M. Kohls and M. Sezer (2014) “Top Degree of Coinvariants,”
International Mathematics Research Notices, Vol. 2014, No. 22, pp. 6079–6093
Advance Access Publication July 24, 2013
doi:10.1093/imrn/rnt158

On The Top Degree of Coinvariants

Martin Kohls[1] and Müfit Sezer[2]

[1]Technische Universität München, Zentrum Mathematik-M11, Boltzmannstrasse 3, 85748 Garching, Germany and [2]Department of Mathematics, Bilkent University, Ankara 06800, Turkey

Correspondence to be sent to: kohls@ma.tum.de

For a finite group G acting faithfully on a finite-dimensional F-vector space V, we show that in the modular case, the top degree of the vector coinvariants grows unboundedly: $\lim_{m\to\infty} \operatorname{topdeg} F[V^m]_G = \infty$. In contrast, in the nonmodular case we identify a situation where the top degree of the vector coinvariants remains constant. Furthermore, we present a more elementary proof of Steinberg's theorem which says that the group order is a lower bound for the dimension of the coinvariants which is sharp if and only if the invariant ring is polynomial.

1 Introduction

A central problem in invariant theory is to compute the generators of the invariants of a group action. One crucial element in this task is determining the degrees of the generators as the knowledge of these degrees reduces this problem to a problem in a finite-dimensional vector space. This gives obtaining efficient degree bounds a big computational significance and research in this direction has always been fashionable since the days of Noether to our days, with some recent spectacular breakthroughs, for example, [26]. Before we go into more details, we fix our setup. For a shorthand notion, we will call a finite-dimensional representation V of a finite group G over a

Received November 8, 2012; Revised March 27, 2013; Accepted July 5, 2013
Communicated by Prof. Corrado De Concini

field F a *G-module*. The action of G on V induces an action on the symmetric algebra $F[V] = S(V^*)$ that is given by $\sigma(f) = f \circ \sigma^{-1}$ for $\sigma \in G$ and $f \in F[V]$. Let $F[V]^G$ denote the corresponding ring of invariants. By a classical theorem of Noether, it is a finitely generated algebra, and $\beta(F[V]^G)$, the Noether number of the representation, denotes the maximal degree of an indecomposable element, that is, the smallest number b such that invariants of degree $\leq b$ generate the invariant ring. We direct the reader to [15] or [28] for an account on this number. We also define $\beta(G) = \sup_V \beta(F[V]^G)$. Another central object is the Hilbert ideal $I := F[V]^G_+ F[V]$, the ideal in $F[V]$ generated by invariants of positive degree. In this paper, we study the algebra of coinvariants, which is the quotient ring $F[V]_G := F[V]/I$. This finite-dimensional, graded algebra encodes several interesting properties of the invariant ring and there has been a fair amount of research on it, see [2, 3, 8, 11, 14, 16, 21–25] and the references there. The top degree of the coinvariants, denoted topdeg $F[V]_G$, is defined to be the largest degree in which $F[V]_G$ is nonzero. This number shares a similar interest for coinvariants as the Noether number does for invariants.

Equivalently, the top degree can be defined as the smallest number d such that every monomial $m \in F[V]$ of degree $> d$ is contained in the Hilbert ideal. Note that this also implies that the Hilbert ideal is generated by elements of degree at most $d+1$, a fact that played an important role in the proof of the Noether bound in the nonmodular case, that is, when the characteristic of F is zero or $|G| \in F^*$. However, it is conjectured [5, Conjecture 3.8.6] that even in the modular case, that is, when the order of the group is divisible by the characteristic of F, the group order is an upper bound for the degrees of the generators of the Hilbert ideal, which as we will see, may be much smaller than the top degree.

Another natural interpretation comes from regarding $F[V]$ as a (finite) $F[V]^G$-module. Take a minimal set of homogeneous module generators g_i of $F[V]$ over $F[V]^G$, so $F[V] = \sum_{i=1}^{t} F[V]^G g_i$. From the graded Nakayama lemma, it follows that the top degree d equals the maximum of the degrees of the generators, and the number of generators equals the dimension of the coinvariants as a vector space.

Recall that the transfer of $f \in F[V]$ is defined by $\mathrm{Tr}(f) = \sum_{\sigma \in G} \sigma(f)$. Another important application of the top degree is that in the modular case, it yields an upper bound for the maximal degree of an indecomposable transfer: Take $f \in F[V]$ homogeneous. Then we can write $f = \sum_{i=1}^{t} h_i g_i$ with homogeneous invariants h_i and module generators g_i as above. Therefore, $\mathrm{Tr}(f) = \sum_{i=1}^{t} h_i \mathrm{Tr}(g_i)$. Assume $\deg(f)$ is bigger than the top degree of $F[V]_G$. Then all h_i's are zero or of positive degree. We are done if also all $\mathrm{Tr}(g_i)$'s are zero or of positive degree. Note that one of the module generators, say

g_1, is a constant. Since we are in the modular case we have $\mathrm{Tr}(1) = |G| \cdot 1 = 0$, so we are done. Knowing the maximal degree of an indecomposable transfer has been very critical so far, since in almost all modular cases where the Noether number is known, there is an indecomposable transfer of degree equal to the Noether number, see [11]. In the nonmodular case (i.e., the characteristic of F does not divide the group order $|G|$), the invariant ring is generated by transfers and so a bound for the degree of an indecomposable transfer is a bound for the Noether number. Since $\mathrm{Tr}(1) \neq 0$, the argument above does not carry over to this characteristic. Nevertheless, in the nonmodular case, the top degree plus one is an upper bound for the Noether number and this bound is sharp: The Noether number corresponding to the natural action of S_2 on $F[x_1, x_2]$ is 2, while the top degree of the coinvariants is 1.

We now give an outline of the paper. Section 2 is mainly concerned with the nonmodular case, where we collect some consequences of previous work on the top degree of coinvariants. Most notably, a quite recent result of Cziszter and Domokos implies that for a given nonmodular group G, the maximal top degree equals the maximal Noether number minus one. In particular, $|G| - 1$ gives an upper bound for the top degree.

In contrast, we show in Section 3 that for a given faithful modular representation V, the top degree of the vector coinvariants $F[V^m]_G$ grows unboundedly with m. This also fits nicely with a result of Richman [19], which asserts the similar behavior for the Noether number of the vector invariants $F[V^m]^G$.

In Section 4, we consider a nonmodular situation where the lead term ideal of $F[V]^G_+F[V]$ is generated by pure powers of the variables. In this case, we show that the top degree of the vector coinvariants $F[V^m]_G$ is constant. This way, for the natural action of the symmetric group S_n on a polynomial ring with n variables we get a new proof that the top degree of any of the vector coinvariants of this action is $\binom{n}{2}$.

In Section 5, we will give a new elementary proof of Steinberg's celebrated theorem which states that the group order is a lower bound for the dimension of the coinvariants with equality holding if and only if the invariant ring is polynomial.

2 Top Degree in the Nonmodular Case

In this section, we note several facts about the top degree of coinvariants in the nonmodular case, which are a bit spread out in the literature. Although these statements follow rather quickly from previous results, it seems that the statements themselves have not been formulated in terms of coinvariants before. Using a very recent result of Cziszter and Domokos [4], we obtain in Theorem 1 that the supremum of the top degrees of coinvariants is one less than the Noether number of the group. Since the Noether number is bounded by the group order, we establish $|G|-1$ as an upper bound for the top degree of coinvariants of any nonmodular representation. This upper bound also follows directly from Fogarty's proof of the Noether bound. We take the crucial part of this proof here as Lemma 2. Using this lemma, we also obtain a relative bound for the top degree of coinvariants, see Proposition 3. We end this section with a brief discussion of the relation between the Davenport constant and the top degree in the abelian group case.

Theorem 1. Assume that the characteristic of F does not divide the group order $|G|$. Then, for any G-module V, we have

$$\beta(F[V]^G) \leq \operatorname{topdeg} F[V]_G + 1 \leq \beta(G) \leq |G|.$$

In particular, we have that

$$\operatorname{topdeg}(G) + 1 := \sup_V \operatorname{topdeg} F[V]_G + 1 = \beta(G). \qquad \square$$

Proof. Let I denote the Hilbert ideal of $F[V]^G$ and d denote the top degree of $F[V]_G$. As mentioned in Section 1, I is generated by elements of degree at most $d+1$. As we are in the nonmodular case, this implies that $F[V]^G$ is generated by invariants of degree at most $d+1$, which proves the first inequality. By [4, Lemma 3.1], for any G-module V there exists an irreducible G-module U such that $\operatorname{topdeg} F[V]_G + 1 \leq \beta(F[V \oplus U]^G)$, which proves the second inequality. Finally, the Noether number is at most the group order in the nonmodular case, see [9, 12]. Now the last statement follows from choosing a G-module V with $\beta(F[V]^G) = \beta(G)$. ■

There are many bounds for $\beta(G)$ in invariant theory literature. By this theorem, they translate into bounds for $\operatorname{topdeg}(G)+1$. For example, if H is a normal subgroup of G, in the nonmodular case, we have $\beta(G) \leq \beta(H)\beta(G/H)$ [20, Lemma 3.1] (see also [10, (3.1)]). So, we get $\operatorname{topdeg}(G)+1 \leq (\operatorname{topdeg}(G/H)+1)(\operatorname{topdeg}(H)+1)$.

However, for a given module V, its Noether number can be much smaller than the top degree. For example, for the natural action of the symmetric group on n variables, the invariants have Noether number n, while the top degree of the coinvariants is $\binom{n}{2}$.

A key step in Fogarty's proof of $\beta(G) \leq |G|$ in the nonmodular case is the following lemma [12].

Lemma 2 (see [5, Lemma 3.8.1]). Let A be a commutative ring with identity, G a finite group of automorphisms of A, and $J \subseteq A$ a G-stable ideal. If the order of G is invertible in A, then $J^{|G|} \subseteq J^G A$. □

This lemma also yields a relative bound for the top degree of coinvariants.

Proposition 3. Assume H is a normal subgroup of G and the characteristic of F does not divide the index $(G:H)$. Then we have the inequality

$$\operatorname{topdeg}(F[V]_G) + 1 \leq (G:H)(\operatorname{topdeg}(F[V]_H) + 1). \qquad \square$$

Proof. Let m denote the top degree of $F[V]_H$, and d denote the index $(G:H)$. Then all monomials of degree $m+1$ of $F[V]$ lie in $I := F[V]^H_+ \cdot F[V]$. Therefore, all monomials of degree $d(m+1)$ lie in

$$I^d = (F[V]^H_+ \cdot F[V])^d = (F[V]^H_+)^d \cdot F[V].$$

By the previous lemma, applied to the group (G/H) acting on $A = F[V]^H$ and the G/H-stable ideal $J = F[V]^H_+$, we have

$$(F[V]^H_+)^d \subseteq (F[V]^H_+)^{G/H} F[V]^H = F[V]^G_+ F[V]^H \subseteq F[V]^G_+ F[V].$$

Therefore, all monomials of degree $d(m+1)$ lie in $F[V]^G_+ F[V]$. ■

For abelian groups, the top degree of the coinvariants has another interpretation in terms of the *Davenport constant* of the group. We conclude with a discussion on this relationship. For the rest of this section assume that G is an abelian group with $|G| \in F^*$. Since extending the ground field does not change the top degree of coinvariants we assume that F is algebraically closed. In this case, the action is diagonalizable so we may as well assume that $F[V] = F[x_1, \ldots, x_n]$, where $x_1, \ldots, x_n$ is a basis of V^* on which G acts diagonally. For each $1 \leq i \leq n$, let κ_i denote the character corresponding to the action on x_i. Then a monomial $x_1^{a_1} \cdots x_n^{a_n}$ is in $F[V]^G$ if $\sum_{1 \leq i \leq n} a_i \kappa_i = 0$. Moreover, a monomial $x_1^{a_1} \cdots x_n^{a_n}$ is in the Hilbert ideal I if it is divisible by an invariant monomial, that is there exist integers $0 \leq b_i \leq a_i$ such that $\sum_{1 \leq i \leq n} b_i \kappa_i = 0$. For an abelian group G, let $S(G)$ denote the minimal integer such that every set of elements, with repetitions allowed, of size $S(G)$ in G has a subsequence that sums up to zero. It also equals the length of the longest nonshortenable zero sum of elements (with repetitions) of G. This number is called the Davenport constant of G. Since the character group of G is isomorphic to G it follows that every monomial in $F[V]$ of degree $S(G)$ lies in I. This gives $\operatorname{topdeg}(G)+1 \leq S(G)$. On the other hand, by constructing an action using the characters in the longest sequence of elements with no subsequence summing up to zero we get a G-module V with $\operatorname{topdeg} F[V]_G + 1 = S(G)$. Similarly, one can show that $\beta(G) = S(G)$, see also [20, Proposition 2.2]. So, it follows that

$$S(G) = \operatorname{topdeg}(G) + 1 = \beta(G).$$

Results on the Davenport constant therefore apply to the top degree of the coinvariants, and vice versa. See [13] for a survey on the Davenport constant. Here, we just quote two famous results due to Olson [17, 18]: If Z_n denotes the cyclic group of order n, then if $a|b$, we have $S(Z_a \times Z_b) = a + b - 1$. If p is a prime, then $S(Z_{p^{d_1}} \times \cdots \times Z_{p^{d_r}}) = 1 + \sum_{i=1}^{r}(p^{d_i} - 1)$.

3 The Unboundedness of the Top Degree for Modular Coinvariants

In this section, we specialize to the modular case and show that, in contrast to the nonmodular case, the top degree of the coinvariants of a given group can become arbitrarily large. We start with a collection of observations which despite their simplicity give useful upper and lower bounds.

Lemma 4. Let H be a subgroup of G and V be a G-module. Then

$$\operatorname{topdeg} F[V]_H \leq \operatorname{topdeg} F[V]_G \quad \text{and} \quad \dim F[V]_H \leq \dim F[V]_G. \qquad \square$$

Proof. The inclusion $F[V]_+^G \subseteq F[V]_+^H$ induces a degree-preserving surjection

$$F[V]_G = F[V]/F[V]_+^G F[V] \twoheadrightarrow F[V]/F[V]_+^H F[V] = F[V]_H,$$

which immediately establishes the claim. ■

Lemma 5. Let U be a G-submodule of V. Then

$$\operatorname{topdeg} F[U]_G \leq \operatorname{topdeg} F[V]_G \quad \text{and} \quad \dim F[U]_G \leq \dim F[V]_G. \qquad \square$$

Proof. The inclusion $U \subseteq V$ induces the epimorphism

$$\varphi : F[V] \twoheadrightarrow F[U], \quad f \mapsto f|_U,$$

which restricts to a (generally nonsurjective) morphism $F[V]^G \to F[U]^G$. We therefore get a degree-preserving epimorphism

$$\overline{\varphi}:\ F[V]_G = F[V]/F[V]^G_+F[V] \twoheadrightarrow F[U]/F[U]^G_+F[U] = F[U]_G,$$

which yields both inequalities. ■

For a G-module V, let V^m denote the m-fold direct sum of V.

Lemma 6. For any two G-modules V and W, we have,

$$\operatorname{topdeg} F[V\oplus W]_G \le \operatorname{topdeg} F[V]_G + \operatorname{topdeg} F[W]_G.$$

In particular, we have $\operatorname{topdeg} F[V^m]_G \le m \operatorname{topdeg} F[V]_G$ for all $m \in \mathbb{N}$. □

Proof. Assume that $M \in F[V\oplus W]$ is a monomial of degree at least $\operatorname{topdeg} F[V]_G + \operatorname{topdeg} F[W]_G + 1$. Write $M = M'M''$ with $M' \in F[V]$ and $M'' \in F[W]$. Then we have either $\deg M' > \operatorname{topdeg} F[V]_G$ or $\deg M'' > \operatorname{topdeg} F[W]_G$. Without loss of generality, we assume the former inequality. Then $M' \in F[V]^G_+F[V]$, which implies $M \in F[V]^G_+F[V\oplus W] \subseteq F[V\oplus W]^G_+F[V\oplus W]$. ■

Let $V_{\mathrm{reg}} := FG$ denote the regular representation of G. For any G-module V, we have an embedding $V \hookrightarrow V_{\mathrm{reg}}^{\dim_F(V)}$ (choosing an arbitrary basis of V^* yields an epimorphism $(V_{\mathrm{reg}})^{\dim_F(V)} \twoheadrightarrow V^*$, and dualizing yields the desired embedding as V_{reg} is self dual—see also [7, Proof of Corollary 3.11]). Thus, we get the following as a corollary to the preceding lemmas.

Corollary 7. For any G-module V, we have

$$\operatorname{topdeg} F[V]_G \le \dim_F(V) \operatorname{topdeg} F[V_{\mathrm{reg}}]_G. \qquad \square$$

In view of Theorem 1, the main result of this section nicely separates the modular coinvariants from the nonmodular ones.

Theorem 8. Let V be a faithful G-module and assume that the characteristic $p > 0$ of F divides the group order $|G|$. Then

$$\lim_{m\to\infty} \operatorname{topdeg} F[V^m]_G = \infty. \qquad \square$$

Proof. Pick a subgroup H of G of size p. It is well known that the indecomposable H-modules consist of modules V_k for $1 \leq k \leq p$, where V_k is a k-dimensional vector space on which a generator of H acts via a single Jordan block with ones on the diagonal. Therefore, as an H-module, V decomposes in a direct sum $V = \bigoplus_{i=1}^{q} V_{k_i}$. Note that V is also faithful as an H-module, so, without loss of generality, we assume $k_1 \geq 2$. Note that we have an H-module inclusion $V_k \subseteq V_l$ for any pair of integers $1 \leq k \leq l \leq p$. In particular, we have the H-module inclusions

$$V_2 \subseteq V_{k_1} \subseteq \bigoplus_{i=1}^{q} V_{k_i} = V.$$

Therefore, for any $m \in \mathbb{N}$, we have $V_2^m \subseteq V^m$ as H-modules. We now get

$$\operatorname{topdeg} F[V^m]_G \geq \operatorname{topdeg} F[V^m]_H$$

by Lemma 4, and furthermore

$$\operatorname{topdeg} F[V^m]_H \geq \operatorname{topdeg} F[V_2^m]_H$$

by Lemma 5. Moreover, from [22, Theorem 2.1], we get $\operatorname{topdeg} F[V_2^m]_H = m(p-1)$. So, it follows that

$$\operatorname{topdeg} F[V^m]_G \geq m(p-1) \quad \text{for all } m \in \mathbb{N}. \qquad ■$$

We will show next that the dimensions of the vector coinvariants always grow unboundedly as well, even in the nonmodular case. We start again with a simple but useful observation:

Lemma 9. For any G-module V, we have

$$\dim F[V]_G \geq \operatorname{topdeg} F[V]_G + 1. \qquad □$$

Proof. If d is the top degree of $F[V]_G$, then there exists a monomial m of degree d which is not in the Hilbert ideal I. Then every divisor of m is also not contained in I, which means that $F[V]_G$ contains a nonzero class in each degree $\leq d$. As elements of different degrees are linearly independent, this finishes the proof. ■

Proposition 10. For any nontrivial G-module V, we have

$$\lim_{m\to\infty} \dim F[V^m]_G = \infty. \qquad □$$

Proof. We can assume that the action of G is faithful. In the modular case, the result follows from Lemma 9 and Theorem 8. In the nonmodular case, choose a subgroup $H = \langle\sigma\rangle$ of G of prime order q, which is coprime to the characteristic of F. Choose a basis $x_1, \ldots, x_n$ of V^* on which σ acts diagonally. Since V is a faithful H-module as well, we may assume that the action of σ on x_1 is given by multiplication with a primitive qth root of unity. Let $x_{1,1}, \ldots, x_{1,m}$ denote the copies of x_1 in $F[V^m]$. Then none of the linear combinations of these variables lie in the Hilbert ideal $F[V^m]_+^H F[V^m]$, so they form an independent set of classes in $F[V^m]_H$. Therefore, by Lemma 4, we have

$$\dim F[V^m]_G \geq \dim F[V^m]_H \geq m,$$

which clearly establishes the claim. ■

4 Top Degree of Vector Coinvariants in the Nonmodular Case

In this section, we study vector copies of an action of a group in the nonmodular case. Obtaining generating invariants for these actions is generally a difficult problem nevertheless the degrees of polynomials in minimal generating sets do not change in many cases, see [7, Example 3.10] for a rare counter-example. Our computer-aided search of examples indicate that many classes of coinvariants enjoy a similar type of saturation. We note this as a problem for future study.

Problem 11. Assume that V is a nonmodular G-module. Prove or disprove that

$$\operatorname{topdeg} F[V^m]_G = \operatorname{topdeg} F[V]_G$$

for any positive integer m. Find classes of groups and modules for which the equality is true. □

We prove the equality above for a certain special case. First, we review the concept of polarization as we use polarized polynomials in our computations. Let V be a nonmodular G-module and set $A := F[V] = F[x_1, \ldots, x_n]$ and $B := F[V^m] = F[x_{1,1}, \ldots, x_{n,1}, \ldots, x_{1,m}, \ldots, x_{n,m}]$. We use the lexicographic order on B such that

$$x_{1,1} > x_{1,2} > \cdots > x_{1,m} > \cdots > x_{n,1} > \cdots > x_{n,m}$$

and the order on A is obtained by setting $m = 1$. For an ideal I in A or B, we denote the lead term ideal of I with $L(I)$. Also $L(f)$ denotes the lead term of a polynomial f in these rings. We introduce additional variables $t_1, \ldots, t_m$ and define an algebra homomorphism

$$\phi : A \to B[t_1, \ldots, t_m], \quad x_i \mapsto x_{i,1}t_1 + \cdots + x_{i,m}t_m.$$

Then, for any $f \in A$, write

$$\phi(f) = \sum_{i_1,\ldots,i_m} f_{i_1,\ldots,i_m} t_1^{i_1} \cdots t_m^{i_m},$$

where $f_{i_1,\ldots,i_m} \in B$. This process is called polarization and we let $\mathrm{Pol}(f)$ denote the set of coefficients $\phi_{i_1,\ldots,i_m}(f) := f_{i_1,\ldots,i_m}$ of $\phi(f)$. Restricting to invariants, it is well known that we get a map $\mathrm{Pol} : A^G \to \mathfrak{P}(B^G)$, where $\mathfrak{P}(B^G)$ denotes the power set of B^G. Let $I_A := A_+^G A$ denote the Hilbert ideal of A, and similarly I_B denote the Hilbert ideal of B. We show that polarization of a polynomial in I_A gives polynomials in I_B.

Lemma 12. Let $f \in I_A$. Then $\mathrm{Pol}(f) \in \mathfrak{P}(I_B)$. □

Proof. Since each $\phi_{i_1,\ldots,i_m}$ is a linear map, we may take $f = hg$ with $h \in A_+^G$ and $g \in A$. Write $\phi(h) = \sum_{j_1,\ldots,j_m} h_{j_1,\ldots,j_m} t_1^{j_1} \cdots t_m^{j_m}$ and $\phi(g) = \sum_{q_1,\ldots,q_m} g_{q_1,\ldots,q_m} t_1^{q_1} \cdots t_m^{q_m}$. Note that we have $h_{j_1,\ldots,j_m} \in B_+^G$ since polarization preserves degrees. It follows that

$$f_{i_1,\ldots,i_m} = \sum_{j_k+q_k=i_k,\ 1\le k\le m} h_{j_1,\ldots,j_m} g_{q_1,\ldots,q_m} \in B_+^G B,$$

which proves the lemma. ■

We now identify a situation where the equality in Problem 11 holds.

Theorem 13. Let F be a field of characteristic p and V a G-module. Assume that there exist integers $a_1, \ldots, a_n$, strictly smaller than p in the case of positive characteristic, such that $L(I_A) = (x_1^{a_1}, \ldots, x_n^{a_n})$. Then we have

$$\mathrm{topdeg}\, F[V^m]_G = \mathrm{topdeg}\, F[V]_G = \sum_{i=1}^{n} (a_i - 1) \quad \text{for all } m \in \mathbb{N}.$$ □

Proof. Since the monomials in A that do not lie in $L(I_A)$ form a vector space basis for $F[V]_G$, we have $\mathrm{topdeg}\, F[V]_G = \sum_{i=1}^{n}(a_i - 1)$. From Lemma 5, we also have $\mathrm{topdeg}\, F[V]_G \le \mathrm{topdeg}\, F[V^m]_G$. Therefore, to prove the theorem it suffices to show $\mathrm{topdeg}\, F[V^m]_G \le$

$\sum_{i=1}^{n}(a_i - 1)$. To this end, we demonstrate that the lead term ideal $L(I_B)$ contains the set

$$S := \{x_{i,1}^{a_{i,1}} x_{i,2}^{a_{i,2}} \cdot \ldots \cdot x_{i,m}^{a_{i,m}} \mid i = 1, \ldots, n,\ a_{i,1} + \cdots + a_{i,m} = a_i\}.$$

Take a homogeneous element $f \in I_A$ with $L(f) = x_i^{a_i}$. So, $f = x_i^{a_i} + h$ where each term in h is strictly lex-smaller than $x_i^{a_i}$. Then each term of h is of the form $x_i^{b_i} x_{i+1}^{b_{i+1}} \cdots x_n^{b_n}$ with $b_i < a_i$. Considering

$$\phi(x_i^{a_i}) = (t_1 x_{i,1} + \cdots + t_m x_{i,m})^{a_i}$$

and

$$\phi(x_i^{b_i} x_{i+1}^{b_{i+1}} \cdots x_n^{b_n}) = (t_1 x_{i,1} + \cdots + t_m x_{i,m})^{b_i} \cdots (t_1 x_{n,1} + \cdots + t_m x_{n,m})^{b_n},$$

we get by the choice of our order that, for any sequence $a_{i,1}, \ldots, a_{i,m} \in \mathbb{N}_0$ satisfying $a_{i,1} + \cdots + a_{i,m} = a_i$, we have

$$L(\phi_{a_{i,1},\ldots,a_{i,m}}(f)) = L(\phi_{a_{i,1},\ldots,a_{i,m}}(x_i^{a_i})) = \frac{a_i!}{a_{i,1}! \cdots a_{i,m}!} x_{i,1}^{a_{i,1}} x_{i,2}^{a_{i,2}} \cdot \ldots \cdot x_{i,m}^{a_{i,m}}.$$

For positive characteristic p, a_i is strictly smaller than p by hypothesis, so the coefficient is nonzero. Moreover, $\phi_{a_{i,1},\ldots,a_{i,m}}(f) \in I_B$ by the previous lemma. This finishes the proof. ■

Consider the natural action of the symmetric group S_n on $F[V]$. It is well known that $L(I_A) = (x_1, x_2^2, \ldots, x_n^n)$, see, for example, [27, Proposition 1.1]. So, the theorem applies and we get the following corollary, which also appears as the special case $q = 1$ in [6, Lemma 3.1].

Corollary 14. Let F be a field of characteristic p and V be the natural S_n-module. If $p = 0$ or $p > n$, then, for any positive integer m, we have

$$\operatorname{topdeg} F[V^m]_{S_n} = \binom{n}{2}. \qquad \square$$

We want to emphasize here again the sharp contrast to the case $0 < p \leq n$, where by Theorem 8 we have $\lim_{m\to\infty} \operatorname{topdeg} F[V^m]_{S_n} = \infty$.

5 A New Proof for Steinberg's Theorem

The following might be one of the most celebrated results on coinvariants.

Theorem 15 (Steinberg)**.** For any faithful G-module V, we have

$$|G| \leq \dim F[V]_G$$

with equality if and only if $F[V]^G$ is polynomial. □

Note that by the famous Chevalley–Shephard-Todd–Serre–Theorem, $F[V]^G$ being polynomial always implies G is a reflection group, and in the nonmodular case the converse is also true. Steinberg [25] proves the theorem above for the complex numbers using analysis. More recently, Smith [23] generalized the theorem to arbitrary fields, using some heavy machinery from homological algebra. We now give an almost elementary proof.

Proof. The group G acts naturally on the quotient field $F(V)$, hence by Galois theory we have $\dim_{F(V)^G} F(V) = |G|$. Let S be a minimal generating set for $F[V]$ as a module over $F[V]^G$. Then by the graded Nakayama lemma [5, Lemma 3.5.1], S projects injectively onto a vector space basis for $F[V]_G$. Moreover, from Proposition 16, we get that S also generates $F(V)$ as an $F(V)^G$-vector space. So, we have

$$\dim F[V]_G = |S| \geq \dim_{F(V)^G} F(V) = |G|.$$

If equality holds, then S is a basis for $F(V)$ over $F(V)^G$, so it is $F(V)^G$- and hence $F[V]^G$-linearly independent. This implies that $F[V]$ is a free $F[V]^G$-module. Now by [1, Corollary 6.2.3], we get that $F[V]^G$ is polynomial. The reverse implication is straightforward: If $F[V]^G$ is polynomially generated by invariants of degree $d_1, \ldots, d_n$, the Cohen–Macaulayness of $F[V]$ implies that $F[V]$ is freely generated over $F[V]^G$ by $d_1 \cdot \ldots \cdot d_n$ many generators, and it is well known that this product equals $|G|$, see Smith's proof [23] for the details. ■

Above we used the following well-known proposition. We give a proof here due to lack of reference. Let $\mathrm{Quot}(D)$ denote the quotient field of an integral domain D.

Proposition 16. Assume $A \subseteq R$ is an integral extension of integral domains. Then

$$\mathrm{Quot}(R) = \left\{ \frac{r}{a} \middle| r \in R,\ a \in A \setminus \{0\} \right\} = (A \setminus \{0\})^{-1} R.$$

In particular, if $S \subseteq R$ generates R as an A-module, then S generates $\mathrm{Quot}(R)$ as a $\mathrm{Quot}(A)$-vector space. □

Proof. Assume $\frac{f}{g} \in \mathrm{Quot}(R)$ with $f, g \in R$ and $g \neq 0$. Let

$$g^t + a_{t-1}g_{t-1} + \cdots + a_1 g + a_0 = 0$$

be a monic equation of minimal degree satisfied by g. Then $a_0 \neq 0$ and dividing this equation by g shows $\frac{a_0}{g} \in R$. Therefore, $\frac{f}{g} = \frac{f}{a_0} \cdot \frac{a_0}{g} \in (A \setminus \{0\})^{-1} R$. ■

Acknowledgement

We thank M. Domokos for pointing out that Corollary 14 has already appeared in his paper [6]. We also thank the anonymous referee for useful comments.

Funding

The visit of the first author to Bilkent University was funded by Tübitak and that of the second author to TU München was funded by Gregor Kemper. This research was partially supported by Tübitak-Tbag/112T113 (to M.S.).

References

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

[2] Broer, A., V. Reiner, L. Smith, and P. Webb. “Extending the coinvariant theorems of Chevalley, Shephard-Todd, Mitchell, and Springer.” *Proceedings of the London Mathematical Society* (3) 103, no. 5 (2011): 747–85.

[3] Campbell, H. E. A., I. P. Hughes, R. J. Shank, and D. L. Wehlau. “Bases for rings of coinvariants.” *Transformation of Groups* 1, no. 4 (1996): 307–36.

[4] Cziszter, K. and M. Domokos. “On the generalized Davenport constant and the Noether number.” *Central European Journal of Mathematics* 11, no. 9 (2013): 1605–15.

[5] Derksen, H. and G. Kemper. “Computational Invariant Theory.” *Invariant Theory and Algebraic Transformation Groups, I*. Encyclopaedia of Mathematical Sciences 130. Berlin: Springer, 2002.

[6] Domokos, M. “Vector invariants of a class of pseudoreflection groups and multisymmetric syzygies.” *Journal of Lie Theory* 19, no. 3 (2009): 507–25.

[7] Draisma, J., G. Kemper, and D. Wehlau. “Polarization of separating invariants.” *Canadian Journal of Mathematics* 60, no. 3 (2008): 556–71.

[8] Dwyer, W. G. and C. W. Wilkerson. “Poincaré duality and Steinberg’s theorem on rings of coinvariants.” *Proceedings of the American Mathematical Society* 138, no. 10 (2010): 3769–75.

[9] Fleischmann, P. “The Noether bound in invariant theory of finite groups.” *Advances in Mathematics* 156, no. 1 (2000): 23–32.

[10] Fleischmann, P. and W. Lempken. “On Degree Bounds for Invariant Rings of Finite Groups over Finite Fields.” In *Finite Fields: Theory, Applications, and Algorithms (Waterloo, Ontario, 1997)*, 33–41. Contemporary Mathematics 225. Providence, RI: American Mathematical Society, 1999.

[11] Fleischmann, P., M. Sezer, R. J. Shank, and C. F. Woodcock. “The Noether numbers for cyclic groups of prime order.” *Advances in Mathematics* 207, no. 1 (2006): 149–55.

[12] Fogarty, J. “On Noether’s bound for polynomial invariants of a finite group.” *Electronic Research Announcements of the American Mathematical Society* 7 (2001): 5–7 (electronic).

[13] Gao, W. and A. Geroldinger. “Zero-sum problems in finite abelian groups: a survey.” *Expositiones Mathematicae* 24, no. 4 (2006): 337–69.

[14] Kane, R. “Poincaré duality and the ring of coinvariants.” *Canadian Mathematical Bulletin* 37, no. 1 (1994): 82–8.

[15] Knop, F. “On Noether’s and Weyl’s bound in positive characteristic.” In *Invariant Theory in All Characteristics*, 175–188. CRM Proceedings and Lecture Notes 35. Providence, RI: American Mathematical Society, 2004.

[16] Kohls, M. and M. Sezer. “Gröbner bases for the Hilbert ideal and coinvariants of the dihedral group D_{2p}.” *Mathematische Nachrichten* 285, no. 16 (2012): 1974–80.

[17] Olson, J. E. “A combinatorial problem on finite Abelian groups. I.” *Journal of Number Theory* 1, no. 1 (1969): 8–10.

[18] Olson, J. E. “A combinatorial problem on finite Abelian groups. II.” *Journal of Number Theory* 1, no. 2 (1969): 195–9.

[19] Richman, D. R. “Invariants of finite groups over fields of characteristic p.” *Advances in Mathematics* 124, no. 1 (1996): 25–48.

[20] Schmid, B. J. “Finite Groups and Invariant Theory.” In *Topics in Invariant Theory (Paris, 1989/1990)*, 35–66. Lecture Notes in Mathematics 1478. Berlin: Springer, 1991.

[21] Sezer, M. “Coinvariants and the regular representation of a cyclic P-group.” *Mathematische Zeitschrift* 273, no. 1–2 (2013): 539–46.

[22] Sezer, M. and R. J. Shank. “On the coinvariants of modular representations of cyclic groups of prime order.’ ’*Journal of Pure and Applied Algebra* 205, no. 1 (2006): 210–25.

[23] Smith, L. “A modular analog of a theorem of R. Steinberg on coinvariants of complex pseudoreflection groups.” *Glasgow Mathematical Journal* 45, no. 1 (2003): 69–71.

[24] Smith, L. “On R. Steinberg’s theorem on algebras of coinvariants.” *Forum Mathematicum* 21, no. 6 (2009): 965–79.

[25] Steinberg, R. “Differential equations invariant under finite reflection groups.” *Transactions of the American Mathematical Society* 112 (1964): 392–400.

[26] Symonds, P. "On the Castelnuovo-Mumford regularity of rings of polynomial invariants." *Annals of Mathematics* (2) 174, no. 1 (2011): 499–517.

[27] Wada, T. and H. Ohsugi. "Gröbner bases of Hilbert ideals of alternating groups." *Journal of Symbolic Computation* 41, no. 8 (2006): 905–8.

[28] Wehlau, D. L. "The Noether number in invariant theory." *Comptes Rendus Mathématiques de l'Académie des Sciences. La Société Royale du Canada. Mathematical Reports of the Academy of Science. The Royal Society of Canada* 28, no. 2 (2006): 39–62.