Journal of Algebra 423 (2015) 87–92

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Decomposing modular coinvariants

Müfit Sezer [1]

Department of Mathematics, Bilkent University, Ankara 06800, Turkey

ARTICLE INFO

Article history:
Received 18 June 2014
Available online 24 October 2014
Communicated by Gunter Malle

Keywords:
Coinvariants
Modular actions

ABSTRACT

We consider the ring of coinvariants for a modular representation of a cyclic group of prime order p. We show that the classes of the terminal variables in the coinvariants have nilpotency degree p and that the coinvariants are a free module over the subalgebra generated by these classes. An incidental result we have is a description of a Gröbner basis for the Hilbert ideal and a decomposition of the corresponding monomial basis for the coinvariants with respect to the monomials in the terminal variables.

Introduction

Let V denote a finite dimensional representation of a finite group G over a field $\mathbf{F}$. The induced action on the dual V^* extends as degree preserving algebra automorphisms to the symmetric algebra $S(V^*)$ which we denote by $\mathbf{F}[V]$. The ring of invariant polynomials $\mathbf{F}[V]^G := \{f \in \mathbf{F}[V] \mid g(f) = f \ \forall g \in G\}$ is a graded finitely generated subalgebra. The Hilbert ideal I is the ideal $\mathbf{F}[V]^G_+ \cdot \mathbf{F}[V]$ in $\mathbf{F}[V]$ generated by invariants of positive degree. In this paper we study the ring of coinvariants which is the quotient ring

$$\mathbf{F}[V]_G := \mathbf{F}[V]/I.$$

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

[1] The author is supported by a grant from Tübitak: 112T113.

http://dx.doi.org/10.1016/j.jalgebra.2014.08.059
0021-8693/© 2014 Elsevier Inc. All rights reserved.

Since G is finite, $\mathbf{F}[V]_G$ is a finite dimensional vector space. Note also that coinvariants are naturally a G-module as I is closed under the action of G. Coinvariants often contain information about the invariants. For instance, if $|G|$ is a unit in $\mathbf{F}$, then $\mathbf{F}[V]^G$ is polynomial if and only if $\mathbf{F}[V]_G$ satisfies Poincaré duality, see [4,6,13]. Even in the modular case, that is when $|G|$ is divisible by the characteristic of $\mathbf{F}$, some weaker versions of this equivalence still hold in small dimensions see [8,12]. Since $\mathbf{F}[V]_G$ is a finite dimensional vector space, the largest degree of a non-zero component is also finite. It is well known that in the non-modular case the top degree is bounded by the group order but it can be arbitrarily large otherwise [7]. In many modular cases the top degree of the coinvariants also coincides with the maximum degree of an indecomposable invariant and getting efficient bounds for the top degree has been critical when studying effective generation of invariant rings, see for example [5,10].

We now fix our setup. Let p be a prime integer and $\mathbf{F}$ a field of characteristic p. For the rest of the paper, G denotes the cyclic group of prime order p. Fix a generator σ of G. There are exactly p indecomposable G-modules $V_1, \dots, V_p$ over $\mathbf{F}$ and each indecomposable module V_i is afforded by a Jordan block of dimension i with 1's on the diagonal. Let V be an arbitrary G-module over $\mathbf{F}$. Assume that V has l summands so we can write $V = \sum_{1 \leq j \leq l} V_{n_j}$. Since adding a trivial summand to a module does not affect the coinvariants we assume as well that $n_j > 1$ for $1 \leq j \leq l$. We set $\mathbf{F}[V] = \mathbf{F}[X_{i,j} \mid 1 \leq i \leq n_j,\ 1 \leq j \leq l]$ 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 $\sigma(X_{1,j}) = X_{1,j}$. Following the established convention, we call the variables $X_{n_j,j}$ for $1 \leq j \leq l$ terminal variables. We use graded reverse lexicographic order on the monomials in $\mathbf{F}[V]$ with $X_{1,j} < \cdots < X_{n_j,j}$. We denote the leading monomial of a polynomial f by $\mathrm{LM}(f)$. We also use lower case letters to denote the images of the variables in the coinvariants.

Certain examples of coinvariants for modular representations of G are studied in [9] and for each example, among other things, a reduced Gröbner basis for the Hilbert ideal and the corresponding monomial basis for the coinvariants are given. The goal of this paper is to demonstrate that some of the properties of the coinvariants and the Hilbert ideal that are identified in the cases studied in that source hold in general for an arbitrary module V. We show that the Hilbert ideal I is generated by the orbit products of $X_{n_j,j}$ for $1 \leq j \leq l$ (which we denote by $N(X_{n_j,j})$) and polynomials in $A := \mathbf{F}[X_{i,j} \mid 1 \leq i \leq n_j - 1,\ 1 \leq j \leq l]$. Notice that $\mathrm{LM}(N(X_{n_j,j})) = X^p_{n_j,j}$. Therefore we get that, apart from the monomials $X^p_{n_j,j}$ for $1 \leq j \leq l$, no monomial in the unique minimal generating set for the lead term ideal of I is divisible by any $X_{n_j,j}$ for $1 \leq j \leq l$. We go on to prove that there is an isomorphism of graded $\mathbf{F}$-algebras

$$\mathbf{F}[x_{n_1,1}, \dots, x_{n_l,l}] \cong \mathbf{F}[t_1, \dots, t_l]/\left(t_1^p, \dots, t_l^p\right),$$

where $t_1, \dots, t_l$ are independent variables. Moreover, we show that $\mathbf{F}[V]_G$ is a free module over $\mathbf{F}[x_{n_1,1}, \dots, x_{n_l,l}]$.

For more background on modular invariant theory we refer the reader to [2] and [3].

1. Reductions and results

For a polynomial $f \in \mathbf{F}[V]$ and $1 \le j \le l$, let $f^{(i,j)}$ denote the i-th partial derivative of f with respect to $X_{n_j,j}$. We first observe that the action of σ commutes with differentiation with respect to $X_{n_j,j}$.

Lemma 1. *Let $f \in \mathbf{F}[V]$ and fix $1 \le j \le l$. Then $\sigma(f^{(1,j)}) = \sigma(f)^{(1,j)}$. Therefore $\mathbf{F}[V]^G$ is closed under differentiation with respect to $X_{n_j,j}$.*

Proof. Since both differentiation and the action of σ are additive it is enough to assume that $f = gX_{n_j,j}^k$, where g is a polynomial in the variables except $X_{n_j,j}$ and k is a non-negative integer. First assume that k is positive. Notice that

$$\sigma\bigl(f^{(1,j)}\bigr) = \sigma\bigl(kgX_{n_j,j}^{k-1}\bigr) = k\sigma(g)(X_{n_j,j} + X_{n_j-1,j})^{k-1}.$$

On the other hand we also have

$$\sigma(f)^{(1,j)} = \bigl(\sigma(g)(X_{n_j,j} + X_{n_j-1,j})^k\bigr)^{(1,j)} = k\sigma(g)(X_{n_j,j} + X_{n_j-1,j})^{k-1}.$$

Since the action of σ does not increase the $X_{n_j,j}$ degree of a polynomial, both sides of the identity in the assertion of the lemma are zero if $k = 0$. Hence the result follows. □

Notice that since I consists of finite sums $\sum f_i g_i$ with $f_i \in \mathbf{F}[V]_+^G$ and $g_i \in \mathbf{F}[V]$, by the Leibniz rule and the previous lemma we get that I is closed under differentiation with respect to $X_{n_j,j}$ for $1 \le j \le l$ as well. We also note a combinatorial result that applies to any polynomial in $\mathbf{F}[V]$ whose degree in a terminal variable is strictly less than p.

Lemma 2. *Let $f \in \mathbf{F}[V]$ be a polynomial of degree $k < p$ in one of the terminal variables, say $X_{n_j,j}$. Write $f = f_k X_{n_j,j}^k + f_{k-1} X_{n_j,j}^{k-1} + \cdots + f_0$, where $f_k, \ldots, f_0$ are polynomials in the variables except $X_{n_j,j}$. Then we have*

$$\sum_{0 \le i \le k} \frac{(-1)^i}{i!} X_{n_j,j}^i f^{(i,j)} = f_0.$$

Proof. Fix d for some $0 \le d \le k$. Consider $\sum_{0 \le i \le k} \frac{(-1)^i}{i!} X_{n_j,j}^i (f_d X_{n_j,j}^d)^{(i,j)}$. This summation is equal to

$$\begin{aligned} 2\sum_{0 \le i \le d} \frac{(-1)^i}{i!} X_{n_j,j}^i \bigl(f_d X_{n_j,j}^d\bigr)^{(i,j)} &= \sum_{0 \le i \le d} \frac{(-1)^i}{i!} X_{n_j,j}^i d \cdots (d-i+1) f_d X_{n_j,j}^{d-i} \\ &= \sum_{0 \le i \le d} (-1)^i \binom{d}{i} f_d X_{n_j,j}^d. \end{aligned}$$

Notice that this sum is f_0 if $d = 0$ and is zero otherwise. This gives the desired equality. □

Theorem 3. *The Hilbert ideal I is generated by the orbit products $N(X_{n_j,j})$ for $1 \le j \le l$ and polynomials in A. Moreover, the lead term ideal of I is generated by $X_{n_j,j}^p$ for $1 \le j \le l$ and monomials in A.*

Proof. Let $f \in \mathbf{F}[V]^G$. By [11, Proposition 2.1] f has a decomposition

$$f = g_1 N(X_{n_1,1}) + g_2 N(X_{n_2,2}) + \cdots + g_l N(X_{n_l,l}) + r,$$

where $r \in \mathbf{F}[V]^G$ is the normal form of f with respect to the Gröbner basis $\{N(X_{n_1,1}), \ldots, N(X_{n_l,l})\}$ of the ideal $(N(X_{n_1,1}), \ldots, N(X_{n_l,l}))$ in $\mathbf{F}[V]$. Therefore we may assume that $f \in \mathbf{F}[V]^G$ is of degree $< p$ as a polynomial in $X_{n_j,j}$ for $1 \le j \le l$. Say, as a polynomial in $X_{n_1,1}$, f has degree $k < p$ and write $f = f_k X_{n_1,1}^k + f_{k-1} X_{n_1,1}^{k-1} + \cdots + f_0$, where $f_k, \ldots, f_0$ are polynomials in all variables except $X_{n_1,1}$. By Lemma 1 all derivatives of f with respect to $X_{n_1,1}$ are also invariant. Then the identity $\sum_{0 \le i \le k} \frac{(-1)^i}{i!} X_{n_1,1}^i f^{(i,1)} = f_0$ from the previous lemma gives that $f_0 \in I$. Furthermore, since the coefficients of f and f_0 are units in this identity it also gives the equality of the ideals

$$\left(f, f^{(1,1)}, \ldots, f^{(k,1)}\right) = \left(f_0, f^{(1,1)}, \ldots, f^{(k,1)}\right)$$

in $\mathbf{F}[V]$. Therefore f is in the ideal generated by $f_0, f^{(1,1)}, \ldots, f^{(k,1)}$. Note that these polynomials have degree $< k$ in $X_{n_1,1}$. Moreover since differentiation with respect to $X_{n_1,1}$ does not increase the degree with respect to any variable, their degrees with respect to other terminal variables are still strictly less than p. Therefore by induction on the degree k we get that I is generated by the norms $N(X_{n_j,j})$ for $1 \le j \le l$ and polynomials that are of degree zero in $X_{n_1,1}$ and of degree $< p$ in the $X_{n_j,j}$ for $2 \le j \le l$. Since I is closed under differentiation with respect to any terminal variable, we can repeat this process by applying the identity of the previous lemma (with respect to other terminal variables) to the successive constant terms. So we get that I is generated by $N(X_{n_j,j})$ for $1 \le j \le l$ and polynomials in A. Finally, recall that by Buchberger's algorithm a Gröbner basis is obtained by reduction of S-polynomials by polynomial division, see [1, §1.7]. But the S-polynomial of two polynomials in A is also in A and via polynomials in A it also reduces to a polynomial in A. Moreover, the S-polynomial of $N(X_{n_j,j})$ and a polynomial in A and the S-polynomial of a pair $N(X_{n_j,j})$ and $N(X_{n_{j'},j'})$ reduce to zero since their leading monomials are pairwise relatively prime for any $1 \le j \ne j' \le l$. Hence the result follows. □

Remark 4. Let Λ denote the set of monomials in $\mathbf{F}[V]$ that do not belong to the lead term ideal of I. Then the images of monomials in Λ in $\mathbf{F}[V]_G$ form a vector space basis for $\mathbf{F}[V]_G$. The previous theorem gives us that a monomial $M \in A$ is in Λ if and only if $M X_{n_1,1}^{k_1} \cdots X_{n_l,l}^{k_l}$ is in Λ for all $0 \le k_j \le p-1$ for $1 \le j \le l$. It follows that

$(1+t+t^2+\cdots+t^{p-1})^l$ divides the Hilbert polynomial of $\mathbf{F}[V]_G$ and that the vector space dimension of $\mathbf{F}[V]_G$ is divisible by p^l. In the next theorem we show that this is not a combinatorial accident.

Theorem 5. *We have an isomorphism of graded* $\mathbf{F}$*-algebras*

$$\mathbf{F}[x_{n_1,1},\dots,x_{n_l,l}] \cong \mathbf{F}[t_1,\dots,t_l]/\bigl(t_1^p,\dots,t_l^p\bigr),$$

where $t_1,\dots,t_l$ *are independent variables. Moreover,* $\mathbf{F}[V]_G$ *is a free module over* $\mathbf{F}[x_{n_1,1},\dots,x_{n_l,l}]$*. In particular,* $\frac{H_{\mathbf{F}[V]_G}(t)}{(1+t+t^2+\cdots+t^{p-1})^l} \in \boldsymbol{Z}[t]$*, where* $H_{\mathbf{F}[V]_G}(t)$ *is the Hilbert polynomial of* $\mathbf{F}[V]_G$*.*

Proof. We first show that the nilpotency degree of $x_{n_j,j}$ in $\mathbf{F}[V]_G$ is p for $1 \le j \le l$. Pick $0 < i < p$. Then $x^i_{n_j,j} = 0$ for some $1 \le j \le l$ implies that $X^i_{n_j,j} \in I$. This is a contradiction to the description of the lead term ideal of I given by the previous theorem. Next we show that $x^p_{n_j,j} = 0$ for $1 \le j \le l$. Equivalently, we prove $X^p_{n_j,j} \in I$. Without loss of generality take $j = 1$. Set $\tilde{N} = N(X_{n_1,1}) - X^p_{n_1,1}$. Notice that $\tilde{N}$ is a polynomial of degree $< p$ in $X_{n_1,1}$. Call this degree k. So Lemma 2 applies and we get $\sum_{0\le i\le k} \frac{(-1)^i}{i!} X^i_{n_1,1}\tilde{N}^{(i,1)} = f_0$, where f_0 is the constant term (as a polynomial in $X_{n_1,1}$) of $\tilde{N}$. But since they differ by $X^p_{n_1,1}$, the constant terms of $\tilde{N}$ and $N(X_{n_1,1})$ are equal. On the other hand since $N(X_{n_1,1})$ is the orbit product of $X_{n_1,1}$, all terms in $N(X_{n_1,1})$ are divisible by $X_{n_1,1}$. It follows that $f_0 = 0$. Moreover, since $\tilde{N}$ and $N(X_{n_1,1})$ differ by a polynomial whose derivative with respect to $X_{n_1,1}$ is zero, their derivatives are all equal. But all derivatives of $N(X_{n_1,1})$ are invariant by Lemma 1. It follows that $\tilde{N}^{(i,1)} \in \mathbf{F}[V]^G$ for $0 < i \le k$. Therefore the equality $\sum_{0\le i\le k} \frac{(-1)^i}{i!} X^i_{n_1,1}\tilde{N}^{(i,1)} = 0$ gives us that $\tilde{N} \in I$. So $X^p_{n_1,1} \in I$ as well.

Let $t_1,\dots,t_l$ be independent variables and consider the natural graded surjection from $\mathbf{F}[t_1,\dots,t_l]$ to $\mathbf{F}[x_{n_1,1},\dots,x_{n_l,l}]$. Since nilpotency degree of $x_{n_j,j}$ is p for $1 \le j \le l$, the kernel of this map contains the ideal $(t_1^p,\dots,t_l^p)$. If this ideal does not contain the kernel, then I contains a polynomial in $X_{n_1,1},\dots,X_{n_l,l}$ such that no monomial in that polynomial is divisible by any $X^p_{n_j,j}$ for $1 \le j \le l$. This is a contradiction to the description of the lead term ideal of I in the previous theorem. So we establish the isomorphism in the assertion of the theorem.

Secondly, let Λ' denote the set of monomials in A that do not belong to the lead term ideal of I, i.e., $\Lambda' = \Lambda \cap A$. Then by the previous remark the images of these monomials in $\mathbf{F}[V]_G$ generate $\mathbf{F}[V]_G$ as a module over $\mathbf{F}[x_{n_1,1},\dots,x_{n_l,l}]$. In fact they generate freely since $MX^{k_1}_{n_1,1}\cdots X^{k_l}_{n_l,l}$ is in Λ for all $M \in \Lambda'$ and $0 \le k_j \le p-1$ for $1 \le j \le l$ and the images of monomials in Λ form a vector space basis for $\mathbf{F}[V]_G$.

Final statement follows easily from the second one because the Hilbert polynomial of $\mathbf{F}[t_1,\dots,t_l]/(t_1^p,\dots,t_l^p)$ is $(1+t+t^2+\cdots+t^{p-1})^l$. □

Acknowledgments

This study was done during my visit to University of Nebraska on Fulbright Visiting Scholar Program. I thank Luchezar Avramov for many helpful discussions. Also, initially this paper was targeting indecomposable representations only. I thank Jim Shank for pointing out that the argument generalizes to decomposable representations as well and the referee for helpful comments.

References

[1] William W. Adams, Philippe Loustaunau, An Introduction to Gröbner Bases, Grad. Stud. Math., vol. 3, American Mathematical Society, Providence, RI, 1994.

[2] H.E.A. Eddy Campbell, David L. Wehlau, Modular invariant theory, in: Invariant Theory and Algebraic Transformation Groups, in: Encyclopaedia Math. Sci., vol. 139, Springer-Verlag, Berlin, 2011, p. 8.

[3] Harm Derksen, Gregor Kemper, Computational invariant theory, in: Invariant Theory and Algebraic Transformation Groups, I, in: Encyclopaedia Math. Sci., vol. 130, Springer-Verlag, Berlin, 2002.

[4] W.G. Dwyer, C.W. Wilkerson, Poincaré duality and Steinberg's theorem on rings of coinvariants, Proc. Amer. Math. Soc. 138 (10) (2010) 3769–3775.

[5] P. Fleischmann, M. Sezer, R.J. Shank, C.F. Woodcock, The Noether numbers for cyclic groups of prime order, Adv. Math. 207 (1) (2006) 149–155.

[6] Richard Kane, Poincaré duality and the ring of coinvariants, Canad. Math. Bull. 37 (1) (1994) 82–88.

[7] M. Kohls, M. Sezer, On the top degree of coinvariants, Int. Math. Res. Not. IMRN (2014), http://dx.doi.org/10.1093/imrn/rnt158, in press.

[8] Tzu-Chun Lin, Rings of coinvariants and p-subgroups, Proc. Amer. Math. Soc. 138 (12) (2010) 4243–4247.

[9] Müfit Sezer, R. James Shank, On the coinvariants of modular representations of cyclic groups of prime order, J. Pure Appl. Algebra 205 (1) (2006) 210–225.

[10] Müfit Sezer, R. James Shank, Rings of invariants for modular representations of the klein four group, Trans. Amer. Math. Soc. (2014), in press.

[11] R. James Shank, David L. Wehlau, Noether numbers for subrepresentations of cyclic groups of prime order, Bull. Lond. Math. Soc. 34 (4) (2002) 438–450.

[12] Larry Smith, On a theorem of R. Steinberg on rings of coinvariants, Proc. Amer. Math. Soc. 131 (4) (2003) 1043–1048 (electronic).

[13] Robert Steinberg, Differential equations invariant under finite reflection groups, Trans. Amer. Math. Soc. 112 (1964) 392–400.