BULL. AUSTRAL. MATH. SOC. 13A50
VOL. 60 (1999) [509–520]

ON RINGS OF INVARIANTS OF NON-MODULAR ABELIAN GROUPS

H.E.A. CAMPBELL, J.C. HARRIS AND D.L. WEHLAU

In memory of Paul Erdös

We study the ring of invariant Laurent polynomials associated to the action of a finite diagonal group G on the symmetric algebra of a vector space over a field $\mathbf{F}$. Here the characteristic p of the field $\mathbf{F}$ necessarily does not divide the order $q = |G|$ of the group, so G is said to be non-modular. For certain representations of such groups, we can characterise generators of the ring of invariant polynomials in the original symmetric algebra, extending results of Campbell, Hughes, Pappalardi and Selick. In particular we obtain a recursive formula for the number of minimal generators for these rings of invariants.

1. INTRODUCTION

We study the invariant theory of finite Abelian groups G in characteristics not dividing the order q of G. Such a group is said to be non-modular. We are able to characterise a generating set of monomials for the ring of invariants for certain representations of certain cyclic groups, which are general versions of the groups studied in [3]. We have been unable to characterise generating monomials for S^G for more general G. The reduced regular representation is of interest. In particular, in [7], Dixmier, Erdös, and Nicolas, and in [10], Kac, determine lower bounds for the number of algebra generators needed for the ring of invariants of the reduced regular representation of $\mathbf{Z}/n\mathbf{Z}$. The motivation in both papers is an application to the study of the classical invariant theory of binary forms. Our representations of these groups are better behaved so our results are stronger. In particular the analogue of our Proposition 5.3 is known to be false in general for the reduced regular representation of a cyclic group. Elashvili and Jibladze have considered this question in detail in [8, 9].

We suppose V is a vector space of dimension $\ell + 1$ over a field $\mathbf{F}$ of characteristic p possibly 0 with p not dividing q. By extending the field, if necessary, we may assume G acts diagonally on V and hence maps monomials to monomials in the symmetric algebra $R = \mathrm{Sym}(V)$ of V. It follows that G also acts on the ring K of Laurent polynomials

Received 30th March, 1999
This research supported in part by the Natural Sciences and Engineering Research Council of Canada.

and that K^G is again a ring of Laurent polynomials. We examine various extensions of these ideas to the case of relative invariants associated to a character of the group (weight submodules) and also to a case of particular interest to topologists, the invariants of the group acting on a polynomial algebra tensored with an exterior algebra. Our techniques are elementary.

This paper is a sequel to the paper [3] which was in turn a sequel of [4]. This paper is related also to our paper [2]. In that paper, we study the minimal free resolutions o. the 3-dimensional representations of the some of the groups studied here in Section 5. We show that these resolutions display a kind of internal duality by giving an explicit construction of the resolutions.

We note that many of the methods here apply also to diagonalisable infinite groups (see [12, 13], for example).

2. Diagonalisation.

Let V be a vector space of dimension $\ell+1$ over the field $\mathbf{F}$ with basis $\{u_\ell, \dots, u_0\}$ and let $G \subset GL(V) \cong GL_{\ell+1}(\mathbf{F})$ be any non-modular Abelian subgroup of order q. Then G can be diagonalised. That is, there is a finite field extension $\widehat{\mathbf{F}} \supset \mathbf{F}$ and a basis $\{y_\ell, \dots, y_0\}$ for $\widehat{\mathbf{F}} \otimes V = W$ with respect to which all elements of G, considered as a subgroup of $GL_{\ell+1}(\widehat{\mathbf{F}})$, are diagonal. In more detail, there exists a primitive q-th root of unity $\zeta \in \widehat{\mathbf{F}}$ with the property that for each $g \in G$ we have $g = \mathrm{diag}(\zeta^{a_\ell}, \dots, \zeta^{a_0})$ with respect to the basis $\{y_\ell, \dots, y_0\}$. We shall write $\theta(g) = (a_\ell, \dots, a_0)$.

The symmetric algebras of V and W. There are two sorts of algebras associated with V and W which we wish to consider. The first are the symmetric algebras of V and W over their respective fields

$$R = \mathrm{Sym}(V) \cong \mathbf{F}[\mathbf{u}_\ell, \dots, \mathbf{u}_0]$$
$$S = \mathrm{Sym}(W) \cong \widehat{\mathbf{F}}[\mathbf{u}_\ell, \dots, \mathbf{u}_0] = \widehat{\mathbf{F}}[\mathbf{y}_\ell, \dots, \mathbf{y}_0]$$

and their respective rings of invariants, denoted R^G and S^G. Note that diagonal groups map monomials in $y_\ell, \dots, y_0$ to scalar multiples of themselves, so that S^G has a basis given by invariant monomials. We also study $T = \mathbf{F}[\mathbf{y}_\ell, \dots, \mathbf{y}_0]$ and we define $T^G = S^G \cap T$ although the notation is misleading: the group G does not act on T.

Isotypic modules for cyclic groups. For the moment we suppose G is a cyclic group with generator g of order q. We write $\theta = \theta(g)$. We take a monomial y^I in S^G. Then $g(y^I) = \zeta^{\theta \cdot I} y^I$ where $\cdot$ denotes the usual dot product of vectors in the lattice $\mathbf{Z}^n$. We write $\theta \cdot I = m(I)q + w(I)$ for $0 \leqslant w(I) < q$. We call $m(I)$ the multiplicity of I and $w(I)$ the weight of I. For $0 \leqslant w < q$, we define $\mathcal{W}(w)$ to be the $\widehat{\mathbf{F}}$-vector space spanned by the monomials y^I having weight w. We have $S^G = \mathcal{W}(0)$. We observe that

multiplication in S maps $\mathcal{W}(w) \otimes \mathcal{W}(w')$ to $\mathcal{W}(w+w')$, where $w+w'$ is taken mod q. In particular $\mathcal{W}(w)$ is a module over S^G. We call the isotypic component $\mathcal{W}(w)$ the weight w submodule and we observe that $S = \bigoplus_{w=0}^{q-1} \mathcal{W}(w)$.

We are particularly interested in the invariant monomials, those which are mapped to themselves by all elements of G. We note that a monomial y^I is invariant if and only if we have $\theta \cdot I \equiv 0 \pmod{q}$. We shall call such an exponent sequence I invariant.

Now G has exactly q irreducible representations over $\widehat{\mathbf{F}}$. It is natural to think of S as a graded representation of G and ask for its decomposition into isotypic components. This is exactly the decomposition $S = \bigoplus_{w=0}^{q-1} \mathcal{W}(w)$. In the literature, the elements of the weight submodules are sometimes referred to as semi-invariants or as relative invariants.

ISOTYPIC MODULES FOR ARBITRARY NON-MODULAR ABELIAN GROUPS. We write $G = G_1 \times \cdots \times G_r$ for some collection of cyclic groups $\{G_s\}$ with generators $\{g_s\}$ of orders $\{q_s\}$. We shall assume some such decomposition to be fixed throughout the paper. We note in passing that the torsion decomposition of G results in a minimal number of generators for G, [**1**, Theorem 6.4, page 472]. This is a useful observation for those readers interested in computations.

We define $\theta_s = \theta(g_s) = (a_{s,\ell}, \ldots, a_{s,0})$. It follows from the equation $g_s^{q_s} = 1$ that each entry $a_{s,i}$ of θ_s is divisible by q/q_s. We write $\theta_s = q\rho_s/q_s$. We extend the notion of multiplicity and weight to $G = G_1 \times \cdots \times G_r$ by setting $m(I) = \big(m_1(I), \ldots, m_r(I)\big)$ and $w(I) = \big(w_1(I), \ldots, w_r(I)\big)$ where we have $\rho_s \cdot I = m_s(I)q_s + w_s(I)$ with $0 \leqslant w_s < q_s$. We obtain weight submodules $\mathcal{W}(w_1, \ldots, w_r)$ for $0 \leqslant w_s < q_s$. Now G is non-modular and Abelian, and so G is isomorphic to its character group. Therefore, the weight submodules $\mathcal{W}(w_1, \ldots, w_r)$ again have the property that $S = \oplus \mathcal{W}(w_1, \ldots, w_r)$ corresponding to the decomposition of S into graded isotypic components over $\widehat{\mathbf{F}}$. We note that $S^G = \mathcal{W}(0, \ldots, 0)$. Of course, $\mathcal{W}(w_1, \ldots, w_r)$ is a module over S^G just as above.

We let $\mathcal{W}(w_1, \ldots, w_{r-1}, *)$ denote the submodule of S with basis consisting of those monomials y^I with $w_s(I) = w_s$ for $0 \leqslant s \leqslant r-1$. We observe that $\mathcal{W}(w_1, \ldots, w_{r-1}, w_r)$ can be thought of as the submodule of $\mathcal{W}(w_1, \ldots, w_{r-1}, *)$ with basis consisting of those monomials y^I of $\mathcal{W}(w_1, \ldots, w_{r-1}, *)$ with $w_r(I) = w_r$. In particular, we have

$$(S^{G_1 \times \cdots \times G_{r-1}})^{G_r} = S^G.$$

Some degree of care is required when reading this equation. We are here assuming that the group G has been diagonalised. In computations, one sometimes diagonalises first G_1 and then proceeds onto $G_1 \times G_2$.

A BOUND ON THE DEGREES OF GENERATORS FOR S^G. The following simple direct argument (see [**11**, Lemma 2.1]) shows that the invariant rings of the groups we study are generated in degrees less than or equal to the order of the group. Suppose we are given

an invariant monomial y^I, $I = (i_\ell, \dots, i_0)$, of degree d bigger than q. We consider the ordered list of exponent sequences $J_0 = I$, $J_1, \dots,$ $J_d = (0, \dots, 0)$ constructed as follows: J_{t+1} is formed from J_t by subtracting a 1 from the rightmost non-zero entry in J_t. We observe that y^{J_t} properly divides y^{J_s} if $t > s$. We consider the weight vector associated to each such sequence $w(J_t) = \big(w_1(J_t), \dots, w_r(J_t)\big)$. Since there are only q possible weight vectors, by the pigeon-hole principle there exists $t > s \geqslant 1$ with $w(J_s) = w(J_t)$. Therefore, $y^{J_s - J_t}$ is an invariant monomial properly dividing y^I.

A SLIGHT EXTENSION OF THE SYMMETRIC ALGEBRAS. The second sort of algebras we wish to consider are the algebras described by declaring all elements of V and W to have degree 2 and taking the free graded commutative algebras on $V \oplus s^{-1}V$ and $W \oplus s^{-1}W$ over their respective fields. Here $s^{-1}V$ denotes a copy of V with all elements taken to be of degree 1 and basis $\{v_\ell, \dots, v_0\}$ where $v_i = s^{-1}u_i$. In other words we have the algebras

$$R \otimes D \cong \mathbf{F}[\mathbf{u}_\ell, \dots, \mathbf{u}_0] \otimes \Lambda[\mathbf{v}_\ell, \dots, \mathbf{v}_0],$$
$$S \otimes E \cong \widehat{\mathbf{F}}[\mathbf{u}_\ell, \dots, \mathbf{u}_0] \otimes \Lambda[\mathbf{v}_\ell, \dots, \mathbf{v}_0] = \widehat{\mathbf{F}}[\mathbf{y}_\ell, \dots, \mathbf{y}_0] \otimes \Lambda[\mathbf{x}_\ell, \dots, \mathbf{x}_0],$$

Here $\Lambda[z_\ell, \dots, z_0]$ denotes the exterior algebra on the stated generators over the appropriate ground field. Also, we assume that $\{x_\ell, \dots, x_0\}$ is constructed from $\{v_\ell, \dots, v_0\}$ by mimicking the construction of the y's from the u's. Then G also acts on the exterior algebras above; and this action is diagonal when written in terms of the x's. We write $(R \otimes D)^G$, $(S \otimes E)^G$ for the G-invariants. We also consider $T \otimes F = \mathbf{F}[\mathbf{y}_\ell, \dots, \mathbf{y}_0] \otimes \Lambda[\mathbf{x}_\ell, \dots, \mathbf{x}_0]$ and even $(T \otimes F)^G$, although G does not act on $T \otimes F$. We shall call an exponent sequence (I, J) invariant if the corresponding monomial $y^I x^J$ is invariant. These representations of G admit weight decompositions similar to those discussed above, but we shall not pursue this further here.

We note that some of these rings of invariants can be realised as cohomology algebras. If $\mathbf{F} = \mathbf{F_p}$, the prime field, then we consider the group $V \rtimes G$ and its classifying space denoted here by X. By a standard theorem, see [5, pp.257–258], when p is odd, we have $H^*(X; \mathbf{F_p}) \cong (\mathbf{R} \otimes \mathbf{D})^{\mathbf{G}}$. It is also possible to construct a classifying space Y with $H^*(Y; \mathbf{F_p}) \cong \mathbf{R}^{\mathbf{G}}$.

3. Invariant Laurent polynomials.

We work with the rings of Laurent polynomials associated to S and T. That is, we localise S, respectively T, at the multiplicative subset generated by the product $y_\ell \cdots y_0$, to obtain algebras denoted K, respectively L. We observe that $K = \widehat{\mathbf{F}}[\mathbf{y}_\ell^{\pm 1}, \dots, \mathbf{y}_0^{\pm 1}]$ and $L = \mathbf{F}[\mathbf{y}_\ell^{\pm 1}, \dots, \mathbf{y}_0^{\pm 1}]$, so, for example the algebra $K \otimes D$ has basis given by the monomials $y^I x^J$ but now I is allowed to have negative entries. Furthermore, the group G still acts on $K \otimes D$ and we may ask for $(K \otimes D)^G$ and K^G. As above, G maps monomials to scalar multiples of themselves so these rings of invariant Laurent polynomials again

have a basis consisting of invariant monomials. Consequently we may once again refer to $(L \otimes D)^G$ and L^G even though the group G does not act on either $L \otimes D$ or L.

We often find it convenient to recast our results in the language of lattices. We let $\mathcal{L} = \mathbf{Z}^{\ell+1}$ denote the lattice of integer sequences of length $\ell + 1$ under component-wise addition. Given a generator g_s of G_s, we recall that $I \in \mathcal{L}$ has weight $w_s = w_s(I)$ and multiplicity $m_s = m_s(I)$ if $\rho_s \cdot I = m_s q_s + w_s$ for $0 \leqslant w_s < q_s$. We let $\mathcal{L}(w_1, \ldots, w_r)$ denote the collection of integer sequences with weights w_s with respect to a fixed generating set $\{g_s\}$ for G. We shall refer to the sequences which have weight zero for all generators g_s as the invariant sequences and we shall denote the set of all such by $\mathcal{L}^G$. It is clear that $\mathcal{L}^G$ is a sublattice of $\mathcal{L}$.

We let $\mathcal{M}$ denote the set of monomials y^I in K. It is clear that $\mathcal{M}$ is a free Abelian group with respect to multiplication. We extend the notions of weight and multiplicity to this context in the obvious way.

PROPOSITION 3.1. *There is a weight preserving isomorphism of lattices* $\log : \mathcal{M} \to \mathcal{L}$. *That is,* $I + J = \log(y^I y^J) = \log(y^I) + \log(y^J)$. *Furthermore, the following diagram commutes*

$$\begin{array}{ccc} \mathcal{M}(w) \times \mathcal{M}(w') & \xrightarrow{\times} & \mathcal{M}(w + w') \\ \downarrow \log & & \downarrow \log \\ \mathcal{L}(w) \times \mathcal{L}(w') & \xrightarrow{+} & \mathcal{L}(w + w'). \end{array}$$

INVARIANT LAURENT POLYNOMIALS OF CYCLIC GROUPS. For the moment we concentrate our attention on the case of a cyclic group G with generator g of order q, and we write θ for $\theta(g) = (a_\ell, \ldots, a_0)$.

PROPOSITION 3.2. *We may suppose that* $\gcd(a_\ell, \ldots, a_0) = 1$.

PROOF: Let $\alpha = \gcd(a_\ell, \ldots, a_0)$. Then $\theta = \theta(g) = \alpha(b_\ell, \ldots, b_0)$ with $\gcd(b_\ell, \ldots, b_0) = 1$. Let $d = \gcd(\alpha, q)$. Then $g^{q/d}$ acts trivially on W. But $G \subset GL(W)$, so $g^{q/d} = 1$. Therefore $d = 1$ since the order of G is q. Choose β with $\alpha\beta \equiv 1 \bmod q$. Then $\theta(g^\beta) = (b_\ell, \ldots, b_0)$. If $\alpha > 1$, we may replace the generator g of G by the generator g^β. □

By the proposition we may construct a sequence $\Phi = (\phi_\ell, \ldots, \phi_0)$ with the property that $\theta \cdot \Phi = 1$.

THEOREM 3.3. *The ring of G-invariant Laurent polynomials is again a ring of Laurent polynomials. That is, there exist* $\ell + 1$ *algebraically independent monomials* $t_\ell, \ldots, t_0$ *with the property that* $K^G = \widehat{\mathbf{F}}[\mathbf{t}_\ell^{\pm 1}, \ldots, \mathbf{t}_0^{\pm 1}]$ *and* $L^G = \mathbf{F}[\mathbf{t}_\ell^{\pm 1}, \ldots, \mathbf{t}_0^{\pm 1}]$.

PROOF: $\mathcal{L}$ is a free Abelian group of rank $\ell + 1$ and so we conclude that $\mathcal{L}^G$ is also a free Abelian group. Since $\{(q, 0, \ldots, 0), \ldots, (0, \ldots, 0, q)\}$ is a linearly independent set of invariant sequences we conclude that $\mathcal{L}^G$ has rank $\ell + 1$. That is, there must exist $\ell + 1$ invariant sequences $I_\ell, \ldots, I_0$ such that an arbitrary invariant sequence I admits a

https://doi.org/10.1017/S0004972700036674 Published online by Cambridge University Press

unique expression $I = \sum \alpha_s I_s$ for some set of $\alpha_s \in \mathbf{Z}$. We obtain the conclusions of the theorem by setting $t_s = y^{I_s}$.

Alternately, we may take $I_s = a_s(q+1)\Phi - \Delta_s$ for $\ell \geqslant s \geqslant 0$, where Δ_s is the exponent sequence of length $\ell + 1$ which has zeros everywhere except for a 1 in the s-th position from the right counting from 0. We observe that $\theta \cdot I_s = a_s q$ so I_s is invariant and has multiplicity a_s. Furthermore, if $I = (i_\ell, \ldots, i_0)$ is any invariant, then $I = \sum \alpha_s I_s$ for $\alpha_s = m(I)\phi_s - i_s$, as is easily checked. □

The best possible situation in invariant theory is that the ring of invariants of a polynomial algebra is again a polynomial algebra. We view this theorem as an analogue for rings of invariant Laurent polynomials, necessarily in the case of diagonal groups.

We denote by $\mathcal{L}^G(0) \subset \mathcal{L}^G$ the subset of weight zero sequences which have multiplicity zero as well. We observe that $\mathcal{L}^G(0)$ is a sublattice of $\mathcal{L}^G$ of codimension 1.

THEOREM 3.4. *Let $\{I_\ell, \ldots, I_1\}$ be a basis for the multiplicity zero sublattice $\mathcal{L}^G(0)$ and let I_0 be a sequence of weight zero and multiplicity 1. Then the set $\{I_\ell, \ldots, I_0\}$ is a basis for the invariant sublattice $\mathcal{L}^G$. Consequently we obtain a generating set for K^G by defining $t_s = y^{I_s}$.*

PROOF: Let I be any sequence in $\mathcal{L}^G$, that is, any sequence with $\theta \cdot I = mq$. Then $I - mI_0$ is in $\mathcal{L}^G(0)$ and hence $I - mI_0 = \sum_{s=1}^{\ell} \alpha_s I_s$. □

REMARK 3.5. Given an invariant sequence $I = \sum \alpha_s I_s$ we observe from the proof just given that $m(I) = \alpha_0$.

In certain cases we give explicit bases for the invariant sublattice as in the theorem just given.

We may take $I_0 = q\Phi$ where Φ is defined following Proposition 3.2. In the event that $|G| = q = \sum a_s$, we may take $I_0 = (1, \ldots, 1)$.

When $a_0 = 1$ the exponent sequences $I_j = (0, \ldots, 0, 1, 0, \ldots, 0, -a_j)$ for $\ell \geqslant j \geqslant 1$ form a basis for the multiplicity zero sublattice and we may take $I_0 = (0, \ldots, 0, q)$.

LAURENT WEIGHT SUBMODULES FOR CYCLIC GROUPS. We denote by $K(w)$ the set of Laurent polynomials with basis the monomials of K of weight w for $0 \leqslant w < q$. It follows immediately from Proposition 3.1 that $K(w)$ is a module over the Laurent ring $K^G = K(0)$.

PROPOSITION 3.6. *If I is any sequence of weight w and multiplicity 0, then $K(w) = K^G \cdot y^I$.*

PROOF: If $y^J \in K(w)$ then $y^{J-I} \in K^G$. □

Again, the best possible situation in invariant theory is that a weight module be free over the ring of invariants. This corollary may be viewed as an analogue for weight modules consisting of Laurent polynomials.

INVARIANT LAURENT POLYNOMIALS FOR ARBITRARY NON-MODULAR GROUPS. We observe that Theorem 3.3 applies to any group acting diagonally on any ring of Laurent polynomials. In particular, if H is a group which acts on $K^G = \widehat{\mathbf{F}}[\mathbf{t}_\ell^{\pm 1}, \ldots, \mathbf{t}_0^{\pm 1}]$ in such a way as to map the generators t_s to scalar multiples of themselves then $(K^G)^H$ is again a ring of Laurent polynomials. In our situation, we have $G = G_1 \times \cdots \times G_r$ as above. It is easy to see that $K^G = (K^{G_1})^H$, where $H = G_2 \times \cdots \times G_r$. It is also easy to see that H acts diagonally on K^{G_1} since our generating set consists of monomials in the y's. This observation reduces the problem of constructing generators for K^G to the case G is cyclic. We observe that the analogue of Proposition 3.6 also holds.

4. ALGEBRA GENERATORS FOR OUR RINGS OF INVARIANTS

In this section we reduce the detection of minimal sets of generators for our various rings of invariants to the detection of a minimal set of generators for S^G.

Suppose we are given a graded algebra A over one of the fields in question. We define $D(A)$ to be the ideal of A generated by all non-trivial products, that is, $D(A) = A_+^2$ where A_+ denotes the elements of positive degree in A. We define the space of indecomposables associated to A to be the quotient $A_+/D(A)$. We note that a minimal generating set for the algebra A is any subset of A_+ whose images in $A_+/D(A)$ form a basis. We let $Q(A)$ denote such a minimal algebra generating set. $Q_i(A)$ will denote the subset of this minimal algebra generating set consisting of those elements of degree i.

We say a non-negative invariant exponent sequence I is decomposable if there exist non-negative non-zero invariant exponent sequences J and K such that $I = J + K$, otherwise we say I is an indecomposable invariant sequence. In the cases of interest to us, we note that $Q(S^G)$ and $Q(T^G)$ consist of indecomposable invariant monomials y^I. These notions admit the obvious extensions to $y^I x^J$.

LEMMA 4.1.

$$\begin{aligned} \big|Q_i(R^G)\big| &= \big|Q_i(S^G)\big|. \\ \big|Q_i\big((R\otimes D)^G\big)\big| &= \big|Q_i\big((S\otimes E)^G\big)\big|, \\ Q(S^G) &= Q(T^G), \\ Q\big((S\otimes E)^G\big) &= Q\big((T\otimes F)^G\big), \end{aligned}$$

where $|X|$ denotes the cardinality of the set X.

PROOF: The first two statements follow from $S^G = R^G \otimes_{\mathbf{F}} \widehat{\mathbf{F}}$ and $(S\otimes E)^G = (R\otimes D)^G \otimes_{\mathbf{F}} \widehat{\mathbf{F}}$. The third and fourth statements are trivial. □

In light of this result we focus our attention on $(S\otimes E)^G$ and S^G. When $y^I x^J$ is an invariant monomial we shall refer to the sequence (I, J) as invariant. We note that J must consists of 0's and 1's.

We define $z_i = y_i^{-1}x_i$ with degree -1; note that z_i is invariant. We define the support of y^I, denoted supp(I), to be $\{\ell \mid i_\ell > 0\}$. Let $\mathcal{E}(I)$ denote a basis for the exterior algebra over $\widehat{\mathbf{F}}$ on generators z_ℓ for $\ell \in \text{supp}(I)$.

THEOREM 4.2. *$(S \otimes E)^G$ is minimally generated as an algebra by the set $\{y^{I-J}x^J = y^I z^J \mid y^I \in Q(S^G)$ and $z^J \in \mathcal{E}(I)\}$. Note that there are $2^{|\text{supp}(I)|}$ such generators of $(S \otimes E)^G$ for each generator y^I of S^G.*

PROOF: We show for any I and J (where J consists of 0's and 1's) that $y^{I-J}x^J$ is a generator of $(S \otimes E)^G$ if and only if y^I is a generator of S^G. Suppose $y^{I-J}x^J$ decomposes, that is $y^{I-J}x^J = (y^{I_1-J_1}x^{J_1})(y^{I_2-J_2}x^{J_2})$ where $(I_t - J_t, J_t)$ is a non-negative non-zero invariant. We obtain $y^I = y^{I_1}y^{I_2}$ by dividing this equation by $z^J = z^{J_1}z^{J_2}$. Conversely, if $y^I = y^{I_1}y^{I_2}$, choose J_1 and J_2 with $\text{supp}(J_t) \subset \text{supp}(I_t)$ and $J_1 + J_2 = J$. Then multiplication by $z^J = z^{J_1}z^{J_2}$ yields $y^I z^J = (y^{I_1}z^{J_1})(y^{I_2}z^{J_2})$. □

5. Certain representations of certain cyclic groups

Our purpose in the present section is to characterise the generators of S^G in terms of a generating set of invariant Laurent monomials in some special cases.

Here we suppose that the generator g of the cyclic group G has $\theta = (a_\ell, \ldots, a_0)$ with $a_s = n^s$ for $s = 0, \ldots, \ell$ for some fixed positive integer n. We further suppose that q, the order of G, equals $\sum n^s$. In particular $\Omega_0 = (1, \ldots, 1)$ is invariant. In this situation we find a generating set for the ring K^G of invariant Laurent polynomials that is somewhat more convenient than the ones constructed in Section 3.

We recall that an invariant sequence I has multiplicity $m(I)$ exactly when $\theta \cdot I = m(I)q$. Of course, any non-negative sequence I of multiplicity 1 corresponds to an indecomposable of S^G. We observe that $\theta \cdot \Omega_0 = q$ so that Ω_0 has multiplicity 1. Next we observe that the sequences $\Omega_\ell = (-1, n, 0, \ldots, 0)$, $\ldots$, $\Omega_2 = (0, \ldots, 0, -1, n, 0)$, $\Omega_1 = (0, \ldots, 0, -1, n)$ are all invariant and have multiplicity 0. Indeed $\{\Omega_s \mid \ell \geqslant s \geqslant 1\}$ is a basis for the multiplicity zero sublattice and $\{\Omega_s \mid \ell \geqslant s \geqslant 0\}$ is a basis for the invariant sublattice. We define $t_s = y^{\Omega_s}$ for $\ell \geqslant s \geqslant 0$. It follows that $\{t_\ell^{\pm 1}, \ldots, t_0^{\pm 1}\}$ is a generating set for the ring K^G of invariant Laurent polynomials

We shall denote by Ω the sequence $(n, 0, \ldots, 0, -1)$. A routine computation shows $\Omega = (n-1)\Omega_0 - (\Omega_\ell + \cdots + \Omega_1)$.

For an arbitrary sequence $I = (i_\ell, \ldots, i_0)$ of $\ell + 1$ integers we define $\sigma(I) = (i_{\ell-1}, \ldots, i_0, i_\ell)$. We note $\Omega = \sigma(\Omega_\ell)$, $\Omega_s = \sigma(\Omega_{s-1})$ for $\ell \geqslant s \geqslant 2$, $\Omega_1 = \sigma(\Omega)$ and $\Omega_0 = \sigma(\Omega_0)$.

LEMMA 5.1. *I is an invariant sequence if and only if $\sigma(I)$ is an invariant sequence. I is an invariant non-negative indecomposable sequence if and only if $\sigma(I)$ is an invariant non-negative indecomposable sequence.*

PROOF: We have $\theta \cdot I = \sum n^s i_s = mq$. We calculate

$$\begin{aligned}\theta \cdot \sigma(I) &= n^\ell i_{\ell-1} + \cdots + ni_0 + i_\ell = n(n^{\ell-1} i_{\ell-1} + \cdots + i_0) + i_\ell \\ &= n(mq - n^\ell i_\ell) + i_\ell = nmq - (n^{\ell+1} - 1) i_\ell \\ &= \big(nm - (n-1) i_\ell\big) q.\end{aligned}$$

□

We say that invariant sequences I and J are *friends* if there is an s with $\sigma^s(I) = J$.

LEMMA 5.2. *If I is a non-negative invariant indecomposable sequence and $J = I - \Omega_s$ is non-negative for some s, $\ell \geqslant s \geqslant 1$ then J is an invariant indecomposable sequence.*

PROOF: Suppose not, then $J = K + L$ for K and L non-negative invariant sequences. So $I - \Omega_s = K + L$. Now $i_s + 1 = k_s + l_s \geqslant 1$ so we have $k_s \geqslant 1$, say. But then $M = K + \Omega_s$ is a non-negative invariant sequence and $I = M + L$, contradicting the indecomposability of I. □

PROPOSITION 5.3. *If I is an invariant indecomposable non-negative sequence then I has a friend of multiplicity 1.*

PROOF: We shall assume that I is a non-negative invariant indecomposable of lowest degree such that all friends of I have multiplicity larger than 1.

We observe that I must have at least one entry equal 0 or else $I = (I - \Omega_0) + \Omega_0$. By choosing a friend of I, if necessary, we may assume that $i_\ell = 0$.

We write $I = \sum b_s \Omega_s$ and we note that then

$$I = (b_0 - b_\ell, b_0 + nb_\ell - b_{\ell-1}, \ldots, b_0 + nb_2 - b_1, b_0 + nb_1).$$

By Remark 3.5, we have $m(I) = b_0$ which is bigger than 1. Furthermore, $b_0 = b_\ell$ since $i_\ell = 0$.

Our immediate goal is to show that I has an entry larger than $n+1$. Suppose $b_1 > 0$. Then $b_0 + nb_1 > n + 1$. If $b_1 \leqslant 0$ and $b_2 > 0$ then $b_0 + nb_2 - b_1 > n + 1$. Similarly, if $b_1, \ldots b_{s-1} \leqslant 0$ and $b_s > 0$ we have $b_0 + nb_s - b_{s-1} > n + 1$. If $b_1, \ldots, b_{\ell-1} \leqslant 0$ then $b_0 + nb_\ell - b_{\ell-1} > n + 1$ since $b_\ell = b_0 > 1$.

Let us suppose that $i_s > n + 1$. Note that since $i_\ell = 0$ we have $s \neq \ell$. Put $J = I - \Omega_{s+1}$. By Lemma 5.2 we have that J is a non-negative invariant indecomposable sequence with the degree of J strictly less than the degree of I. Hence J has a friend of multiplicity 1, call it J'. Since the multiplicity of Ω_{s+1} is 0, I and J have the same multiplicity. Indeed, since $m(\Omega_i) = 0$ for $1 \leqslant i \leqslant \ell$, $\sigma^t(I)$ and $\sigma^t(J)$ have the same multiplicities for $t \neq \ell - s$. However, $\Omega = \sigma^{\ell-s}(\Omega_{s+1})$ has multiplicity $n - 1$. It follows that $J' = \sigma^{\ell-s}(J) = \sigma^{\ell-s}(I) - \Omega$. Let $I' = \sigma^{\ell-s}(I)$. Now $m(J') = m(I') - (n - 1)$, so $m(I') = n$. However, the ℓ-th entry of I' is i_s which is at least $n + 2$. So $m(I')q = \theta \cdot I'$ $\geqslant (n+2)n^\ell > n(n^\ell + n^{\ell-1} + \cdots + 1) = nq$ contradicting our conclusion that $m(I') = n$. □

https://doi.org/10.1017/S0004972700036674 Published online by Cambridge University Press

The generators of multiplicity one are the sequences $I = (i_\ell, \dots, i_0)$ which satisfy the following conditions:

$$\begin{aligned} &0 \leqslant i_\ell \leqslant 1, \qquad 0 \leqslant i_{\ell-1} \leqslant n + 1 - n i_\ell, \qquad \dots, \\ &0 \leqslant i_s \leqslant \sum_{t=0}^{\ell-s} n^t - \sum_{t=s}^{\ell-s} i_t n^{t-s}, \qquad \dots, \\ &0 \leqslant i_1 \leqslant \sum_{t=0}^{\ell-1} n^t - \sum_{t=1}^{\ell-1} i_t n^{t-1}, \qquad i_0 = q - \sum_{s=1}^{\ell} i_s n^s. \end{aligned}$$

Here is a recursive way to compute the number of generators of multiplicity one. We define $J(n,t) = \left\{ I = (\dots, 0, \dots, 0, i_k, \dots, i_0) \;\middle|\; \sum_{s=0}^{\infty} i_s n^s = t,\ i_s \geqslant 0 \right\}$. We observe that if $i_k \neq 0$ then $k \leqslant \log_n(t)$ so that $J(n,t)$ is finite. We define $j(n,t) = |J(n,t)|$. Since $q = \sum_{s=0}^{\ell} n^s$, $J(n,q)$ is the set of generators of multiplicity one. It is easy to see that

$$j(n, nt + r) = j(n, nt)$$

for $0 \leqslant r \leqslant n-1$ since the set function sending $(0, \dots, 0, i_k, \dots, i_0)$ in $J(n,nt)$ to $(0, \dots, 0, i_k, \dots, i_0 + r)$ in $J(n, nt+r)$ is a bijection. We observe that $J(n,t)$ embeds in $J(n,nt)$ via the set function taking $(0, \dots, 0, i_k, \dots, i_0)$ to $(0, \dots, 0, i_k, \dots, i_0, 0)$. Also, $J\big(n, n(t-1)\big)$ embeds in $J(n,nt)$ via the set function taking $(0, \dots, 0, i_k, \dots, i_0)$ to $(0, \dots, 0, i_k, \dots, i_0 + n)$. It follows that

$$j(n,nt) = j\big(n, n(t-1)\big) + j(n,t).$$

REMARK 5.4. We observe that $j(n,t)$ is the number of partitions of t into powers of n and consequently

$$\prod_{s=0}^{\infty} \frac{1}{1 - \lambda^{n^s}} = \sum_{t=0}^{\infty} j(n,t) \lambda^t.$$

Topologists may want to note that for n prime, $j(n,t)$ is the dimension of the dual Brown-Gitler module (after modding out by the Bockstein, for n odd).

The calculation of $j(n,t)$ is called Mahler's partition problem by N. G. de Bruijn, [6]. He gives an asymptotic formula as follows: For $t \to \infty$

$$\begin{aligned} \ln j(n,nt) = {} & \frac{1}{2 \ln n} \left(\ln \frac{t}{\ln n} \right)^2 \\ & + \left(\frac{1}{2} + \frac{1}{\ln n} + \frac{\ln \ln n}{\ln n} \right) \ln t \\ & - \left(1 + \frac{\ln \ln n}{\ln n} \right) \ln \ln t \\ & + \phi \left(\frac{\ln t - \ln \ln t}{\ln n} \right) + o(1). \end{aligned}$$

Here ϕ is a periodic function of period 1, hence bounded. We note that $j(n, n^\ell + \cdots + n + 1) = j\big(n, n(n^{\ell-1} + \cdots + n + 1)\big)$.

The following table gives values of $j(n,q)$ where $q = \sum_{s=0}^{\ell} n^s$ for some small values of n and ℓ.

$n\backslash\ell$	2	3	4	5	6	7
2	6	26	166	1626	25510	664666
3	7	47	682	23132	1913821	3.98×10^8
4	8	80	2368	220288	66499072	6.71×10^{10}
5	9	128	6876	1446167	1.23×10^9	4.35×10^{12}
6	10	194	17242	7155602	1.44×10^{10}	1.44×10^{14}
7	11	281	38516	28591511	1.19×10^{11}	
8	12	392	78512	96846112	7.67×10^{11}	
9	13	530	148678	2.88×10^8	4.02×10^{12}	
10	14	698	265086	7.69×10^8	1.79×10^{13}	

This table gives the number of generators of S^G, $f(n,\ell)$, for some small values of n and ℓ.

$n\backslash\ell$	2	3	4	5	6	7
2	13	79	681	8595	165677	5095775
3	16	159	3151	134388	13229014	
4	19	287	11411	1306983	4.64×10^8	
5	22	475	33706	8634888		
6	25	735	85210	42828867		
7	28	1079	191131			
8	31	1591	390551			
9	34	2067	740686			
10	37	2735	1321881			

Since every generator has a friend of multiplicity one, it is clear that $f(n,\ell) \leqslant (\ell+1)j(n,\ell)$. From the tables it appears that the ratio $f(n,\ell)/j(n,\ell)$ approaches $\ell+1$ as n tends to infinity.

References

[1] M. Artin, *Algebra* (Prentice Hall, Englewood Cliffs, N.J., 1991).

[2] H.E.A. Campbell, J.C. Harris and D.L. Wehlau, 'Internal duality in resolutions of certain rings of invariants', *J. Algebra* **215** (1999), 1–33.

[3] H.E.A. Campbell, I.P. Hughes, F. Pappalardi and P.S. Selick, 'On the ring of invariants of $\mathbf{F}_{2^s}$', *Comment. Math. Helv.* **66** (1991), 322–331.

[4] H.E.A. Campbell and P.S. Selick, 'Polynomial algebras over the Steenrod algebra', *Comment. Math. Helv.* **65** (1990), 171–180.

[5] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Math. Series **19** (Princeton University Press, Princeton, N.J., 1956).

[6] N.G. de Bruijn, 'On Mahler's partition problem', *Indiag. Math.* **10** (1948), 220–230.

[7] P. Erdös, J. Dixmier and J.-L. Nicolas, 'Sur le nombre d'invariants fondamentaux des formes binaires', *C.R. Acad Sci. Paris Sér. I Math.* **305** (1987), 319–322.

[8] A. Elashvili and M. Jibladze, 'Hermite reciprocity for the regular representations of cyclic groups', (preprint).

[9] A. Elashvili and M. Jibladze, Untitled, *Institute of Mathematics of Georgian Academy of Sciences*, (preprint 1996).

[10] V. Kac, 'Root systems, representations of quivers and invariant theory', in *Invariant theory*, Lecture Notes in Math. **996** (Springer-Verlag, Berlin, Heidelberg, New York, 1983), **pp.** 74–108.

[11] B. Schmid, 'Finite groups and invariant theory', in *Topics in invariant theory*, Lecture Notes in Math. **1478** (Springer-Verlag, Berlin, Heidelberg, New York, 1991), **pp.** 35–66.

[12] D.L. Wehlau, 'Constructive invariant theory for tori', *Ann. Inst. Fourier (Grenoble)* **43** (1993), 1055–1066.

[13] D.L. Wehlau, 'When is a ring of torus invariants a polynomial ring?', *Manuscripta Math* **82** (1994), 161–170.

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
Canada K7L 3N6
e-mail: eddy@mast.queensu.ca

Department of Mathematics
University of Toronto
Toronto, Ontario
Canada M5S 1A1
e-mail: harris@math.toronto.edu

Department of Mathematics and Computer Science
Royal Military College
Kingston, Ontario
Canada M5S 1A1
and
Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
Canada K7L 3N6
e-mail: wehlau@mast.queensu.ca