$a^q(x_1) = x_1, a^q(x_i) = x_i + x_{i-1}, \quad i = 2, \ldots, n.$$

It is easy to see that x_n is the generating element of V_n^* and that $V_n \cong V_n^*$. We call such an element x_n the distinguished variable. Let $\mathrm{Irr}(H)$ be the set consisting of all irreducible characters of H over the complex number field. Taking $1 \neq \chi$ to be an element of $\mathrm{Irr}(H)$, then $\mathrm{Irr}(H) = \{\chi^j | j = 0, 1, \ldots, q-1\}$. Since H is a cyclic group, the character χ^j is actually a 1-dimensional representation of H. According to [10, Proposition 1.1],

$$V_{i,j} := V_i \otimes \chi^j, \quad i = 1, \ldots, p, \ j = 0, 1, \ldots, q-1$$

are all non-isomorphic indecomposable modules of G. It can be shown that every indecomposable module of G is a cyclic module. Let V be a G-module, then $\beta(F[V]^G) = \beta(F[V \oplus mV_{1,0}]^G)$, i.e., adding trivial summands does not change the Noether number. A G-module is said to be reduced if it does not contain a copy of $V_{1,0}$ as a summand. For a nonfaithful reduced G-module V, we have $\beta(F[V]^G) = \beta(F[V]^P)$ or $\beta(F[V]^G) = \beta(F[V]^H) = q$. Therefore, it is sufficient to find the Noether number of a faithful reduced G-module V. Also note that for $i = 1, \ldots, p$; $j = 0, 1, \ldots, q-1$, $V_{i,j}^G$, the vector space of fixed points, has dimension one. Therefore, for any G-module W, $\dim(W^P)$ is the number of indecomposable summands in the decomposition of W. According to [8, Theorem 5.1], using Transfer mapping, we can get

$$\beta(F[V_{2,j}]^G) = \beta(F[V_{3,j}]^G) = pq, \quad j = 1, \ldots, q-1.$$

For other G-modules V with Noether number, we have the following conclusion.

Theorem 1.2 *Let V be a faithful reduced G-module over a field F of characteristic p and V does not contain 1-dimensional representation as a summand. Let s be the maximum dimension of the indecomposable summands of V and P be the Sylow p subgroup of G. Then*

(1) If $s = 3$ and V does not contain $V_{3,j}$ as a summand for any $j \in \{1, \dots, q-1\}$, or if $s > 3$ and V does not contain $V_{k,j}$ as a summand for any $j \in \{1, \dots, q-1\}$ and any $k \in \{4, \dots, s\}$, or if $V \cong \oplus \oplus_{t=1}^{q-1} m_t V_{2,t}$, $\sum_{t=1}^{q-1} m_t > 2$, then

$$\beta(F[V]^G) = q(\beta(F[V]^P) - 1).$$

(2) Other cases, i.e., if $V \cong V_{2,j}$ or $V \cong 2V_{2,j}$, or if $s = 3$ and at least one of the summands of V is isomorphic to $V_{3,j}$ with $j \in \{1, \dots, q-1\}$, or if $s > 3$ and at least one of summands of V is isomorphic to $V_{k,j}$ with $k \in \{4, \dots, s\}$ and $j \in \{1, \dots, q-1\}$, then

$$\beta(F[V]^G) = q\beta(F[V]^P).$$

(3) $\beta(F[V]^G) = \beta(F[V \oplus \oplus_{j=1}^{q-1} m_j V_{1,j}]^G)$.

Proof The results (1) and (2) follow from Propositions 2.3 and 3.4, respectively.

(3) Obviously, $\beta(F[V]^P) = \beta(F[V \oplus \oplus_{j=1}^{q-1} m_j V_{1,j}]^P)$. And we have

$$\beta(F[V]^G) = \begin{cases} q(\beta(F[V \oplus \oplus_{j=1}^{q-1} m_j V_{1,j}]^P) - 1), & V \in (1) \\ q\beta(F[V \oplus \oplus_{j=1}^{q-1} m_j V_{1,j}]^P), & V \in (2) \end{cases}$$

Therefore, $\beta(F[V]^G) = \beta(F[V \oplus \oplus_{j=1}^{q-1} m_j V_{1,j}]^G)$. □

Theorem 1.3 *If U is a G-submodule of a G-module V, then $\beta(F[U]^G) \le \beta(F[V]^G)$.*

Proof If V is a nonfaithful G-module, then the conclusion holds by [8, Theorem 4.2]. From Theorem 1.2 (3), we know that adding the 1-dimensional summands does not change the Noether number. Thus it is sufficient to consider the faithful reduced G-module V withnot 1-dimensional summands. If V belongs to the first case of Theorem 1.2, then the submodule U of V also belongs to the first case. Since $\beta(F[U]^P) \le \beta(F[V]^P)$, according to Theorem 1.2 (1) we have $\beta(F[U]^G) \le \beta(F[V]^G)$. If V belongs to the second case in Theorem 1.2, then the submodule U of V belongs to the first or second case. Similarly, it follows from Theorem 1.2. □

2. Upper bounds of Noether numbers

First, by [2, Theorem 3.1], we can obtain an upper bound of Noether numbers for the G-module V.

Proposition 2.1 ([2]) *Let V be a finite dimensional G-module over a field F of characteristic p. Let N be a normal subgroup of G and $|G : N|$ be mutually prime to p. Then $\beta(F[V]^G) \le |G : N|\beta(F[V]^N)$.*

To determine the upper bound on the Noether number of a G-module V, we introduce the definition of a relative Transfer mapping. Let P be a subgroup of G and V be a G-module. Define the relative Transfer mapping:

$$\mathrm{Tr}_P^G : F[V]^P \to F[V]^G,$$

$$\mathrm{Tr}_P^G(f) = \sum_{i=0}^{q-1} a^i f.$$

If $|G : P|$ is mutually prime to p, then the relative Transfer mapping is a surjection.

Since the group G is a cyclic group in this article, according to the relative Transfer mapping the generating elements of $F[V]^G$ are the a-invariant elements in $F[V]^P$. The following is based on the generating elements of $F[V]^P$ to find the polynomial with the maximal degree in $F[V]^G$. Take the faithful reduced G-module $V \cong \oplus_{t=0}^{q-1} m_t V_{2,t}$, $\sum_{t=0}^{q-1} m^t = l > 2$ as an example. Let $x_1, y_1; \dots; x_l, y_l$ be a basis of V^*. From [11, Theorem 6.3], it is known that the minimal generating elements of the invariant ring $F[V]^P$ are

$$x_i, N^P(y_i),\ i = 1, \dots, l;\ u_{ij} = x_i y_j - x_j y_i,\ 1 \le i < j \le l;$$

$$\mathrm{Tr}^P(y_1^{k_1} \dots y_l^{k_l}),\ k_i = 0, 1, \dots, p-1,\ i = 1, \dots, l.$$

The set consisting of this minimal generating elements is denoted as S. The a-invariant element of $F[\oplus_{t=0}^{q-1} m_t V_{2,t}]^P$ satisfies $a(f) = f$, $\forall f \in F[\oplus_{t=0}^{q-1} m_t V_{2,t}]^P$. From Proposition 2.1, we know that its Noether number is less than or equal to $l(p-1)$. Since $\mathrm{Tr}^P(y_1^{p-1} \cdots y_l^{p-1})$ is an a-invariant polynomial, this polynomial is a generating element of $F[V]^G$. We take a subset $S_1 = \{f \in S | a(f) = f\}$ of S. Then S_1 is contained in the minimal generating set of $F[V]^G$. In the following we determine the other indecomposable generating elements. Let ξ be the q-th primitive root of unity. The a-invariant polynomial should satisfy the condition: let $a(f_i) = \xi^{a_i}$, $0 < a_i < q$,

$$\{f_1^{c_1} \cdots f_n^{c_n} | f_i \in S, f_i \notin S_1,\ \sum_{i=1}^n a_i c_i \equiv 0 \bmod (q)\}.$$

Further, the generating element of the a-invariant polynomial should also satisfy that the sequence is non-shortenable, i.e., there is no sequence $(c_1', \dots, c_n')$ with $c_i' \le c_i$ such that

$$\sum_{i=1}^n a_i c_i' \equiv 0 \bmod (q),$$

where $(0, \dots, 0) \ne (c_1', \dots, c_n') \ne (c_1, \dots, c_n)$. According to [12, Lemma 2.1], we obtain the following lemma.

Lemma 2.2 ([12]) *The non-shortenable sequence $(c_1, \dots, c_n)$ such that $\sum_{i=1}^n a_i c_i \equiv 0 \bmod (q)$ holds satisfies $\sum_{i=1}^n c_i \le q$, and $\sum_{i=1}^n c_i$ can be taken to its maximum value q.*

Proposition 2.3 *Let V be a faithful reduced G-module over a field F of characteristic p and V does not contain 1-dimensional representation as a summand. Let s be the maximum dimension of the indecomposable summands of V. Then*

(1) If $s = 3$ and V does not contain $V_{3,j}$ as a summand for any $j \in \{1, \dots, q-1\}$, or if $s > 3$ and V does not contain $V_{k,j}$ as a summand for any $j \in \{1, \dots, q-1\}$ and any $k \in \{4, \dots, s\}$, or if $V \cong \oplus \oplus_{t=1}^{q-1} m_t V_{2,t}, \sum_{t=1}^{q-1} m_t > 2$, then

$$\beta(F[V]^G) \leq q(\beta(F[V]^P) - 1).$$

(2) Other cases, i.e., if $V \cong V_{2,j}$ or $V \cong 2V_{2,j}$, or if $s = 3$ and at least one of the summands of V is isomorphic to $V_{3,j}$ with $j \in \{1, \dots, q-1\}$, or if $s > 3$ and at least one of summands of V is isomorphic to $V_{k,j}$ with $k \in \{4, \dots, s\}$ and $j \in \{1, \dots, q-1\}$, then

$$\beta(F[V]^G) \leq q\beta(F[V]^P).$$

Proof According to Proposition 2.1, there is $\beta(F[V]^G) \leq q\beta(F[V]^P)$. The second case holds and the following prove (1).

Case 1. If $V \cong \oplus_{t=0}^{q-1} m_t V_{2,t}$, $\sum_{t=0}^{q-1} m_t = l > 2$ and V is faithful, then V contains at least $V_{2,j}$, for some $j \in \{1, \dots, q-1\}$. Let a basis of V^* be $x, y; x_1, y_1; \dots; x_{l-1}, y_{l-1}$, where x, y is a basis of $V_{2,j}^*$. According to [11, Theorem 6.3], we have $\beta(F[V]^P) \leq l(p-1)$. After calculating, $\mathrm{Tr}^P(y^{p-1} y_1^{p-1} \cdots y_{l-1}^{p-1})$ is a-invariant, $\mathrm{Tr}^P(y^{p-2} y_1^{p-1} \cdots y_{l-1}^{p-1})$ is not a-invariant. Therefore, $\mathrm{Tr}^P(y^{p-2} y_1^{p-1} \cdots y_{l-1}^{p-1})$ is the maximum degree of a-variable polynomials in the minimal generating set of $F[V]^P$. According to Lemma 2.2, the maximum degree in the generating set of $F[V]^G$ satisfies $\beta(F[V]^G) \leq q[l(p-1) - 1]$.

Case 2. If $s = 3$ and the summands of V do not contain $V_{3,j}$, then V contains at least one 2-dimensional faithful indecomposable module $V_{2,k}$, for some $k \in \{1, \dots, q-1\}$. One may suppose the decomposition of V as

$$V \cong V_{3,0} \oplus V_{2,k} \oplus \oplus_{t=0}^{q-1} m_t V_{2,t}, \ \sum_{t=0}^{q-1} m_t \geq 0.$$

Let a basis of V^* be $x, y, z; x_0, y_0; x_1, y_1; \dots; x_l, y_l$, where x, y, z is a basis of $V_{3,0}^*$ and x_0, y_0 is a basis of $V_{2,k}^*$. According to [5, Proposition 1.1], we have $\beta(F[V]^P) \leq (l+2)(p-1) + 1$. After calculating, $\mathrm{Tr}^P(yz^{p-1} y_0^{p-1} y_1^{p-1} \cdots y_l^{p-1})$ is a-invariant, $\mathrm{Tr}^P(yz^{p-1} y_0^{p-2} y_1^{p-1} \cdots y_l^{p-1})$ is not a-invariant. Therefore, $\mathrm{Tr}^P(yz^{p-1} y_0^{p-2} y_1^{p-1} \cdots y_l^{p-1})$ is the maximum degree of a-variable polynomials in the minimal generating set of $F[V]^P$ by [5, Proposition 1.1] and [13, Corollary 9.16]. According to Lemma 2.2, the maximum degree in the generating set of $F[V]^G$ satisfies $\beta(F[V]^G) \leq q[(l+2)(p-1)]$.

Case 3. If $s > 3$ and the summands of V do not contain $V_{4,j}$, for any $j \in \{1, \dots, q-1\}$, then V contains at least one 2-dimensional faithful indecomposable module $V_{2,k}$, for some $k \in \{1, \dots, q-1\}$. One may suppose the decomposition of V as

$$V \cong V_{4,0} \oplus V_{2,k} \oplus \oplus_{t=0}^{q-1} m_t V_{2,t}, \ \sum_{t=0}^{q-1} m_t \geq 0.$$

Let a basis of V^* be $x, y, z, w; x_0, y_0; x_1, y_1; \dots; x_l, y_l$, where x, y, z, w is a basis of $V_{4,0}^*$ and x_0, y_0 is a basis of $V_{2,k}^*$. According to [5, Proposition 1.1], we have $\beta(F[V]^P) \leq (l+2)(p-1) + p - 2$. After calculating, $\mathrm{Tr}^P(z^{p-2} w^{p-1} y_0^{p-1} y_1^{p-1} \cdots y_l^{p-1})$ is a-invariant, $\mathrm{Tr}^P(z^{p-2} w^{p-1} y_0^{p-2} y_1^{p-1} \cdots y_l^{p-1})$ is not a-invariant. Therefore, $\mathrm{Tr}^P(z^{p-2}w^{p-1}y_0^{p-2}y_1^{p-1}\cdots y_l^{p-1})$ is the maximum degree of a-variable polynomials in the minimal generating set of $F[V]^P$ by [5, Proposition 1.1] and [13, Corollary 9.16]. According to Lemma 2.2, the maximum degree in the generating set of $F[V]^G$ satisfies $\beta(F[V]^G) \le q[(l+2)(p-1)+p-3]$. □

3. Lower bounds of the Noether numbers

In this section, let $G = \langle a \rangle$ be a cyclic group of order pq. Let $P = \langle a^q \rangle$ be a Sylow p subgroup of G.

Lemma 3.1 *Let V be a finite-dimensional G-module. If the invariant f of $F[V]^P$ is indecomposable and $a(f) \ne f$, then f^q is an invariant in $F[V]^G$ and indecomposable in $F[V]^G$.*

Proof If f is an invariant of $F[V]^P$ and $a(f) \ne f$, then f^q is an invariant of $F[V]^G$. Suppose that f^q is decomposable in $F[V]^G$, i.e.,

$$f^q = \sum_{i=1}^{r} f_i h_i,\ f_i, h_i \in F[V]^G, \quad i = 1, \dots, r,$$

where $0 < \deg(f_i)$, $\deg(h_i) < \deg(f)q$. Since P is a subgroup of G, it is obvious that f_i, h_i are also elements of $F[V]^P$. Since the invariant f is indecomposable in $F[V]^P$, $f_i = f^{k_i}$, $h_i = f^{l_i}$, $k_i + l_i = q$, $i = 1, \dots, l$. Therefore, $k_i = 0$ or $k_i = q$ because of $f_i, h_i \in F[V]^G$, which contradicts the assumption. Therefore, it is indecomposable in $F[V]^G$. □

Suppose $V \cong V_{3,0} \oplus V_{2,k} \oplus \oplus_{t=0}^{q-1} m_t V_{2,t}$, $\sum_{t=0}^{q-1} m_t = l$. Choose a basis

$$x, y, z; x_0, y_0; x_1, y_1; \dots; x_l, y_l$$

for V^*, where x, y, z is a basis of $V_{3,0}^*$ and x_0, y_0 is a basis of $V_{2,k}^*$.

Lemma 3.2 *$\mathrm{Tr}^P(yz^{p-1}y_0^{p-2}y_1^{p-1}\cdots y_l^{p-1})$ in $F[V_{3,0} \oplus V_{2,k} \oplus \oplus_{t=0}^{q-1} m_t V_{2,t}]^P$ is indecomposable.*

Proof The proof is by induction on l. When $l = 0$, we prove that $\mathrm{Tr}^P(yz^{p-1}y_0^{p-2})$ in $F[V_{3,0} \oplus V_{2,k}]^P$ is indecomposable. By way of contradiction, suppose that

$$f := \mathrm{Tr}^P(yz^{p-1}y_0^{p-2}) = \sum_{i=1}^{r} f_i h_i,\ f_i, h_i \in F[V_{3,0} \oplus V_{2,k}]^P,$$

where $0 < \deg(f_i)$, $\deg(h_i) < \deg(f)$. We use a graded reverse lexicographic with $z > y > y_0 > x > x_0$. We denote the leading term of a polynomial h with $\mathrm{LT}(h)$. Then $\mathrm{LT}(f) = y^p y_0^{p-2}$ by

$$\sum_{t=0}^{p-1} t^m = \begin{cases} -1, & p-1 \mid m, \\ 0, & p-1 \nmid m, \end{cases}$$

where m is a positive integer. We may assume that $\mathrm{LT}(f_i h_i) \ge \mathrm{LT}(f_{i+1}h_{i+1})$ for $i = 1, \dots, r-1$. Clearly, either $\mathrm{LT}(f_1h_1) = y^p y_0^{p-2}$ or $\mathrm{LT}(f_1h_1) = \mathrm{LT}(f_2h_2) > y^p y_0^{p-2}$. According to the proof procedure of [8, Corollary 5.2], it is easy to know that $y^p y_0^{p-2}$ is the indecomposable element of $F[V_{3,0} \oplus V_{2,k}]^P$. Therefore, $\mathrm{LT}(f_1h_1) = \mathrm{LT}(f_2h_2) > y^p y_0^{p-2}$. Note that $F[V_{3,0} \oplus V_{2,k}] = F[V_{3,0}] \otimes F[V_{2,k}]$ is bi-graded, the action of P respects this grading, and all of our generators are homogeneous with respect to this grading. However, there are no monomials with bi-degree $(p, p-2)$ which are greater than $y^p y_0^{p-2}$. Thus $\mathrm{Tr}^P(yz^{p-1}y_0^{p-2})$ is indecomposable.

For $l > 1$, by way of contradiction, suppose that

$$f := \mathrm{Tr}^P(yz^{p-1}y_0^{p-2}y_1^{p-1}\cdots y_l^{p-1}) = \sum_{i=1}^{r} f_i h_i, f_i, h_i \in F[V]^P,$$

where $0 < \deg(f_i)$, $\deg(h_i) < \deg(f)$.

We may assume that f_i, h_i and $f_i h_i$ are homogeneous with respect to multidegree, and that each $f_i h_i$ has multidegree $(p, p-2, p-1, \ldots, p-1)$. Suppose $m_{q-1} > 0$. Use the inclusion of $U := V_{3,0} \oplus V_{2,k} \oplus \oplus_{t=0}^{q-2} m_t V_{2,t} \oplus (m_{q-1}-1)V_{2,q-1} \oplus V_{1,q-1}$ into V to define a projection

$$\pi : F[V] \to F[U],$$

$$\pi(x_l) = 0, \pi(y_l) = x_l$$

and fix the other variables. Note that π is the algebra homomorphism. Since π is equivariant,

$$\pi(\mathrm{Tr}^P(yz^{p-1}y_0^{p-2}\cdots y_l^{p-1}) = x_l^{p-1}\mathrm{Tr}^P(yz^{p-1}y_0^{p-2}\cdots y_{l-1}^{p-1}).$$

Collecting all factors of x_l, we can write

$$\pi(f_i) = x_l^{k_i}\widetilde{f}_i, \quad \pi(h_i) = x_l^{k_i'}\widetilde{h}_i.$$

Using the homogeneous multidegree assumption gives

$$k_i + k_i' = p-1, \widetilde{f}_i, \widetilde{h}_i \in F[U]^P.$$

Thus $\pi(f) = x_l^{p-1}\sum_{i=1}^{r}\widetilde{f}_i\widetilde{h}_i$. Furthermore,

$$\widetilde{f} := \mathrm{Tr}^P(yz^{p-1}y_0^{p-2}\cdots y_{1-1}^{p-1}) = \sum_{i=1}^{r}\widetilde{f}_i\widetilde{h}_i.$$

By the induction hypothesis, $\widetilde{f}$ is indecomposable in $F[U]^P$. Suppose that one of the factors, say $\widetilde{f}_1 = c$ with $c \neq 0$. Then the multidegree of f_1 is $(0, \ldots, 0, k_1)$ with $k_1 < p$. Hence f_1 is a homogeneous element of degree less than p in $F[V_{2,q-1}]^P = F[x_l, y_l^p - y_l x_l^{p-1}]$. Thus $f_1 = cx_l^{k_1}$. Therefore, $\pi(f_1) = 0$, giving $\widetilde{f}_1 = 0$, which contradicts $\widetilde{f}_1 = c \neq 0$. Thus, $\mathrm{Tr}^P(yz^{p-1}y_0^{p-2}y_1^{p-1}\cdots y_l^{p-1})$ in $F[V]^P$ is indecomposable. □

Suppose $V \cong V_{4,0} \oplus V_{2,k} \oplus \oplus_{t=0}^{q-1} m_t V_{2,t}$, $\sum_{t=0}^{q-1} m_t = l$. Choose a basis

$$x, y, z, w; x_0, y_0; x_1, y_1; \ldots; x_l, y_l$$

for V^*, where x, y, z, w is a basis of $V_{4,0}^*$ and x_0, y_0 is a basis of $V_{2,k}^*$.

Lemma 3.3 *$\mathrm{Tr}^P(z^{p-2}w^{p-1}y_0^{p-2}y_1^{p-1}\cdots y_l^{p-1})$ in $F[V_{4,0} \oplus V_{2,k} \oplus \oplus_{t=0}^{q-1} m_t V_{2,t}]^P$ is indecomposable.*

Proof The proof is by induction on l. When $l = 0$, we prove that $\mathrm{Tr}^P(z^{p-2}w^{p-1}y_0^{p-2})$ in $F[V_{4,0} \oplus V_{2,k}]^P$ is indecomposable. By way of contradiction, suppose that

$$f := \mathrm{Tr}^P(z^{p-2}w^{p-1}y_0^{p-2}) = \sum_{i=1}^{r} f_i h_i, f_i, h_i \in F[V_{4,0} \oplus V_{2,k}]^P,$$

where $0 < \deg(f_i), \deg(h_i) < \deg(f)$. We use a graded reverse lexicographic with $w > z > y > y_0 > x > x_0$. Then $\mathrm{LT}(f) = z^{2p-3}y_0^{p-2}$. We may assume that $\mathrm{LT}(f_ih_i) \geq \mathrm{LT}(f_{i+1}h_{i+1})$ for $i = 1, \ldots, r-1$. Clearly, either $\mathrm{LT}(f_1h_1) = z^{2p-3}y_0^{p-2}$ or $\mathrm{LT}(f_1h_1) = \mathrm{LT}(f_2h_2) > z^{2p-3}y_0^{p-2}$. According to [13, Section 10.1] and [5, Proposition 1.1], $F[V_{4,0} \oplus V_{2,k}]$ is generated by 13 integral invariants, $N^P(w), N^P(y_0)$ and the family of transfers $\mathrm{Tr}^P(w^d z^c y^b y_0^{b_0})$ with $0 \leq d, b_0 \leq p-1$, $0 \leq c \leq p-2$, $b = 0$ or 1, $b + c + d \leq 2p-3$. Let S denote the collection of above invariants. The elements in $\mathrm{LT}(S)$ of the form $z^{2p-3}y_0^{p-2}$ are $\{y_0^p, w^p, z^{p-1+i}, z^{p-1+i}y_0^j\}$ with $i = 0, 1, \ldots, p-2$; $j = 0, 1, \ldots, p-1$. Thus $z^{2p-3}y_0^{p-2}$ is the indecomposable element of $F[V_{4,0} \oplus V_{2,k}]^P$. Therefore,

$$\mathrm{LT}(f_1h_1) = \mathrm{LT}(f_2h_2) > z^{2p-3}y_0^{p-2}.$$

Note that $F[V_{4,0} \oplus V_{2,k}] = F[V_{4,0}] \otimes F[V_{2,k}]$ is bi-graded, the action of P respects this grading, and all of our generators are homogeneous with respect to this grading. However, there are no monomials with bi-degree $(2p-3, p-2)$ which are greater than $z^{2p-3}y_0^{p-2}$. Thus $\mathrm{Tr}^P(z^{p-2}w^{p-1}y_0^{p-2})$ is indecomposable. The induction step is essentially the same as the induction step in the proof of Lemma 3.2. □

Proposition 3.4 *Let V be a faithful reduced G-module over a field F of characteristic p and V does not contain 1-dimensional representation as a summand. Let s be the maximum dimension of the indecomposable summands of V and P be the Sylow p subgroup of G. Then*

(1) If $s = 3$ and V does not contain $V_{3,j}$ as a summand for any $j \in \{1, \ldots, q-1\}$, or if $s > 3$ and V does not contain $V_{k,j}$ as a summand for any $k \in \{4, \ldots, s\}$ and any $j \in \{1, \ldots, q-1\}$, or if $V \cong \oplus \oplus_{t=1}^{q-1} m_t V_{2,t}$, $\sum_{t=1}^{q-1} m_t > 2$, then

$$\beta(F[V]^G) \geq q(\beta(F[V]^P) - 1).$$

(2) Other cases, i.e., if $V \cong V_{2,j}$ or $V \cong 2V_{2,j}$, or if $s = 3$ and at least one of the summands of V is isomorphic to $V_{3,j}$ with $j \in \{1, \ldots, q-1\}$, or if $s > 3$ and at least one of summands of V is isomorphic to $V_{k,j}$ with $k \in \{4, \ldots, s\}$ and $j \in \{1, \ldots, q-1\}$, then

$$\beta(F[V]^G) \geq q\beta(F[V]^P).$$

Proof (1) Using Lemmas 3.1–3.3 and [11, Theorem 6.3], the above conclusions can be obtained.

(2) Case 1. If $s > 3$ and at least one of summands of V contains $V_{k,j}$, where $k \in \{4, \ldots, s\}$ and $j \in \{1, \ldots, q-1\}$, then decompose V as

$$V = V_{r_0,j_0} \oplus V_{r_1,j_1} \oplus \cdots \oplus V_{r_l,j_l},$$

where $r_0 \geq 4$, $j_0 \geq 1$, $r_i \geq 2$, $i = 1, \ldots, l$. For each $i = 0, 1, \ldots, l$, choose a distinguished variable $X_i \in V_{r_i,j_i}^*$. Denote $U = V_{4,j_0} \oplus \oplus_{i=1}^{l} V_{2,j_i}$. Choose a basis

$$x_0, y_0, z_0, w_0; x_1, y_1; \ldots; x_l, y_l$$

for U^*. We determine a P-equivariant surjection $\phi : V^* \to U^*$ by requiring that $\phi(X_0) = w_0, \phi(X_i) = y_i$ for $i = 1, \ldots, l$. This induces a P-equivariant surjection, which we also call ϕ mapping $F[V]$ onto $F[U]$. Thus $\phi(\Delta^j(X_i)) = \Delta^j\phi(X_i)$ for $i = 0, 1, \ldots, l$ and $j = 0, 1, \ldots, p-1$, where $\Delta = a^q - 1$. Restricting to invariants, we get an algebra map $\phi : F[V]^P \to F[U]^P$.

Since ϕ is an algebra homomorphism and since

$$\phi(\mathrm{Tr}^P(\Delta(X_0)^{p-2}X_0^{p-1}X_1^{p-1}\cdots X_l^{p-1})) = \mathrm{Tr}^P(z_0^{p-2}w_0^{p-1}y_1^{p-1}\cdots y_l^{p-1}),$$

is indecomposable in $F[U]^P$ by [5, Lemma 2.2], it follows that

$$\mathrm{Tr}^P(\Delta(X_0)^{p-2}X_0^{p-1}X_1^{p-1}\cdots X_l^{p-1})$$

is indecomposable in $F[V]^P$. By Lemma 3.1, $(\mathrm{Tr}^P(\Delta(X_0)^{p-2}X_0^{p-1}X_1^{p-1}\cdots X_l^{p-1}))^q$ is indecomposable in $F[V]^G$. Therefore, $\beta(F[V]^G) \geq q((l+1)(p-1)+p-2)$, i.e., $\beta(F[V]^G) \geq q\beta(F[V]^P)$.

Case 2. If $s=3$ and at least one of the summands of V is isomorphic to $V_{3,j}$ for $j=1,\dots,q-1$, then decompose V as

$$V = V_{r_0,j_0} \oplus V_{r_1,j_1} \oplus \cdots \oplus V_{r_l,j_l},$$

where $r_0 = 3$, $j_0 \geq 1$, $3 \geq r_i \geq 2$, $i = 1,\dots,l$. For each $i = 0,1,\dots,l$, choose a distinguished variable $y_i \in V^*_{r_i,j_i}$. By [5, Lemma 2.3] and Lemma 3.1, $(\mathrm{Tr}^P(\Delta(y_0)y_0^{p-1}y_1^{p-1}\cdots y_l^{p-1}))^q$ is indecomposable in $F[V]^G$. Therefore, $\beta(F[V]^G) \geq q((l+1)(p-1)+1)$, i.e., $\beta(F[V]^G) \geq q\beta(F[V]^P)$.

Case 3. If $V = V_{2,j}$ or $V = 2V_{2,j}$ for $j = 1,\dots,q-1$, then the proof can be obtained according to Lemma 3.1 and the generating elements of $F[V]^P$. $\square$

Acknowledgements We thank the referees for their time and comments.

References

[1] E. NOETHER. *Der Endlichkeitssatz der Invarianten endlicher Gruppen*. Math. Ann., 1915, **77**(1): 89–92. (in German)

[2] P. FLEISCHMANN. *The Noether bound in invariant theory of finite groups*. Adv. Math., 2000, **156**(1): 23–32.

[3] J. FOGARTY. *On Noether's bound for polynomial invariants of a finite group*. Electron. Res. Announc. Amer. Math. Soc., 2001, **7**: 5–7.

[4] D. RICHMAN. *On vector invariants over finite fields*. Adv. Math., 1990, **81**(1): 30–65.

[5] P. FLEISCHMANN, M. SEZER, R. SHANK, et al. *The Noether number for cyclic groups of prime order*. Adv. Math., 2006, **207**(1): 149–155.

[6] P. SYMONDS. *On the Castelnuovo-Mumford regularity of rings of polynomial invariants*. Ann. of Math. (2), 2011, **174**(1): 499–517.

[7] D. WEHLAU. *Some Problems in Invariant Theory*. Amer. Math. Soc., Providence, RI, 2004.

[8] R. SHANK, D. WEHLAU. *Noether numbers for subrepresentations of cyclic groups of prime order*. Bull. London Math. Soc., 2002, **34**(2): 438–450.

[9] M. SEZER, R. SHANK. *On the coinvariants of modular representations of cyclic groups of prime order*. J. Pure Appl. Algebra, 2006, **205**(1): 210–225.

[10] I. HUGHES, G. KEMPER. *Symmetric powers of modular representations for groups with a Sylow subgroup of prime order*. J. Algebra, 2001, **241**(2): 759–788.

[11] H. E. A. CAMPBELL, R. SHANK, D. WEHLAU. *Vector invariants for the two-dimensional modular representation of a cyclic group of prime order*. Adv. Math., 2010, **225**(2): 1069–1094.

[12] B. J. SCHMID. *Finite Groups and Invariant Theory*. Springer, Berlin, 1991.

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