Hermite reciprocity for the regular representations of cyclic groups

by A. Elashvili* and M. Jibladze**

A. Razmadze Mathematical Institute of the Georgian Academy of Sciences, M. Alexidze st. 1, Tbilisi 380093, Republic of Georgia
e-mail: alela@imath.acnet.ge; jib@imath.acnet.ge

Communicated by Prof. T.A. Springer at the meeting of January 27, 1997

ABSTRACT

A formula is obtained for the dimension $a(n, m)$ of the space of degree m invariants of the regular representation of the n-th order cyclic group. This formula implies in particular that $a(n, m) = a(m, n)$. Moreover, the automorphism group of the multiplicative semigroup generated by invariant monomials of the cyclic group in that representation is determined.

INTRODUCTION

The classical Hermite Reciprocity Law asserts the isomorphism

$$S^m S^n(k^2) \cong S^n S^m(k^2)$$

of symmetric powers of representations of the Lie group $SL_2(k)$ acting standardly on k^2, for a characteristic zero field k (see [4], Remark 12 by V.L. Popov in Appendix 3 of the Russian translation). In particular, the space of degree m polynomial invariants of the irreducible $(n+1)$-dimensional representation is equidimensional with the space of degree n invariants of the irreducible $(m+1)$-dimensional representation.

In [1], one can find certain generalization of this fact, formulated for representations of cyclic groups. We will consider another variation of it, which

*Partially supported by the ISF grant MQZ300.
**Supported by the INTAS grant #93-2618 and the ISF grant MXH200.

also can be called Hermite reciprocity for cyclic groups; however the precise relationship with the original Hermite reciprocity, although clearly apparent, is unknown to us.

In this paper, we will obtain an explicit formula for the dimension $a(n, m)$ of the space of degree m homogeneous polynomial invariants of the regular representation of the n-th order cyclic group. This formula implies that $a(n, m) = a(m, n)$.

Let us also note that in connection with applications of invariant theory to the study of the Steenrod algebra, algebras of invariants of another series of representations of cyclic groups (not regular ones) have been considered in [2], [3].

The authors are grateful to V.L. Popov – correspondence with him has stimulated writing of the present paper in the first place; to G. Almkvist, for supplying us with a copy of [1] and other important related material; and to D. Wehlau, who has sent his works related to ours, and has given valuable remarks on the preliminary version of the paper.

1.

For the cyclic group $C_n = \mathbf{Z}/n\mathbf{Z}$ of order n, let ρ be the following linear representation of that group in the vector space V_n over a field k, with $\dim_k V_n = n$: we will suppose that k has characteristic zero and contains a primitive root of unity of degree n. We will denote this root by ζ, and identify it with a generator of C_n. Moreover we fix a base $e_0, e_1, \ldots, e_{n-1}$ in V_n, and define the action in the representation by

$$\rho(\zeta)e_j = \zeta^j e_j.$$

It must be clear that ρ is isomorphic to the *regular representation* of the cyclic group $\mathbf{Z}/n\mathbf{Z}$. This representation can be extended to a representation in the algebra $P[V_n]$ of polynomial functions on V_n, which may be identified with the standard polynomial algebra $k[y_0, y_1, \ldots, y_{n-1}]$. Consider the algebra of invariants of this representation, $P[V_n]^{C_n} \subset k[y_0, y_1, \ldots, y_{n-1}]$, which has a finite set of generators by Hilbert's theorem; these generators may be chosen to be homogeneous. In fact they may be chosen to be monomials, as ρ is diagonal. Now it is easy to check that a monomial $y_0^{\lambda_0} y_1^{\lambda_1} \ldots y_{n-1}^{\lambda_{n-1}}$ is invariant under ρ iff the numbers $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ satisfy the congruence

$$(1) \qquad \sum_{j=0}^{n-1} j\lambda_j \equiv 0 \,(\mathrm{mod}\, n).$$

Let us call *degree* of a solution $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ of (1) the total degree of the corresponding invariant monomial $y_0^{\lambda_0} y_1^{\lambda_1} \ldots y_{n-1}^{\lambda_{n-1}}$, i.e. $\sum_{j=0}^{n-1} \lambda_j$.

Let $A(n, m)$ be the set of all nonnegative integer solutions of degree m of the congruence (1), and denote $a(n, m) = \# A(n, m)$ (here and in the sequel $\# S$ means the number of elements in a finite set S). In what follows, $\varphi(x)$ is the

Euler function, the greatest common divisor of integers n, m is denoted by (n, m) and $(k)_n$ denotes the residue of k modulo n.

Theorem 1. *("Hermite reciprocity"). The dimension $a(n, m)$ of the vector space of degree m homogeneous invariants of the regular representation of the cyclic group of order n is given by*

$$(2) \qquad a(n, m) = \frac{1}{n+m} \sum_{d \mid (n,m)} \varphi(d) \binom{n/d + m/d}{n/d};$$

in particular,

$$a(n, m) = a(m, n).$$

Proof. We will make use of a formula by T. Molien: if one denotes by $a(G, m)$ the dimension of the space of degree m invariants for a finite group $G \subseteq \mathrm{GL}(V)$ of linear transformations of a vector space V, there is an equality of formal power series:

$$\sum_{m=0}^{\infty} a(G, m) t^m = \frac{1}{\# G} \sum_{\gamma \in G} \frac{1}{\det(1 - t\gamma)}$$

(see e.g. [4]). If $G \subseteq \mathrm{GL}(V)$ realizes the regular representation of G, then this formula can be simplified as follows (see [1]):

$$\sum_{m=0}^{\infty} a(G, m) t^m = \frac{1}{\# G} \sum_{d=1}^{\infty} \varphi_G(d)(1 - t^d)^{-\frac{\# G}{d}},$$

where $\varphi_G(d)$ is the number of elements of order d in G.

In our case, when $G = \rho(C_n)$, an element $\rho(\zeta^k) \in G$ has order d iff ζ^k is a primitive root of unity of degree d; so there are $\varphi(d)$ such elements. Taking this into account, one obtains

$$\sum_{m=0}^{\infty} a(n, m) t^m = \frac{1}{n} \sum_{d \mid n} \varphi(d)(1 - t^d)^{-\frac{n}{d}}.$$

Now substituting

$$(1 - t^d)^{-\frac{n}{d}} = \sum_{j=0}^{\infty} \binom{-\frac{n}{d}}{j} (-1)^j t^{dj} = \sum_{j=0}^{\infty} \binom{\frac{n}{d} + j - 1}{j} t^{dj},$$

one obtains

$$\sum_{m=0}^{\infty} a(n, m) t^m = \frac{1}{n} \sum_{d \mid n} \varphi(d) \sum_{j=0}^{\infty} \binom{\frac{n}{d} + j - 1}{j} t^{dj} =$$

$$\frac{1}{n} \sum_{j=0}^{\infty} \sum_{d \mid n} \varphi(d) \binom{\frac{n}{d} + j - 1}{j} t^{dj} = \frac{1}{n} \sum_{m=0}^{\infty} \left(\sum_{d \mid n, d \mid m} \varphi(d) \frac{(\frac{n}{d} + \frac{m}{d} - 1)!}{(\frac{n}{d} - 1)! \frac{m}{d}!} \right) t^m.$$

Hence

$$a(n, m) = \frac{1}{n} \sum_{d | n, d | m} \varphi(d) \frac{(\frac{n}{d} + \frac{m}{d} - 1)!}{(\frac{n}{d} - 1)! \frac{m}{d}!} = \frac{1}{n} \sum_{d | n, d | m} \varphi(d) \frac{\frac{d}{n+m} \cdot \frac{n+m}{d}!}{\frac{d}{n} \cdot \frac{n}{d}! \frac{m}{d}!}$$

$$= \frac{1}{n} \sum_{d | (n,m)} \varphi(d) \frac{n}{n+m} \frac{\frac{n+m}{d}!}{\frac{n}{d}! \frac{m}{d}!} = \frac{1}{n+m} \sum_{d | (n,m)} \varphi(d) \frac{\frac{n+m}{d}!}{\frac{n}{d}! \frac{m}{d}!}.$$

We have obtained

$$a(n, m) = \frac{1}{n+m} \sum_{d | (n,m)} \varphi(d) \frac{\frac{n+m}{d}!}{\frac{n}{d}! \frac{m}{d}!},$$

which is the equality claimed. □

Remark 1. It is clear that $a(n, m)$, being the number of solutions of the congruence (1), has also a combinatorial definition, in terms of partitions of multiples of n into no more than m parts, each less than n. Hence it would be desirable to have a combinatorial explanation of the above formula giving Hermite reciprocity. We are going to do this in a sequel to this paper (a joint work with D. Pataraia).

Remark 2. From (2) one easily derives the following equality of formal power series

$$\sum_{n,m=0}^{\infty} a(n, m) x^n y^m = - \sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \log(1 - x^k - y^k).$$

Also, (2) can be written in terms of Dirichlet series: one has

$$\zeta(s+t+1) \sum_{n,m=1}^{\infty} a(n, m) n^{-s} m^{-t} = \zeta(s+t) \sum_{n,m=1}^{\infty} \frac{(n+m-1)!}{n!\, m!} n^{-s} m^{-t},$$

where $\zeta(x)$ is the Riemann zeta function.

2.

The set $A(n) = \cup_m A(n, m)$ of all nonnegative solutions of (1) carries a structure of a commutative monoid, i.e. semigroup, under componentwise addition, with the trivial solution as zero element.

Theorem 2. *For $n \neq 2$, the automorphism group of the monoid $A(n)$ is isomorphic to $\mathbf{Z}/n\mathbf{Z}^*$ – the automorphism group of $\mathbf{Z}/n\mathbf{Z}$.*

Proof. The theorem being trivially true for $n < 2$, let us concentrate on the case $n > 2$. In this proof, we will represent $A(n)$ by a submonoid of a free abelian group with generators e_i, $0 \leq i < n$, by identifying $(\lambda_0, \lambda_1, \dots \lambda_{n-1}) \in A(n)$ with $\lambda_0 e_0 + \lambda_1 e_1 + \dots + \lambda_{n-1} e_{n-1}$.

Call an element X of a monoid *extremal* if for any X', X'' in the monoid such that $X' + X''$ is a multiple of X, it follows that both X' and X'' are also multiples of X. Obviously any monoid automorphism carries extremal elements to extremal ones. On the other hand, it is clear that any extremal element of $A(n)$ has exactly one nonzero component, hence is one of the $X(i) = \frac{n}{(i,n)} e_i$, $0 \leq i < n$. Indeed, as soon as an element Y has at least two nonzero components – say i-th and j-th – one can find a natural N such that the i-th component of NY will exceed $\frac{n}{(i,n)}$. Then $NY - X(i)$ will belong to $A(n)$, i.e. $NY = X(i) + Z$ for some $Z \in A(n)$. But all positive multiples of Y have nonzero j-th component, hence $X(i)$ cannot coincide with any of them. It follows that Y is not extremal.

One obtains that any automorphism α of $A(n)$ permutes the extremal elements $X(i)$, i.e., $\alpha(X(i)) = X(\sigma_\alpha(i))$, for a certain permutation $\sigma_\alpha \in S_n$ from the symmetric group on $n = \{0, 1, \dots, n-1\}$.

Lemma. *For any automorphism α of $A(n)$, $n \neq 2$, let σ_α be the corresponding permutation as above. Then for any $0 \leq i < n$, $(\sigma_\alpha(i), n) = (i, n)$.*

Proof. As above, we only consider the case $n > 2$. Then for any $0 \leq i < n$ there exists $0 < j < n$ with $j \neq i$ and $(j, n) = 1$. Hence the congruence $i + jx \equiv 0 \pmod n$ has a solution, say, b. It follows that $Y = e_i + be_j$ is in $A(n)$. One checks that $(i, n)X(i) + bX(j) = nY$. Then also $(i, n)X(\sigma_\alpha(i)) + bX(\sigma_\alpha(j)) = n\alpha(Y)$, so that all components of the left hand side are divisible by n. But since $j \neq i$, also $\sigma_\alpha(j) \neq \sigma_\alpha(i)$, so the last equality implies $n \mid (i, n)\frac{n}{(\sigma_\alpha(i), n)}$, i.e. $(\sigma_\alpha(i), n) \mid (i, n)$. Now the same argument for α^{-1} in place of α gives $(i, n) \mid (\sigma_\alpha(i), n)$, which proves the lemma. □

Remark 3. For $n = 2$, $A(2)$, being a free commutative monoid with two generators e_0 and $2e_1$, has a unique nontrivial automorphism violating the lemma.

Now for any $0 \leq i, j < n$, there is a unique $0 \leq k < n$ with $X(i, j) = e_i + e_j + e_k \in A(n)$. This $X(i, j)$ satisfies

$$nX(i, j) = (i, n)X(i) + (j, n)X(j) + (k, n)X(k).$$

Applying our automorphism α one then obtains

$$n\alpha(X(i, j)) = (i, n)X(\sigma_\alpha(i)) + (j, n)X(\sigma_\alpha(j)) + (k, n)X(\sigma_\alpha(k)).$$

Using the lemma one has $\alpha(X(i, j)) = e_{\sigma_\alpha(i)} + e_{\sigma_\alpha(j)} + e_{\sigma_\alpha(k)}$. Since $\alpha(X(i, j))$ belongs to $A(n)$, this implies $\sigma_\alpha(i) + \sigma_\alpha(j) + \sigma_\alpha(k) \equiv 0 \pmod n$. We have obtained

$$i + j + k \equiv 0 \pmod n \Rightarrow \sigma_\alpha(i) + \sigma_\alpha(j) + \sigma_\alpha(k) \equiv 0 \pmod n,$$

which means that σ_α is an automorphism of $\mathbf{Z}/n\mathbf{Z}$.

Conversely it is very well known that any element of $(\mathbf{Z}/n\mathbf{Z})^*$ is multiplication by an invertible element of the ring $\mathbf{Z}/n\mathbf{Z}$, i.e. by a k with $(k, n) = 1$. And any such k gives rise to an obvious automorphism of $A(n)$ that carries an element X with components x_i to the one with components $x_{(ki)_n}$. □

Remark 4. The notion of extremal element has appeared in the literature under various names: see e.g. [5], 4.6. Its use in our proof has been inspired by the work of J. Gubeladze [6].

REFERENCES

1. Almkvist, G. and R. Fossum – Decomposition of exterior and symmetric powers of indecomposable $\mathbf{Z}/p\mathbf{Z}$-modules in characteristic p and relations to invariants. Séminaire P. Dubreil 1976–77. Lect. Notes in Math. **641**, Springer-Verlag, Berlin and New York (1978).
2. Campbell, H.E.A., J.C. Harris and D.L. Wehlau – On rings of invariants of non-modular abelian groups. Preprint, July 1994.
3. Campbell, H.E.A. and P.S. Selick – Polynomial algebras over the Steenrod algebra. Comment. Math. Helv. **65**, 171–180 (1990).
4. Springer, T.A. – Invariant theory. Lecture Notes in Math. **585**, Springer-Verlag, Berlin and New York (1977).
5. Stanley, R. – Enumerative combinatorics. Vol. I, Wadsworth & Brooks/Cole, Monterey, California (1986).
6. Swan, R.G. – Gubeladze's proof of Anderson's conjecture. In: "Azumaya algebras, actions and modules (Bloomington, In., 1990)", Contemp. Math. **125**, 215–250 (1992).

Received November 1996.