Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 318 (2007) 372–376
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

A note on the Hilbert ideals of a cyclic group of prime order ☆

Müfit Sezer *

Department of Mathematics, Bilkent University, Ankara 06800, Turkey

Received 29 December 2006

Available online 17 September 2007

Communicated by Harm Derksen

Abstract

The Hilbert ideal is the ideal generated by positive degree invariant polynomials of a finite group. For a cyclic group of prime order p, we show that the image of the transfer lie in the ideal generated by invariants of degree at most $p-1$. Consequently we show that the Hilbert ideal corresponding to an indecomposable representation is generated by polynomials of degree at most p, confirming a conjecture of Harm Derksen and Gregor Kemper for this case.

Keywords: Invariant theory; Hilbert ideals; Degree bounds

Introduction

Let V denote a finite dimensional representation of a finite group G over a field F. Then there is an induced action on V^* which extends to a degree preserving action by ring automorphisms on the symmetric algebra $S(V^*)$. It is well known that the algebra of invariant polynomials

$$S(V^*)^G = \left\{ f \in S(V^*) \;\middle|\; g(f) = f,\ \forall g \in G \right\}$$

is a finitely generated subalgebra. An important characteristic of $S(V^*)^G$ is the Noether number, $\beta(V)$, which is defined to be the smallest integer n such that $S(V^*)^G$ is generated by homoge-

☆ Research supported by a grant from Bogazici University Research Fund: 06HB601.
* Current address: Department of Mathematics, Bogazici University, Bebek 34342, Istanbul, Turkey.
E-mail address: mufit.sezer@boun.edu.tr.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2007.08.022

neous polynomials of degree at most n. By a theorem due to Noether [8] in characteristic 0 and to Fleischmann [2] and Fogarty [4] in general non-modular characteristic ($|G| \in F^*$), $\beta(V) \leqslant |G|$. On the other hand, for any group G, Richman [9] constructed modular representations with arbitrarily large $\beta(V)$. Therefore the restriction on $|G|$ cannot be removed. It has been conjectured that $\beta(V) \leqslant \max\{|G|, \dim(V)(|G|-1)\}$, [1, 3.9.10]. The Noether number for an arbitrary representation of a cyclic group of prime order has been computed in [3]. We refer the reader to [6] and [11] for an overview of known results on Noether numbers.

The Hilbert ideal which we denote by $S(V^*)^{G,+} \cdot S(V^*)$ is the ideal in $S(V^*)$ generated by invariants of positive degree. Derksen and Kemper [1, 3.8.6 (b)] has made the following conjecture.

Conjecture 1. *The Hilbert ideal is generated by homogeneous elements of degree at most $|G|$.*

Notice that the bound on $\beta(V)$ due to Noether, Fleischmann and Fogarty implies the assertion of this conjecture for non-modular representations. As for modular representations, a reduced Gröbner basis for the Hilbert ideal for several representations of a cyclic group of prime order is given in [10] and in all cases considered there, calculations confirm Conjecture 1. Moreover, if V is a permutation module Conjecture 1 is also known to be true, see [2, 4.1]. Here we study the situation where G is a cyclic group of prime order. Our main result is that the image of the transfer lie in the ideal in $S(V^*)$ generated by invariants of degree at most $p-1$, see Theorem 4. Consequently we recover the assertion of Conjecture 1 for indecomposable modules.

For the remainder of the paper, let F be a field of characteristic p for a prime number p and let G be the cyclic group of order p and σ a generator of G. It is well known that there are exactly p indecomposable G-modules $V_1, V_2, \ldots, V_p$ and the action of σ on V_n is afforded by a Jordan block of dimension n with ones on the diagonal. Moreover V_p is the only indecomposable module which is projective. Let Δ denote $\sigma - 1$. Moreover, define $\mathrm{Tr} = \sum_{l=1}^{p} \sigma^l$ which we will call the transfer map. Note that the space of fixed points V_n^G has dimension one and that every invariant in the free module V_p is in the image of the transfer since it is a multiple of the sum of basis elements which are permuted by G.

We recommend [1] and [7] as a reference for invariant theory of finite groups.

Reductions in the Hilbert ideal

Consider the decomposition $V^* = \bigoplus_{i=1}^{k} W_i$ of V^* into a direct sum of indecomposable modules. Let z_i be a G-module generator for W_i and define $d_i = \dim W_i$. Then

$$\left\{\Delta^j z_i \;\middle|\; 1 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant d_i - 1\right\}$$

is a basis for V^*. Consider the subalgebra A in $S(V^*)$ generated by these basis elements except the terminal variables, i.e.,

$$A = F\left[\left\{\Delta^j z_i \;\middle|\; 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant d_i - 1\right\}\right].$$

We use a graded reverse lexicographic with $\Delta^j z_i > \Delta^{j+1} z_i$ for $0 \leqslant j \leqslant d_i - 1$. Let $m = w_1 w_2 \cdots w_{p-1}$ be a monomial of degree $p-1$ in $S(V^*)$. Define $\Delta_m = u_1 u_2 \cdots u_{p-1}$, where $\Delta(w_i) = u_i$. Note that Δ_m is either 0 or a monomial of degree $p-1$ in A. Also notice that

for each monomial $m' \in A$, there exists a monomial $m \in S(V^*)$ such that $\Delta_m = m'$. For $S \subseteq \{1, 2, \ldots, p-1\}$, define $X_S = \prod_{j\in S} w_j$ and $X_{S'} = \frac{m}{X_S}$. For a monomial t in $S(V^*)$ define

$$F_{m,t} = \sum_{S\subseteq\{1,2,\ldots,p-1\}} (-1)^{|S|} X_{S'} \operatorname{Tr}(tX_S).$$

Note that $F_{m,t}$ is in $S(V^*)^{G,+} \cdot S(V^*)$. We will denote the leading term of a polynomial f with $\operatorname{LT}(f)$, and the subspace of A consisting of polynomials of degree i including 0 with A_i. The following lemma includes a generalization of [3, 3.1, 3.2].

Lemma 2. *The polynomial $F_{m,t}$ has the following properties*:

1. $F_{m,t} = 0$ *if* $\Delta_m = 0$.
2. $\operatorname{LT}(F_{m,t}) = -\Delta_m t$ *if* $\Delta_m \neq 0$.
3. $F_{m,t} \in A_{p-1} \cdot S(V^*)$.

Proof. Note that

$$\sigma^l(t)\left(\prod_{j=1}^{p-1}\bigl(w_j - \sigma^l(w_j)\bigr)\right) = \sum_{S\subseteq\{1,2,\ldots,p-1\}} (-1)^{|S|} X_{S'}\sigma^l(tX_S).$$

Summing over $l \in \boldsymbol{F}_p$ yields

$$F_{m,t} = \sum_{l\in\boldsymbol{F}_p} \sigma^l(t)\left(\prod_{j=1}^{p-1}\bigl(w_j - \sigma^l(w_j)\bigr)\right).$$

Note that $\Delta_m = 0$ if and only if $u_i = 0$ for some $1 \leqslant i \leqslant p-1$. In this case $w_i - \sigma^l(w_i) = 0$ for all $l \in \boldsymbol{F}_p$. Hence all summands in $F_{m,t}$ are zero. Now we consider the case $\Delta_m \neq 0$ and capture the leading term of $F_{m,t}$ from the summation above. Note that

$$\operatorname{LT}\bigl(\sigma^l(t)\bigr) = t.$$

Furthermore since $1 - \sigma^l = (1 + \sigma + \sigma^2 + \cdots + \sigma^{l-1}) \cdot (1 - \sigma)$, it follows that $w_j - \sigma^l(w_j) = (1 + \sigma + \sigma^2 + \cdots + \sigma^{l-1})(-u_j)$ and therefore we have

$$\operatorname{LT}\bigl(w_j - \sigma^l(w_j)\bigr) = -lu_j.$$

Thus the lead term of $\sigma^l(t)(\prod_{j=1}^{p-1}(w_j - \sigma^l(w_j)))$ is $(-l)^{p-1}t\prod_{j=1}^{p-1} u_j = l^{p-1}\Delta_m t$. Therefore the leading term of $F_{m,t}$ is $\sum_{l\in\boldsymbol{F}_p} l^{p-1}\Delta_m t = -\Delta_m t$.

For the last assertion, note that the variables that appear in $w_j - \sigma^l(w_j)$ are in A. Thus $F_{m,t}$ is a sum of monomials all divisible by a product of $p-1$ variables in A. □

Lemma 3. $A_{p-1} \subseteq S(V^*)^{G,+} \cdot S(V^*)$.

Proof. Let f be a polynomial in $A_{p-1} \setminus S(V^*)^{G,+} \cdot S(V^*)$ with minimal leading monomial m'. Choose $t = 1$. Since $m' \in A$, there exists a monomial $m \in S(V^*)$ such that $\Delta_m = m'$. From the second part of the previous lemma the leading term of $F_{m,1}$ is $-m'$. Therefore the leading monomial of $m' + F_{m,1}$ is strictly smaller than m'. Furthermore we have $m' + F_{m,1} \in A_{p-1}$ by the last assertion of the same lemma, which yields a contradiction. □

For a positive integer i, let $S(V^*)^{G,+}_{\leqslant i} \cdot S(V^*)$ denote the ideal in $S(V^*)$ generated by invariants of positive degree at most i.

Theorem 4. *The image of the transfer is contained in* $S(V^*)^{G,+}_{\leqslant p-1} \cdot S(V^*)$.

Proof. Let h be a monomial in $S(V^*)$ of degree strictly greater than $p-1$. Write $h = mt$, where m and t are monomials and the degree of m is $p-1$. Since $F_{m,t} \in A_{p-1} \cdot S(V^*)$ and $A_{p-1} \subseteq S(V^*)^{G,+} \cdot S(V^*)$ from the previous two lemmas, it follows that $F_{m,t}$ is contained in $S(V^*)^{G,+}_{\leqslant p-1} \cdot S(V^*)$. Notice that

$$F_{m,t} = \operatorname{Tr}(h) + \sum_{S \subsetneq \{1,2,\ldots,p-1\}} (-1)^{|S|} X_{S'} \operatorname{Tr}(t X_S).$$

For a proper subset S of $\{1, 2, \ldots, p-1\}$, the degree of tX_S is strictly smaller than the degree of h. Therefore $\operatorname{Tr}(h)$ is contained in the ideal in $S(V^*)$ generated by $S(V^*)^{G,+}_{\leqslant p-1}$ and transfers of strictly smaller degree. Thus the conclusion follows by induction on the degree of h. □

Proposition 5. *Let V be an indecomposable G-module. Then*

$$S(V^*)^{G,+} \cdot S(V^*) = S(V^*)^{G,+}_{\leqslant p} \cdot S(V^*).$$

Proof. Let z denote a G-module generator for V^*. Consider the invariant polynomial $N(z) = \prod_{l \in \boldsymbol{F}_p} \sigma^l(z)$. It is proven in [5, 2.9] that

$$S(V^*) = B \oplus N(z) \cdot S(V^*)$$

as G-modules, where B is the set of polynomials in $S(V^*)$ whose degree is strictly less than p as a polynomial in z. Moreover by Lemma 2.10 from the same source, B_i, the set of polynomials of degree i in B including 0, is a free G-module for $i \geqslant p$. It follows that an invariant polynomial f of degree greater than p can be written as $f = \operatorname{Tr}(h) + N(z) \cdot g$, where $g \in S(V^*)^G$ and $h \in S(V^*)$. Therefore the result follows from Theorem 4 since the degree of $N(z)$ is p. □

Acknowledgments

The author thanks the anonymous referee for valuable comments that improved the exposition. Thanks are also due to Jim Shank for reading an earlier draft of the paper and suggesting some improvements and a correction.

References

[1] H. Derksen, G. Kemper, Computational Invariant Theory, Encyclopaedia Math. Sci., vol. 130, Springer-Verlag, 2002.
[2] P. Fleischmann, The Noether bound in invariant theory of finite groups, Adv. Math. 152 (2000) (2002) 23–32.
[3] 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.
[4] J. Fogarty, On Noether's bound for polynomial invariants of a finite group, Electron. Res. Announc. Amer. Math. Soc. 7 (2001) 5–7.
[5] I. Hughes, G. Kemper, Symmetric power of modular representations, Hilbert series and degree bounds, Comm. Algebra 28 (2000) 2059–2089.
[6] M.D. Neusel, Degree bounds—An invitation to postmodern invariant theory, Topology Appl. 154 (4) (2007) 792–814.
[7] M.D. Neusel, L. Smith, Invariant Theory of Finite Groups, Math. Surveys Monogr., vol. 94, Amer. Math. Soc., 2002.
[8] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, Math. Ann. 77 (1916) 28–35.
[9] D. Richman, Invariants of finite groups over fields of characteristic p, Adv. Math. 124 (1996) 25–48.
[10] M. Sezer, R.J. Shank, On the coinvariants of modular representations of cyclic groups of prime order, J. Pure Appl. Algebra 205 (1) (2006) 210–225.
[11] D.L. Wehlau, The Noether number in invariant theory, C. R. Math. Acad. Sci. Soc. R. Can. 28 (2) (2006) 39–62.