THE NOETHER NUMBERS FOR CYCLIC GROUPS OF PRIME ORDER

P. FLEISCHMANN, M. SEZER, R.J. SHANK, AND C.F. WOODCOCK

ABSTRACT. The Noether number of a representation is the largest degree of an element in a minimal homogeneous generating set for the corresponding ring of invariants. We compute the Noether number for an arbitrary representation of a cyclic group of prime order, and as a consequence prove the "$2p-3$ conjecture".

1. INTRODUCTION

Let V denote a finite dimensional representation of a finite group G over a field $\mathbf{F}$, i.e., V is a finite module over the group ring $\mathbf{F}G$. The action of G on V induces an action of G on the dual V^* which extends to an action by degree preserving algebra automorphisms on the symmetric algebra of V^*, $\mathbf{F}[V] := S(V^*)$. The *ring of invariants*,

$$\mathbf{F}[V]^G := \{f \in \mathbf{F}[V] \mid g(f) = f, \ \forall g \in G\},$$

is a finitely generated subring of $\mathbf{F}[V]$, and can be interpreted as the ring of regular functions on the categorical quotient $V//G$. Since the action of G on $\mathbf{F}[V]$ preserves degree, the generators can be chosen to be homogeneous. The *Noether number* of the representation, $\beta(V)$, is defined to be the least integer d such that $\mathbf{F}[V]^G$ is generated by homogeneous elements of degree less than or equal to d. Emmy Noether [13] proved that if $\mathbf{F}$ has characteristic zero, then $\beta(V) \le |G|$. This result has been extended to all non-modular representations by Fleischmann [8] and Fogarty [9]. It is clear that a non-trivial non-modular representation of a cyclic group of prime order has Noether number $|G|$. In fact, cyclic groups are the only groups with non-modular representations having $|G|$ as the Noether number (see Schmid [17] for characteristic zero and Sezer [18] for the generalisation to non-modular representations). It follows from the work of Richman (see [15] and [16]), that $|G|$ is not an upper bound for $\beta(V)$ for modular representations. It has been conjectured that $\beta(V) \le \max\{|G|, \dim(V)(|G|-1)\}$ (see [5, Remark 3.9.10]). Derksen & Kemper have shown that

$$\beta(V) \le n(|G|-1) + |G|^{n \cdot 2^{n-1}+1} \cdot n^{2^{n-1}+1}$$

with $n := \dim(V)$ [5, Theorem 3.9.11], and Karagueuzian & Symonds [11] have shown that if $\mathbf{F} = \mathbf{F}_q$ then $\beta(V) \le (q^n-1)(nq-n-1)/(q-1)$ (for $n > 2$). The Noether number is an important characteristic of the ring of invariants. For example, *a prior* knowledge of the Noether number reduces the construction of a generating set to a problem in linear algebra.

For the remainder of the paper, $\mathbf{F}$ will denote a field of characteristic p for a prime number p, and $\mathbf{Z}/p$ will denote the cyclic group of order p. Despite the simplicity of the representation theory of $\mathbf{Z}/p$, the corresponding rings of invariants can be surprisingly complicated. From Ellingsrud & Skjelbred [7], we know that these rings of invariants almost always fail to be Cohen-Macaulay. While formulae for the Hilbert series are known for all representations of $\mathbf{Z}/p$, see Almkvist & Fossum [1] and Hughes & Kemper [10], explicit generating invariants are known for only a few special cases.

Choose a generator σ for $\mathbf{Z}/p$. In $\mathbf{F}\mathbf{Z}/p$, define $\Delta := \sigma - 1$ and $\mathrm{Tr} := \sum_{i=1}^{p} \sigma^i$. The isomorphism type of a representation of $\mathbf{Z}/p$ is determined by the Jordan canonical form of σ. If $n \leq p$, then the $n \times n$ matrix over $\mathbf{F}$ consisting of a single Jordan block with eigenvalue 1, has order p and determines an indecomposable $\mathbf{F}\mathbf{Z}/p$-module, which we denote by V_n. Note that for $n > p$, this matrix has order at least p^2 and, therefore, does not give a representation of $\mathbf{Z}/p$. Recall that 1 is the only p^{th} root of unity in $\mathbf{F}$. Thus $V_1, V_2, \ldots, V_p$ is a complete list, up to isomorphism, of the indecomposable $\mathbf{F}\mathbf{Z}/p$-modules. For a positive integer k, we will denote the direct sum of k copies of V_n by kV_n. Explicit generating sets for $\mathbf{F}[V_2]^{\mathbf{Z}/p}$ and $\mathbf{F}[V_3]^{\mathbf{Z}/p}$ were given by Dickson [6]. Generators for $\mathbf{F}[V_4]^{\mathbf{Z}/p}$ and $\mathbf{F}[V_5]^{\mathbf{Z}/p}$ can be found in [20]. The problem of finding an explicit generating set for $\mathbf{F}[V_n]^{\mathbf{Z}/p}$ for $n > 5$, remains open. Even when the invariants of the indecomposable summands are well understood, it can be difficult to construct generating sets for decomposable representations. Campbell & Hughes, in [4], describe a generating set for $\mathbf{F}[kV_2]^{\mathbf{Z}/p}$, proving a conjecture of Richman [15]. Generating sets have recently been constructed for $\mathbf{F}[V_2 + V_3]^{\mathbf{Z}/p}$ [21] and $\mathbf{F}[2V_3]^{\mathbf{Z}/p}$ [3]. Using the known generating sets, it is easy to see that $\beta(V_2) = \beta(V_3) = \beta(2V_2) = p$. It follows from [4] and [15], that $\beta(kV_2) = k(p-1)$ for $k > 2$. By [19, Remark 3.3], $\beta(V_4) = 2p - 3$. This paper is devoted to computing the Noether number for all remaining modular representations of $\mathbf{Z}/p$. An $\mathbf{F}\mathbf{Z}/p$-module is called *reduced* if it is has no trivial summands. Note that, for any $\mathbf{F}\mathbf{Z}/p$-module W, we have $\beta(kV_1 + W) = \beta(W)$, i.e., adding trivial summands does not change the Noether number. Therefore, it is sufficient to compute β for reduced $\mathbf{F}\mathbf{Z}/p$-modules. Also note that $V_n^{\mathbf{Z}/p}$, the vector space of fixed points, has dimension one. Therefore, for any $\mathbf{F}\mathbf{Z}/p$-module W, $\dim(W^{\mathbf{Z}/p})$ is the number of indecomposable summands in the decomposition of W.

Proposition 1.1. *Suppose that W is a reduced finite dimensional $\mathbf{F}\mathbf{Z}/p$-module.*
(a) If W contains a summand isomorphic to V_n with $n > 3$, then
$$\beta(W) = (p-1)\dim(W^{\mathbf{Z}/p}) + p - 2.$$
(b) If W is isomorphic to $mV_2 + \ell V_3$ with $\ell > 0$, then
$$\beta(W) = (p-1)\dim(W^{\mathbf{Z}/p}) + 1.$$

Proof. The first result follows from the lower bound given in Theorem 2.1 and the upper bound given in Corollary 3.4. The second result follows from the lower bound given in Theorem 2.1 and the upper bound given in Corollary 2.8 of [19].   □

We note that the "$2p - 3$ conjecture" [21, Conjecture 6.1] is a special case of Proposition 1.1 (a), and that Conjecture 1.1 of [19] follows from Theorem 3.3.

For general facts concerning the invariant theory of finite groups, see [2], [5] or [12].

2. Lower bounds

It is well known that $\beta(V_2) = \beta(V_3) = \beta(2V_2) = p$. For all other reduced representations, W, the number $(p-1)\dim(W^{\mathbf{Z}/p})$ is a lower bound for $\beta(W)$ (see [21, Proposition 3.1]). If $W = kV_2$ with $k > 2$, then this lower bound is sharp (see [4] and [15]). This section is devoted to proving the following theorem.

Theorem 2.1. *Suppose that W is a non-trivial reduced $\mathbf{FZ}/p$-module. Define $k :=\dim(W^{\mathbf{Z}/p})$. If W contains a summand isomorphic to V_n with $n > 3$, then $\beta(W) \geq k(p-1) + p - 2$. If W contains a summand isomorphic to V_n with $n > 2$, then $\beta(W) \geq k(p-1) + 1$.*

Recall that for a submodule $U \leq W$, $\beta(U) \leq \beta(W)$ [21, Theorem 4.2]. Thus to construct a lower bound, it is sufficient to find a lower bound for a submodule. To prove the first result, we give a lower bound for $\beta((k-1)V_2 + V_4)$ and to prove the second result, we give a lower bound for $\beta((k-1)V_2 + V_3)$.

Choose a basis $\{x_1, y_1, x_2, y_2, \ldots, x_{k-1}, y_{k-1}, w, x, y, z\}$ for $((k-1)V_2 + V_4)^*$ with $\Delta(y_i) = x_i$, $\Delta(x_i) = 0$, $\Delta(z) = y$, $\Delta(y) = x$, $\Delta(x) = w$ and $\Delta(w) = 0$.

Lemma 2.2. $\mathrm{Tr}\left((y_1 \cdots y_{k-1}z)^{p-1}y^{p-2}\right)$ *is indecomposable in* $\mathbf{F}[(k-1)V_2 + V_4]^{\mathbf{Z}/p}$.

Proof. Define $H := \mathrm{Tr}\left((y_1 \cdots y_{k-1}z)^{p-1}y^{p-2}\right)$. The proof is by induction on k. For $k = 1$, the result follows from Remark 3.3 of [19]. Assume $k > 1$. Suppose, by way of contradiction, that $H = \sum f_i h_i$ for some $f_i, h_i \in \mathbf{F}[(k-1)V_2 + V_4]_+^{\mathbf{Z}/p}$. We may assume that f_i, h_i and $f_i h_i$ are homogeneous with respect to multidegree, and that each $f_i h_i$ has multidegree $(p-1, p-1, \ldots, p-1, 2p-3)$. Use the inclusion of $V_1 + (k-2)V_2 + V_4$ into $(k-1)V_2 + V_4$ to define a projection $\pi : \mathbf{F}[(k-1)V_2 + V_4] \to \mathbf{F}[V_1 + (k-2)V_2 + V_4]$. Note that π is the algebra homomorphism taking x_1 to 0, y_1 to x_1 and fixing the other variables. Since π is equivariant, $\pi(H) = \mathrm{Tr}\left(\pi\left((y_1 \cdots y_{k-1}z)^{p-1}y^{p-2}\right)\right) = x_1^{p-1}\mathrm{Tr}\left((y_2 \cdots y_{k-1}z)^{p-1}y^{p-2}\right)$. Collecting all factors of x_1, write $\pi(f_i) = x_1^{n_i}\widetilde{f}_i$ and $\pi(h_i) = x_1^{m_i}\widetilde{h}_i$. Using the homogeneous multidegree assumption, $n_i + m_i = p-1$ and $\widetilde{f}_i, \widetilde{h}_i \in \mathbf{F}[(k-2)V_2 + V_4]^{\mathbf{Z}/p}$. Thus $\pi(H) = x_1^{p-1}\sum \widetilde{f}_i\widetilde{h}_i$. Therefore $\widetilde{H} := \mathrm{Tr}\left((y_2 \cdots y_{k-1}z)^{p-1}y^{p-2}\right) = \sum \widetilde{f}_i\widetilde{h}_i$. By the induction hypothesis, $\widetilde{H}$ is indecomposable in $\mathbf{F}[(k-2)V_2 + V_4]^{\mathbf{Z}/p}$. It is clear that $\widetilde{f}_i, \widetilde{h}_i \in \mathbf{F}[(k-2)V_2 + V_4]^{\mathbf{Z}/p}$. Suppose that one of the factors, say $\widetilde{f}_1$, is of degree zero. Then the multidegree of f_1 is $(n_1, 0, 0, \ldots, 0)$ with $n_1 < p$. Hence f_1 is a homogeneous element of degree less than p in $\mathbf{F}[x_1, y_1^p - x_1^{p-1}y_1] \cong \mathbf{F}[V_2]^{\mathbf{Z}/p}$. Thus $f_1 = cx_1^{n_1}$ for some $c \in \mathbf{F}$. Therefore $\pi(f_1) = 0$, giving $\widetilde{f}_1 = 0$. Hence $\sum \widetilde{f}_i\widetilde{h}_i$ determines a decomposition of $\widetilde{H}$, providing the required contradiction. $\square$

Choose a basis $\{x_1, y_1, \ldots, x_{k-1}, y_{k-1}, x, y, z\}$ for $((k-1)V_2 + V_3)^*$ with $\Delta(y_i) = x_i$, $\Delta(x_i) = 0$, $\Delta(z) = y$, $\Delta(y) = x$ and $\Delta(x) = 0$. We use the graded reverse lexicographic order with $x_1 < y_1 < x_2 < \cdots < y_{k-1} < x < y < z$.

Lemma 2.3. $\mathrm{Tr}\left((y_1 \cdots y_{k-1}z)^{p-1}y\right)$ *is indecomposable in* $\mathbf{F}[(k-1)V_2 + V_3]^{\mathbf{Z}/p}$.

Proof. The proof is by induction on k. For $k = 1$, $\mathbf{F}[V_3]^{\mathbf{Z}/p}$ is a hypersurface with generators in degrees 1, 2, p and p (see [6] or [14, Proposition 5.8]); the element

$\text{Tr}(yz^{p-1})$ has lead monomial y^p and may be chosen to be one of the generators. The induction step is essentially the same as the induction step in the proof of Lemma 2.2.   □

3. AN UPPER BOUND

Suppose that W is a reduced finite dimensional $\mathbf{FZ}/p$-module. The purpose of this section is to construct an upper bound on $\beta(W)$. Decompose W into a direct sum of indecomposable modules: $W = \oplus_{i=1}^{k} W_i$. For each i, choose an $\mathbf{FZ}/p$-module generator z_i for W_i^*. Define $d_i := \dim(W_i)$. Then

$$\bigcup_{i=1}^{k} \{\Delta^t(z_i) \mid t = 0, 1, \ldots, d_i - 1\}$$

is a basis for W^*. We use this basis to determine generating variables for $\mathbf{F}[W]$. Let A be the subalgebra of $\mathbf{F}[W]$ generated by

$$\bigcup_{i=1}^{k} \{\Delta^t(z_i) \mid t = 1, \ldots, d_i - 1\},$$

i.e., the subalgebra formed by omitting the "terminal variables". Suppose that $m = u_1 u_2 \cdots u_{p-1}$ is a monomial of degree $p - 1$ in A. For each u_i, there exists a variable, say w_i, with $\Delta(w_i) = u_i$. Define $m' = w_1 w_2 \cdots w_{p-1}$. Note that m' is a monomial of degree $p - 1$ in $\mathbf{F}[W]$. Define

$$F := \sum_{\ell \in \mathbf{F}_p} \prod_{j=1}^{p-1} \left(w_j - \sigma^\ell(w_j) \right),$$

where $\mathbf{F}_p$ denotes the field with p elements. For $S \subseteq \{1, 2, \ldots, p - 1\}$, define $S' = \{1, 2, \ldots, p - 1\} \setminus S$. Further define $X_S = \prod_{j \in S} w_j$ and $X_{S'} = \prod_{j \in S'} w_j$.

Lemma 3.1.
$$F = \sum_{S \subseteq \{1,2,\ldots,p-1\}} (-1)^{|S|} X_{S'} \text{Tr}(X_S).$$

Proof. Expanding, and using the fact that σ^ℓ is an algebra automorphism, gives

$$\prod_{j=1}^{p-1} \left(w_j - \sigma^\ell(w_j) \right) = \sum_{S \subseteq \{1,2,\ldots,p-1\}} (-1)^{|S|} X_{S'} \sigma^\ell(X_S).$$

Summing over $\ell \in \mathbf{F}_p$ gives the required formula.   □

We use a graded reverse lexicographic order with $\Delta^t(z_i) > \Delta^{t+1}(z_i)$ for $t < d_i - 1$, and denote the lead term of a polynomial f by $\text{LT}(f)$.

Lemma 3.2. $\text{LT}(F) = -m$.

Proof. Note that $\sigma^\ell(w_j) = w_j + \ell u_j + \cdots$, where the missing terms are lower in the order. Thus the lead term of $w_j - \sigma^\ell(w_j)$ is $-\ell u_j$. Since the lead term of a product is the product of the lead terms, we have $\text{LT}\left(\prod_{j=1}^{p-1} \left(w_j - \sigma^\ell(w_j) \right) \right) =$

$(-\ell)^{p-1} \prod_{j=1}^{p-1} u_j = \ell^{p-1} m$. Thus F is a sum of polynomials all with lead monomial m. The result follows from the fact that $\sum_{\ell \in \mathbf{F}_p} \ell^{p-1} = -1$. $\qquad\square$

Recall that the *Hilbert ideal* of W is the ideal in $\mathbf{F}[W]$ generated by homogeneous invariants of positive degree. The ring of *coinvariants*, denoted by $\mathbf{F}[W]_{\mathbf{Z}/p}$, is the finite dimensional graded algebra consisting of the quotient of $\mathbf{F}[W]$ by the Hilbert ideal.

Theorem 3.3. *The top degree of $\mathbf{F}[W]_{\mathbf{Z}/p}$ is bounded above by $k(p-1) + p - 2$.*

Proof. The Hilbert series of a graded ideal in $\mathbf{F}[W]$, and the series for the corresponding ideal of lead terms, coincide. Thus it is sufficient to bound the top degree of the quotient by the lead term ideal of the Hilbert ideal. It follows from Lemma 3.2 that every monomial of degree $p-1$ in A is in the lead term ideal. Furthermore, z_i^p is the lead term of the orbit product of z_i. Thus the monomials lying outside the lead term ideal are of the form $\gamma \prod_{i=1}^{k} z_i^{n_i}$ were γ is a monomial in A with degree at most $p-2$, and $n_i \leq p - 1$. $\qquad\square$

Corollary 3.4. *The Noether number of W is bounded above by $k(p-1) + p - 2$.*

Proof. The top degree of the coinvariants gives an upper bound for the degrees of a generating set of the image of transfer. It follows from [10, Lemma 2.12] that $\mathbf{F}[W]^{\mathbf{Z}/p}$ is generated by transfers, orbit products and elements of at most degree $k(p-1) - (\dim(W) - k)$. Thus the upper bound for the top degree of the coinvariants given in Theorem 3.3 gives an upper bound for the Noether number of W. $\qquad\square$

References

[1] G. Almkvist, R. Fossum, *Decompositions of exterior and symmetric powers of $\mathbf{Z}/p\mathbf{Z}$-modules in characteristic p and relations to invariants*, Séminaire d'Algèbre Paul Dubreil, 30ème année (Paris, 1976–1977), pp. 1–111, Lecture Notes in Math. **641**, Springer, 1978.

[2] D. Benson, *Polynomial Invariants of Finite Groups*, London Math. Soc. Lecture Note Series **190**, Cambridge Univ. Press, 1993.

[3] H.E.A. Campbell, B. Fodden, D.L. Wehlau, *Invariants of the diagonal C_p-action on V_3*, to appear in J. Algebra, http://www.mast.queensu.ca~wehlau/

[4] H.E.A. Campbell, I.P. Hughes, *Vector invariants of $U_2(\mathbf{F}_p)$: A proof of a conjecture of Richman*, Adv. in Math. **126** (1997) 1–20.

[5] H. Derksen, G. Kemper, *Computational Invariant Theory*, Encycl. Math. Sci. **130**, Springer, 2002.

[6] L.E. Dickson, *On invariants and the theory of numbers*, The Madison Colloquium (1913) Amer. Math. Soc., reprinted by Dover, 1966.

[7] G. Ellingsrud, T. Skjelbred, *Profondeur d'anneaux d'invariants en caractéristique p*, Compos. Math. **41** (1980) 233–244.

[8] P. Fleischmann, *The Noether bound in invariant theory of finite groups*, Adv. in Math. **152** (2000) 23–32.

[9] J. Fogarty, *On Noether's bound for polynomial invariants of a finite group*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001) 5–7.

[10] I.P. Hughes, G. Kemper, *Symmetric Powers of Modular Representations, Hilbert Series and Degree Bounds*, Comm. Algebra **28** (2000) 2059–2088.

[11] D.B. Karagueuzian, P. Symonds, *The module structure of a group action on a polynomial ring: a finiteness theorem*, preprint, http://www.ma.umist.ac.uk/pas/preprints/

[12] M.D. Neusel, L. Smith, *Invariant Theory of Finite Groups*, Math. Surveys and Monographs **94**, Amer. Math. Soc., 2002.

[13] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1916) 28–35.

[14] B.P. Peskin, *Quotient Singularities and Wild p-Cyclic Actions*, J. Algebra **81** (1983) 72–99.

[15] D. Richman, *On vector invariants over finite fields*, Adv. in Math. **81** (1990) 30–65.

[16] D. Richman, *Invariants of finite groups over fields of characteristic p*, Adv. Math. **124** (1996) 25–48.

[17] B.J. Schmid, *Finite groups and invariant theory*, Topics in invariant theory (Paris, 1989–1990), pp. 35–66, Lecture Notes in Math. **1478**, Springer, 1991.

[18] M. Sezer, *Sharpening the generalized Noether bound in the invariant theory of finite groups*, J. Algebra **254** (2002) 252–263.

[19] M. Sezer, R.J. Shank, *On the coinvariants of modular representations of cyclic groups of prime order*, to appear in J. Pure Appl. Algebra, http://www.kent.ac.uk/IMS/personal/rjs/index.htm

[20] R.J. Shank, *S.A.G.B.I. bases for rings of formal modular seminvariants*, Comment. Math. Helv. **73** (1998) 548–565.

[21] R.J. Shank, D.L. Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order* , Bull. London Math. Soc. **34** (2002) 438–450.

DEPARTMENT OF MATHEMATICS, BOĞAZIÇI UNIVERSITY,
TR-34342 BEBEK, ISTANBUL, TURKEY

E-mail address: mufit.sezer@boun.edu.tr

INSTITUTE OF MATHEMATICS, STATISTICS & ACTUARIAL SCIENCE,
UNIVERSITY OF KENT AT CANTERBURY, CT2 7NF, UK

E-mail address: P.Fleischmann@kent.ac.uk

E-mail address: R.J.Shank@kent.ac.uk

E-mail address: C.F.Woodcock@kent.ac.uk