Math. Nachr. **285**, No. 16, 1974 – 1980 (2012) / **DOI** 10.1002/mana.201100316

Gröbner bases for the Hilbert ideal and coinvariants of the dihedral group D_{2p}

Martin Kohls[*1] and **Müfit Sezer**[**2]

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

Received 27 November 2011, revised 30 January 2012, accepted 2 April 2012
Published online 30 May 2012

Key words Dihedral groups, coinvariants, Hilbert ideal, universal Gröbner bases
MSC (2010) 13A50

We consider a finite dimensional representation of the dihedral group D_{2p} over a field of characteristic two where p is an odd integer and study the corresponding Hilbert ideal I_H. We show that I_H has a universal Gröbner basis consisting of invariants and monomials only. We provide sharp bounds for the degree of an element in this basis and in a minimal generating set for I_H. We also compute the top degree of coinvariants when p is prime.

© 2012 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

1 Introduction

Let V be a finite dimensional representation of a finite group G over a field F. There is an induced action of G on the symmetric algebra $F[V]$ of V^* that is given by $g(f) = f \circ g^{-1}$ for $g \in G$ and $f \in F[V]$. Let $F[V]^G$ denote the ring of invariant polynomials in $F[V]$. One of the main goals in invariant theory is to determine $F[V]^G$ by computing the generators and relations. A closely related object is the Hilbert ideal, denoted I_H, which is the ideal in $F[V]$ generated by invariants of positive degree. The Hilbert ideal often plays an important role in invariant theory as it is possible to extract information from it about the invariant ring. There is also substantial evidence that the Hilbert ideal is better behaved than the full invariant ring in terms of constructive complexity. The invariant ring is in general not generated by invariants of degree at most the group order when the characteristic of F divides the group order (this is known as the modular case) but it has been conjectured [2, Conjecture 3.8.6 (b)] that the Hilbert ideal always is. Apart from the non-modular case this conjecture is known to be true if V is a trivial source module [3] or if $G = \boldsymbol{Z}_p$ and V is an indecomposable module [10]. Furthermore, Gröbner bases for I_H have been determined for some classes of groups. The reduced Gröbner bases corresponding to several representations of $\boldsymbol{Z}_p$ have been computed in a study of the module structure of the coinvariant ring $F[V]_G$ which is defined to be $F[V]/I_H$, see [11]. The reduced Gröbner bases for the natural action of the symmetric and the alternating group can be found in [1] and [14], respectively. These bases have applications in coding theory, see [7].

In this paper we consider a representation of the dihedral group D_{2p} over a field of characteristic two where p is an odd integer. Invariants of D_{2p} in characteristic zero have been studied by Schmid [9] where she shows beyond other things that $\boldsymbol{C}[V]^{D_{2p}}$ is generated by invariants of degree at most $p+1$. More recently, bounds for the degrees of elements in both generating and separating sets over an algebraically closed field of characteristic two have been computed, see [6]. We continue further in this direction and show that the Hilbert ideal I_H is generated by invariants up to degree p and not less. We also construct a universal Gröbner basis for I_H, i.e., a set $\mathcal{G}$ which forms a Gröbner basis of I_H for any monomial order. Somewhat unexpectedly, the only polynomials that are not invariant in this set are monomials. Moreover, the maximal degree of a polynomial in this basis is $p+1$. This is

* Corresponding author: e-mail: kohls@ma.tum.de, Phone: +49 89 289 17451, Fax: +49 89 289 17457
** e-mail: sezer@fen.bilkent.edu.tr, Phone: +90 312 290 1085, Fax: +90 312 266 45 79

WILEY ONLINE LIBRARY
© 2012 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

also atypical for Gröbner basis calculations because passing from a generating set to a Gröbner basis increases the degrees rapidly in general. Then we turn our attention to the coinvariants. Of particular interest are the top degree and the dimension of $F[V]_G$, because a vector space basis for $F[V]_G$ yields a basis for the invariants that can be obtained by averaging over the group and these invariants may be crucial in efficient generation of the whole invariant ring, see for example [4]. Perhaps among the most celebrated results on coinvariants is one due to Steinberg [13] which says that the group order $|G|$ is a lower bound for the dimension of $F[V]_G$ as a vector space, which is sharp if and only if the invariant ring $F[V]^G$ is polynomial, see also [12]. Using the Gröbner basis for I_H we compute the top degree of the coinvariants of D_{2p} when p is prime. It turns out that for faithful representations, the top degree equals the upper bound for the maximum degree of a polynomial in a minimal generating set that was given in [6]. Also we present upper bounds for the top degree and the dimension of coinvariants of arbitrary finite groups, which might be part of the folklore, but do not seem to have appeared explicitly yet.

2 The Hilbert ideal

We start by fixing our notation. Let $p \geq 3$ be an odd integer and let G denote the dihedral group of order $2p$, generated by an element σ of order 2 and an element ρ of order p. We also let F denote a field of characteristic two which contains a primitive pth root of unity. Let r and s be non-negative integers. We assume that G acts on the polynomial ring

$$F[V] = F[x_1, \ldots, x_r, y_1, \ldots, y_r, z_1, \ldots, z_s, w_1, \ldots, w_s]$$

as follows: The element σ permutes x_i and y_i for $i = 1, \ldots, r$ and z_i and w_i for $i = 1, \ldots, s$ respectively. Furthermore, ρ acts trivially on z_i and w_i for $i = 1, \ldots, s$, while $\rho(x_i) = \lambda_i x_i$ and $\rho(y_i) = \lambda_i^{-1} y_i$ for λ_i a non trivial p-th root of unity for $i = 1, \ldots, r$. Up to choice of a basis, this is the form of an arbitrary reduced G-action, see [6]. We will write u to denote any of the variables of $F[V]$, and then v for $\sigma(u)$. Let further M denote the set of monomials of $F[V]$. For $m \in M^\rho$, we write $o(m)$ for the orbit sum of m, i.e., $o(m) = m$ if $m \in M^G$ and $o(m) = m + \sigma(m)$ if $m \in M^\rho \setminus M^G$. Recall that $F[V]^G$ is generated by orbit sums of ρ-invariant monomials, see [6, Lemma 2].

Lemma 2.1

(a) *Every monomial m can be written as a product $m_1 \cdots m_k \cdot m'$ of ρ-invariant monomials $m_1, \ldots, m_k$ and a monomial m' such that the degrees of all these monomials are at most p. Moreover, if $m \in M^\rho$, then we may take $m' = 1$.*

(b) *The ideals*

$$\begin{aligned} I &= \langle \{um \mid m \in M^\rho \text{ and } u \text{ a variable dividing } m\}\rangle \\ \text{and } \ I' &= \langle \{um \mid m \in M^\rho \text{ of degree at most } p \text{ and } u \text{ a variable dividing } m\}\rangle \end{aligned}$$

of $F[V]$ are equal.

Proof. (a) Let $a_1, \ldots, a_p$ be a sequence of p non-zero elements in $\boldsymbol{Z}/p\boldsymbol{Z}$. For $1 \leq k \leq p$, consider the partial sums $S_k := a_1 + \cdots + a_k$. If $S_i = S_j$ for some $1 \leq i < j \leq p$, then $a_{i+1} + \cdots + a_j = 0$. On the other hand, if all S_k are different, then $S_i = 0$ for some $1 \leq i \leq p$. This shows that the sequence $a_1, \ldots, a_p$ has a non-empty subsequence whose sum is zero. Equivalently, every monomial of degree p has a nontrivial divisor that is in M^ρ. Now let m be a monomial of degree at least $p+1$. We just saw that m has a nontrivial subfactor of degree at most p that is ρ-invariant. Removing this factor from m and repeating this process, one ends up with a remainder of degree at most p. Moreover, if $m \in M^\rho$, this remainder is also in M^ρ.

(b) We have to show $I \subseteq I'$, so take $um \in I$ with u a variable dividing m, where m is a ρ-invariant monomial of degree at least $p+1$. By the first part of the lemma we can write $m = m_1 \cdots m_k$, where each m_i is a ρ-invariant monomial of degree at most p for $1 \leq i \leq k$. We may assume u divides m_1. Then $um_1 \in I'$ and so $um \in I'$ as desired. □

Note that a result of Fleischmann [3, Theorem 4.1] implies that the Hilbert ideal is generated by invariants up to degree $2p$. In the following proposition, among other things, we sharpen this bound to p. We mention that part (c) is not used later and just stated for its own interest.

© 2012 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

Proposition 2.2

(a) *The Hilbert ideal I_H is generated by invariants of positive degree at most p.*

(b) *If $m \in M^\rho$ and $u|m$, then $um \in I_H$.*

(c) *If $m \in M^\rho$ and u_1 and u_2 are variables such that $u_1^2|m$ and ρ acts on u_1 and u_2 by multiplication with the same root of unity, then $mu_2 \in I_H$.*

Proof. (a) Let I denote the ideal of $F[V]$ generated by invariants of positive degree at most p. We have to show that the Hilbert ideal, which is generated by orbit sums of ρ-invariant monomials of positive degree, equals I. For the sake of a proof by contradiction, take a ρ-invariant monomial m of minimal degree d such that $o(m)$ is not in I. First assume $m \in M^G$, and take a variable u appearing in m. Then also $v = \sigma(u)$ appears in m, so $uv|m$, and as uv is an invariant of degree 2, this shows that $m \in I$. Secondly, assume $m \in M^\rho \setminus M^G$. Since $d > p$, by Lemma 2.1(a) we have a factorization $m = m_1 m_2$ of m into two ρ-invariant monomials m_1, m_2 of degree strictly smaller than d. We consider

$$o(m) = m_1 m_2 + \sigma(m_1 m_2) = m_1(m_2 + \sigma(m_2)) + \sigma(m_2)(m_1 + \sigma(m_1)),$$

where $m_i + \sigma(m_i)$ for $i = 1, 2$ respectively are either zero or orbit sums of ρ-invariant monomials of degree strictly smaller than d, hence they are in I by induction.

(b) Write $m = um'$, where m' is a monomial. Then $um = u^2 m' = u(m + \sigma(m)) + uv\sigma(m')$ is in I_H, because $(m + \sigma(m))$ and uv are.

(c) Write $m = u_1^2 m'$, where m' is a monomial. Then

$$u_2 m = u_2 u_1^2 m' = u_1(u_2 u_1 m' + \sigma(u_2 u_1 m')) + u_1(\sigma(u_2 u_1 m'))$$

is in I_H: The first summand is a multiple of the orbit sum of the ρ-invariant monomial $u_2 u_1 m'$, and the second one is a multiple of the invariant $u_1 v_1$. □

We recall the following notation: For a given monomial order $<$ on M and a polynomial f we write $\mathrm{LM}(f)$ for the leading monomial of f. Also, for a subset $\mathcal{G} \subseteq F[V]$ and $f \in F[V]$ we write $f \to_\mathcal{G} 0$ if there exist elements $a_1, \dots, a_n \in F[V]$ and $g_1, \dots, g_n \in \mathcal{G}$ such that $f = a_1 g_1 + \dots + a_n g_n$ and $\mathrm{LM}(f) \geq \mathrm{LM}(a_i g_i)$ for $i = 1, \dots, n$. In this case we say f reduces to zero modulo $\mathcal{G}$. Notice that $f \to_\mathcal{G} 0$ implies $af \to_\mathcal{G} 0$ for any $a \in F[V]$.

Lemma 2.3 *Let $f, g \in F[V]$ with $\mathrm{LM}(f) > \mathrm{LM}(g)$. Then $f \to_\mathcal{G} 0$ and $g \to_\mathcal{G} 0$ for a set $\mathcal{G} \subseteq F[V]$ imply $(f + g) \to_\mathcal{G} 0$.*

Proof. We have $f = \sum a_i g_i$ and $g = \sum b_i g_i$ for some $a_i, b_i \in F[V]$ and $g_i \in \mathcal{G}$ with $\mathrm{LM}(a_i g_i) \leq \mathrm{LM}(f)$ and $\mathrm{LM}(b_i g_i) \leq \mathrm{LM}(g) < \mathrm{LM}(f)$. Then $(f+g) = \sum (a_i + b_i) g_i$ gives $(f+g) \to_\mathcal{G} 0$ because $\mathrm{LM}((a_i + b_i) g_i) \leq \max\{\mathrm{LM}(a_i g_i), \mathrm{LM}(b_i g_i)\} \leq \mathrm{LM}(f) = \mathrm{LM}(f + g)$. □

Let $\mathcal{G}$ denote the following set of polynomials:

$$\begin{array}{rll} m + \sigma(m) & \text{for} & m \in M^\rho \setminus M^G \text{ of degree at most } p, \\ um & \text{for} & m \in M^\rho \text{ of degree at most } p \text{ and } u \text{ a variable dividing } m, \\ x_i y_i,\ z_j w_j & \text{for} & i = 1, \dots, r \text{ and } j = 1, \dots, s. \end{array}$$

We show that $\mathcal{G}$ is a universal Gröbner basis of I_H. We need the following lemma.

Lemma 2.4 *Let $m \in M^\rho$. Then $(m + \sigma(m)) \to_\mathcal{G} 0$.*

Proof. We assume $m \in M^\rho \setminus M^G$ since $m + \sigma(m) = 0$ if $m \in M^G$. We also take $\deg(m) > p$ because otherwise $m + \sigma(m) \in \mathcal{G}$. Then by Lemma 2.1(a) there exist ρ-invariant monomials m_1, m_2 of degree strictly smaller than the degree of m such that $m = m_1 m_2$. Without loss of generality, we assume $m > \sigma(m)$. So we have either $m_1 > \sigma(m_1)$ or $m_2 > \sigma(m_2)$. We harmlessly assume $m_1 > \sigma(m_1)$. Consider the equation

$$m + \sigma(m) = m_1 m_2 + \sigma(m_1 m_2) = m_2(m_1 + \sigma(m_1)) + \sigma(m_1)(m_2 + \sigma(m_2)).$$

© 2012 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

By induction on the degree both $m_1 + \sigma(m_1)$ and $m_2 + \sigma(m_2)$ reduce to zero modulo $\mathcal{G}$ and hence, so do their respective monomial multiples $m_2(m_1 + \sigma(m_1))$ and $\sigma(m_1)(m_2 + \sigma(m_2))$. Hence the result follows from the previous lemma because we have $\mathrm{LM}(m_2(m_1 + \sigma(m_1))) = m_1 m_2$ and $m_1 m_2 > \sigma(m_1) m_2$ and $m_1 m_2 > \sigma(m_1)\sigma(m_2)$. $\square$

Theorem 2.5 *$\mathcal{G}$ forms a universal Gröbner basis of I_H.*

Proof. First note that by Proposition 2.2(b) all elements of $\mathcal{G}$ lie in I_H. Conversely, by Proposition 2.2(a), I_H is generated by orbit sums $o(m)$ of monomials $m \in M^\rho$ of degree at most p. If $m \notin M^G$, then $o(m) = m + \sigma(m) \in \mathcal{G}$, by construction. Otherwise, if $u|m$, we have $uv|m$, so again $o(m) = m \in \langle \mathcal{G} \rangle$. This establishes that the ideal generated by $\mathcal{G}$ is exactly I_H.

Next we show that the polynomials in $\mathcal{G}$ satisfy Buchberger's criterion. Recall that for $f_1, f_2 \in F[V]$, the s-polynomial $s(f_1, f_2)$ is defined to be $\frac{T}{\mathrm{LT}(f_1)} f_1 - \frac{T}{\mathrm{LT}(f_2)} f_2$, where T is the least common multiple of the leading monomials of f_1 and f_2 and $\mathrm{LT}(f)$ denotes the lead term of the polynomial f. Buchberger's criterion says that $\mathcal{G}$ is a Gröbner Basis of I_H if and only if $s(f_1, f_2) \rightarrow_{\mathcal{G}} 0$ for all $f_1, f_2 \in \mathcal{G}$. Since the s-polynomial of two monomials is zero, we just check the s-polynomials of $m + \sigma(m)$ for $m \in M^\rho \setminus M^G$ with each of the four families of polynomials in $\mathcal{G}$. We will also use the well-known fact that $s(f_1, f_2)$ reduces to zero modulo $\{f_1, f_2\}$ if the leading monomials of f_1 and f_2 are relatively prime, see [5, Exercise 9.3].

(1) Let $m = u_1^{a_1} \cdots u_k^{a_k} m'$ and $n = u_1^{b_1} \cdots u_k^{b_k} n'$ be monomials in $M^\rho \setminus M^G$ of degree at most p with $a_j, b_j > 0$ for $1 \leq j \leq k$ and m' and n' are relatively prime monomials. We further assume that neither m' nor n' is divisible by any of u_j for $1 \leq j \leq k$ and $m > \sigma(m)$ and $n > \sigma(n)$. Let f_1, f_2 denote $m + \sigma(m)$ and $n + \sigma(n)$, respectively. Notice that $s(f_1, f_2) = \frac{T}{\mathrm{LT}(f_1)}(\sigma(m)) - \frac{T}{\mathrm{LT}(f_2)}(\sigma(n))$. If $a_j > b_j$ for some $1 \leq j \leq k$, then $\frac{T}{\mathrm{LT}(f_2)}$ is divisible by u_j and so $\frac{T}{\mathrm{LT}(f_2)}(\sigma(n))$ is divisible by $u_j v_j$ because $\sigma(n)$ is divisible by v_j. Similarly, if $b_{j'} > a_{j'}$ for some $1 \leq j' \leq k$, then $\frac{T}{\mathrm{LT}(f_1)}(\sigma(m))$ is divisible by $u_{j'} v_{j'}$. It follows that if there are indices $1 \leq j, j' \leq k$ such that $a_j > b_j$ and $b_{j'} > a_{j'}$, then $s(f_1, f_2) \rightarrow_{\mathcal{G}} 0$. So we may assume $a_j \geq b_j$ for $1 \leq j \leq k$. Therefore we are reduced to two cases.

First assume that $a_j \geq b_j$ for $1 \leq j \leq k$ and for one of the indices the inequality is strict, say $a_1 > b_1$. As in the previous paragraph $\frac{T}{\mathrm{LT}(f_2)}(\sigma(n))$ is divisible by $u_1 v_1$. Meanwhile, we have $\frac{T}{\mathrm{LT}(f_1)}(\sigma(m)) = n' v_1^{a_1} \cdots v_k^{a_k} \sigma(m')$. But since n is in M^ρ, ρ acts on n' and on $v_1^{b_1} \cdots v_k^{b_k}$ by multiplication with the same root of unity. So $n' v_1^{a_1 - b_1} \cdots v_k^{a_k - b_k} \sigma(m')$ is in M^ρ as well because it is obtained by multiplying the ρ-invariant monomial $v_1^{a_1} \cdots v_k^{a_k} \sigma(m')$ with $\frac{n'}{v_1^{b_1} \cdots v_k^{b_k}}$. Since $a_1 > b_1 > 0$, this shows that $\frac{T}{\mathrm{LT}(f_1)}(\sigma(m))$ is divisible by the product of the ρ-invariant monomial $n' v_1^{a_1 - b_1} \cdots v_k^{a_k - b_k} \sigma(m')$ and the variable v_1 that divides this monomial. By Lemma 2.1(b), $\frac{T}{\mathrm{LT}(f_1)}(\sigma(m))$ is also divisible by a monomial in $\mathcal{G}$.

Secondly, assume that $a_j = b_j$ for $1 \leq j \leq k$. Then we get $s(f_1, f_2) = v_1^{a_1} \cdots v_k^{a_k} (n'\sigma(m') + m'\sigma(n'))$. But ρ multiplies m' and n' with the same root of unity and hence it multiplies n' and $\sigma(m')$ with reciprocal roots of unity. This puts $n'\sigma(m')$ (and $m'\sigma(n')$) in M^ρ. Hence $s(f_1, f_2) \rightarrow_{\mathcal{G}} 0$, by the previous lemma.

(2) We compute the s-polynomial $s(f_1, f_2)$, where $f_1 = m + \sigma(m)$ for a monomial m in M^ρ of degree at most p and f_2 is the product of a ρ-invariant monomial of degree at most p with a variable that divides this monomial. As before, we assume $m > \sigma(m)$. Write $m = u_1^{a_1} \cdots u_k^{a_k} m'$ and $f_2 = u_1^{b_1} \cdots u_k^{b_k} n'$ where $a_j, b_j > 0$ with relatively prime monomials m' and n'. We further assume m' and n' are not divisible by any of u_j. We have $s(f_1, f_2) = \frac{T}{\mathrm{LT}(f_1)}(\sigma(m))$. Notice that if $b_j > a_j$ for some $1 \leq j \leq k$, then $\frac{T}{\mathrm{LT}(f_1)}$ is divisible by u_j and so $\frac{T}{\mathrm{LT}(f_1)}(\sigma(m))$ is divisible by $u_j v_j$. Hence $s(f_1, f_2)$ reduces to zero modulo $\mathcal{G}$. Therefore we assume $a_j \geq b_j$ for $1 \leq j \leq k$. So, $s(f_1, f_2) = n' v_1^{a_1} \cdots v_k^{a_k} \sigma(m')$. By construction there is a variable w such that w^2 divides f_2 and f_2/w is in M^ρ. We consider two cases.

First assume that w^2 divides n'. We have

$$s(f_1, f_2) = n' v_1^{a_1} \cdots v_k^{a_k} \sigma(m') = \left(\frac{n'\sigma(m') v_1^{a_1 - b_1} \cdots v_k^{a_k - b_k}}{w} \right) (w v_1^{b_1} \cdots v_k^{b_k}).$$

Since f_2/w is in M^ρ, ρ multiplies n'/w and $v_1^{b_1} \cdots v_k^{b_k}$ with the same (non-zero) scalar. Therefore, since $\sigma(m') v_1^{a_1} \cdots v_k^{a_k} \in M^\rho$, we get $\frac{n'\sigma(m') v_1^{a_1 - b_1} \cdots v_k^{a_k - b_k}}{w} \in M^\rho$ as well. Hence $s(f_1, f_2)$ is divisible by the product

© 2012 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

of w with a ρ-invariant monomial that is divisible by w. By Lemma 2.1(b), $s(f_1, f_2)$ is divisible by a monomial in $\mathcal{G}$.

Since n' and $u_1^{b_1} \cdots u_k^{b_k}$ are relatively prime, we can assume as the remaining case that w does not divide n'. Then $w = u_j$ for some $1 \le j \le k$. Say, $w = u_1$. We also have $a_1 \ge b_1 \ge 2$. Similar to the first case we have

$$s(f_1, f_2) = n' v_1^{a_1} \cdots v_k^{a_k} \sigma(m') = \big(n'\sigma(m') v_1^{a_1 - b_1 + 1} v_2^{a_2 - b_2} \cdots v_k^{a_k - b_k}\big)\big(v_1^{b_1 - 1} v_2^{b_2} \cdots v_k^{b_k}\big).$$

Notice that since $f_2/u_1 \in M^\rho$, ρ acts on n' and $v_1^{b_1-1} v_2^{b_2} \cdots v_k^{b_k}$ by multiplication with the same scalar. Hence $\big(n'\sigma(m') v_1^{a_1-b_1+1} v_2^{a_2-b_2} \cdots v_k^{a_k-b_k}\big)$ lies in M^ρ because $\sigma(m') v_1^{a_1} \cdots v_k^{a_k}$ is already ρ-invariant. It follows that, since $a_1 - b_1 + 1 \ge 1$ and $b_1 - 1 \ge 1$, $s(f_1, f_2)$ is divisible by the product of v_1 with a ρ-invariant monomial that is divisible by v_1. So we get that $s(f_1, f_2)$ is divisible by a monomial in $\mathcal{G}$ by Lemma 2.1(b).

(3) We compute the s-polynomial $s(f_1, f_2)$ where $f_1 = m + \sigma(m)$ ($m > \sigma(m)$) for a monomial m in M^ρ of degree at most p and f_2 is a product uv for some variable u. Since we assume m and uv are not relatively prime we take $m = u^a m'$ where u does not divide m'. If v divides m' then both m and $\sigma(m)$ are divisible by uv and so $s(f_1, f_2)$ equals $\sigma(m)$. Hence it is divisible by uv and we are done. Therefore we assume v does not divide m so we have $s(f_1, f_2) = v\sigma(m)$. But v divides $\sigma(m)$, and the latter is in M^ρ and is of degree at most p. Hence $v\sigma(m)$ is an element of $\mathcal{G}$. □

3 Bounds for coinvariants

Before we specialize to the dihedral group, we start this section with a general result that is probably part of the folklore, but it seems it has not been written down explicitly yet. In the following theorem, G is an arbitrary finite group and F an arbitrary field. If the field is large enough, Dades' algorithm [2, Proposition 3.3.2] provides a homogeneous system of parameters with each element of degree $|G|$. Note that field extensions do not affect the degree structure of coinvariants, so in particular we can assume $d_i = |G|$ for all i in the following theorem.

Theorem 3.1 *Assume $d_1, \ldots, d_n$ are the degrees of a homogeneous system of parameters of $F[V]^G$, where $n = \dim V$. Then we have*

$$\text{(a)} \quad \operatorname{topdeg}(F[V]_G) \le \sum_{i=1}^n (d_i - 1),$$

$$\text{(b)} \quad \dim(F[V]_G) \le \prod_{i=1}^n d_i.$$

In particular, we have $\operatorname{topdeg}(F[V]_G) \le \dim(V)(|G|-1)$ *and* $\dim(F[V]_G) \le |G|^n$. *If the system of parameters generates $F[V]^G$, we have equalities in* (a) *and* (b).

P r o o f. Let A be the subalgebra of $F[V]^G$ generated by a homogeneous system of parameters with the given degrees. As the group G is finite and $F[V]$ is Cohen-Macaulay, we have that $F[V]$ is a free A-module, say $F[V] = \bigoplus_{i=1}^r A g_i$ with $g_1, \ldots, g_r$ homogeneous elements of degrees $m_1 \le \cdots \le m_r$. Then r equals the dimension and m_r equals the top degree of $F[V]/(A_+ \cdot F[V])$, respectively. As $A_+ \subseteq F[V]_+^G$, the numbers r and m_r are bigger than or equal to the dimension and top degree of $F[V]/I_H$ respectively. As the Hilbert series of $F[V]/(A_+ \cdot F[V])$ is given by

$$H(t) = \frac{\prod_{i=1}^n \big(1 - t^{d_i}\big)}{(1-t)^n} = \prod_{i=1}^n \big(1 + t + t^2 + \cdots + t^{d_i - 1}\big),$$

we get $m_r = \deg H(t) = \sum_{i=1}^n (d_i - 1)$ and $r = H(1) = \prod_{i=1}^n d_i$, which proves (a) and (b). □

Now we restrict ourselves to the coinvariants of the dihedral groups. We need the following for our main result.

Proposition 3.2 (Schmid [9, proof of Proposition 7.7]) *Let $x_1, \ldots, x_t \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\}$ ($p \ge 2$ a natural number) be a sequence of $t \ge p+1$ nonzero elements. Then there exists a pair of indices $k_1, k_2 \in \{1, \ldots, t\}$, $k_1 \ne k_2$ such that $x_{k_1} = x_{k_2}$ with the additional property that there exists a subset of indices $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, t\} \setminus \{k_1, k_2\}$ such that*

$$x_{k_1} + x_{i_1} + \cdots + x_{i_r} = \overline{0}.$$

© 2012 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

If p is prime, any pair of indices $k_1, k_2 \in \{1, \dots, t\}$, $k_1 \neq k_2$ such that $x_{k_1} = x_{k_2}$ has this additional property.

Note that when p is not a prime, this additional property is not guaranteed for an arbitrary choice of indices k_1, k_2 with $x_{k_1} = x_{k_2}$. For example when $p = sl$ with $s, l > 1$, consider $x_1 = x_2 = \bar{1}$ and $x_i = \bar{s}$ for $i = 3, \dots, p+1$ and take $k_1 = 1$, $k_2 = 2$.

Theorem 3.3 *Assume the notation of Section 2. For p an odd prime, the top degree of the coinvariants of the dihedral group D_{2p} in characteristic two equals $s + \max(r, p)$ if $r \geq 1$, and equals s if $r = 0$.*

P r o o f. We write d for the top degree of $F[V]_G$. For a polynomial $f \in F[V]$, let $\deg_{xy} f$ denote the degree of f in the variables $x_1, \dots, x_r, y_1, \dots, y_r$, and define $\deg_{zw} f$ similarly. Let m be a monomial. The proof consists of four observations.

(i) If $\deg_{zw} m > s$, then m is divisible either by $z_i w_i$ or one of z_i^2 or w_i^2 for some $i = 1, \dots, s$, in particular $m \in I_H$. This implies $d \leq s$ in case $r = 0$.

(ii) If $\deg_{xy} m > \max(r, p)$ then $\deg_{xy} m > r$ implies that m is divisible by $x_i y_i$ or x_i^2 or y_i^2 for some $i = 1, \dots, r$. In the first case $m \in I_H$, so without loss of generality we can assume $x_i^2 | m$ for some i. By Proposition 3.2, $\deg_{xy} m > p$ implies that there exists a factorization $m = (x_i n) x_i n'$ such that $x_i n$ is a ρ-invariant monomial of degree at most p. As $x_i^2 n$ is an element of $\mathcal{G}$, we have $m \in I_H$. Now (i) and (ii) imply that if $\deg(m) > s + \max(r, p)$, then $m \in I_H$, hence $d \leq s + \max(r, p)$.

(iii) We claim that $n := y_1 \cdots y_r w_1 \cdots w_s$ is not in I_H, hence $d \geq r + s$. Otherwise, n would be divisible by the leading monomial of an element of $\mathcal{G}$. Since no variable in n has multiplicity bigger than one, n is in fact divisible by $\mathrm{LM}(m + \sigma(m))$ for some monomial $m \in M^\rho \setminus M^G$ of degree at most p. As $\mathcal{G}$ is a universal Gröbner basis, we can choose a lexicographic order $>$ with $x_i > y_j$ and $z_i > w_j$ for all i, j and assume $m > \sigma(m)$. We fix this order until the end of the proof. Then $m | n$ implies that $m = y_{i_1} \cdots y_{i_k} w_{j_1} \cdots w_{j_l}$, but then $\sigma(m) = x_{i_1} \cdots x_{i_k} z_{j_1} \cdots z_{j_l} > m$ by the choice of our order, a contradiction.

(iv) Finally if $r \geq 1$, we claim that $n := y_1^p w_1 \cdots w_s$ is not in I_H, hence $d \geq p + s$. As before, $n \in I_H$ would imply that n is divisible by the leading monomial of an element of $\mathcal{G}$. Notice that a ρ-invariant monomial divisor of n either is divisible by y_1^p or is not divisible by y_1 at all. It follows that the only leading monomial of a member of $\mathcal{G}$ that divides n is of the form $\mathrm{LM}(m + \sigma(m))$ for some monomial $m \in M^\rho \setminus M^G$ of degree at most p. Assuming $m > \sigma(m)$, we see that m would be of the form $w_{i_1} \cdots w_{i_k}$ or $y_1^p w_{i_1} \cdots w_{i_k}$, so $\sigma(m)$ would be of the form $z_{i_1} \cdots z_{i_k}$ or $x_1^p z_{i_1} \cdots z_{i_k}$ respectively. In each case, we have the contradiction $\sigma(m) > m$ by choice of our monomial order. □

The following (counter-)example shows that the condition of p being a prime in Theorem 3.3 cannot be dropped.

Example 3.4 Let $r = p = 9$ and $s = 0$. Fix a primitive 9-th root of unity λ. We assume that $\rho(x_1) = \lambda x_1$ and $\rho(x_i) = \lambda^3 x_i$ for $2 \leq i \leq 9$. Consider the monomial $m = x_1^2 y_2 \cdots y_9$. We verify that $m \notin I_H$ as follows. Choose a lexicographic order such that $x_i > y_j$ for $1 \leq i, j \leq 9$. If $m \in I_H$, then it is divisible by the leading monomial m' of an element of $\mathcal{G}$, because $\mathcal{G}$ is a a universal Gröbner basis of I_H. We show that this is not possible by considering each family of leading monomials in $\mathcal{G}$. Clearly, m' cannot be $x_i y_i$ for some $1 \leq i \leq 9$. Also, m has no nontrivial ρ-invariant subfactor that is divisible by x_1. Therefore m' is not equal to a product of a variable with a ρ-invariant monomial that is divisible by this variable. Finally assume that m' is the leading monomial of $m' + \sigma(m')$ and $m' \in M^\rho$. Since $m' \in M^\rho$, m' is a factor of $y_2 \cdots y_9$. But then, we get a contradiction because $\sigma(m') > m'$ by our choice of order. Hence the top degree of coinvariants is at least 10, which is bigger than $s + \max(r, p) = 9$. Therefore, we cannot remove the restriction on p being a prime in Theorem 3.3.

Example 3.5 We take $r = 1$, $s = 0$ and write x and y for x_1 and y_1. Then $F[V]^G = F[xy, x^p + y^p]$, see e.g., [6, Remark 5]. In particular, all elements in the Hilbert ideal of degree less than p are divisible by xy, so the bound in Proposition 2.2 (a) is sharp. A universal Gröbner Basis of I_H is given by $\mathcal{G} = \{xy, x^p + y^p, x^{p+1}, y^{p+1}\}$. If we choose lexicographic order with $x > y$, we see that the lead term ideal of I_H is minimally spanned by $\{xy, x^p, y^{p+1}\}$. In particular, any Gröbner Basis must contain an element of degree $p + 1$. The generators of $F[V]^G$ form a homogeneous system of parameters in degrees $d_1 = 2$ and $d_2 = p$. Thus, Theorem 3.1 yields the sharp bounds $\mathrm{topdeg}(F[V]_G) \leq (d_1 - 1) + (d_2 - 1) = p = s + \max(r, p)$ and $\dim(F[V]_G) \leq d_1 d_2 = 2p$.

Note that in case $r \geq 1$, the top degree of the coinvariants is the same as the upper bound for the degrees of elements in a minimal generating set for the invariant ring that is given in [6, Theorem 4]. If $r = 0$, what we really

© 2012 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

consider are the vector invariants of the permutation action of $\boldsymbol{Z}_2$. In this case, the fact that the top degree of the coinvariants is s also follows from [11, Theorem 2.1]. The maximal degree of elements in a minimal generating set in this case is also given by s if $s \geq 2$, see [8]. It would hence be tempting to conjecture that the invariant ring is always generated by invariants of degree at most the top degree of the coinvariants. However, in case $r = 0$ and $s = 1$, we have $F[z, w]^G = F[zw, z + w]$, but the top degree of the coinvariants is one.

Acknowledgements We thank the referee for carefully reading the manuscript and many useful remarks. In particular, the referee pointed out to us that we could drop the condition on p being a prime in Theorem 2.5 in the preprint version of this paper, by illustrating some refinements of the preliminary lemmas, which greatly improved our paper. We also thank Tübitak for funding a visit of the first author to Bilkent University, and Gregor Kemper for funding a visit of the second author to TU München. The second author is also partially supported by Tübitak-Tbag/109T384 and Tüba-Gebip/2010.

References

[1] J.-M. Arnaudiès and A. Valibouze, Lagrange resolvents, J. Pure Appl. Algebra **117/118**, 23–40 (1997), Algorithms for algebra (Eindhoven, 1996).
[2] H. Derksen and G. Kemper, Computational invariant theory, Invariant Theory and Algebraic Transformation Groups, I, Encyclopaedia of Mathematical Sciences Vol. 130 (Springer-Verlag, Berlin, 2002).
[3] P. Fleischmann, The Noether bound in invariant theory of finite groups, Adv. Math. **156**(1), 23–32 (2000).
[4] P. Fleischmann, M. Sezer, R. J. Shank, and C. F. Woodcock, The Noether numbers for cyclic groups of prime order, Adv. Math. **207**(1), 149–155 (2006).
[5] G. Kemper, A Course in Commutative Algebra, Graduate Texts in Mathematics Vol. 256 (Springer, Heidelberg, 2011).
[6] M. Kohls and M. Sezer, Invariants of the dihedral group D_{2p} in characteristic two, Math. Proc. Camb. Philos. Soc. **152**(1), 1–7 (2012).
[7] T. Mora and M. Sala, On the Gröbner bases of some symmetric systems and their application to coding theory, J. Symb. Comput. **35**(2), 177–194 (2003).
[8] D. R. Richman, On vector invariants over finite fields, Adv. Math. **81**(1), 30–65 (1990).
[9] B. J. Schmid, Finite groups and invariant theory, in: Topics in Invariant Theory, Lecture Notes in Mathematics Vol. 1478 (Paris, 1989/1990, Springer, Berlin, 1991), pp. 35–66.
[10] M. Sezer, A note on the Hilbert ideals of a cyclic group of prime order, J. Algebra **318**(1), 372–376 (2007).
[11] M. Sezer and R. J. Shank, On the coinvariants of modular representations of cyclic groups of prime order, J. Pure Appl. Algebra **205**(1), 210–225 (2006).
[12] L. Smith, A modular analog of a theorem of R. Steinberg on coinvariants of complex pseudoreflection groups, Glasg. Math. J. **45**(1), 69–71 (2003).
[13] R. Steinberg, Differential equations invariant under finite reflection groups, Trans. Am. Math. Soc. **112**, 392–400 (1964).
[14] T. Wada and H. Ohsugi, Gröbner bases of Hilbert ideals of alternating groups, J. Symb. Comput. **41**(8), 905–908 (2006).

© 2012 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim