Pub. Mat. UAB
Vol. 30 Nº 1 Maig 1986

ON THE POINCARE SERIES OF $H^*(GL(2,2^n),Z/2)$

G.R. Chapman

INTRODUCTION. Let G be a finite group, and A a Noetherian G-ring. Then Evens [3], Venkov [11] show that $H^*(G,A)$, the cohomology ring of G with coefficients in A, is finitely generated. The proofs are essentially non-constructive, and give little information concerning the degrees in which the ring generators occur; a question first raised by Johnson [6]. Explicit descriptions of product structures of cohomology rings are not easy to obtain, a major difficulty being to determine when a set of generators is complete. In this paper, we exhibit a circumstance in which this difficulty may be overcome, and given an example.

Let p be a prime, and let $G_p, [H^*(G,A)]_p$ denote a Sylow p-subgroup of G, $H^*(G,A)$ respectively. Swan [10] shows that when G_p is abelian, then $[H^*(G,A)]_p$ consists of the subring of $H^*(G_p,A)$ fixed under the action induced by inner automorphisms of G. Consider the case when

$p=2$, G_2 is elementary abelian, and A is $Z/2$, the integers mod 2 with trivial G-action. Then $H^*(G_2,Z/2)$ is isomorphic to $R=(Z/2)[x_1,\ldots,x_r]$, a polynomial ring in r indeterminates where r is the rank of G_2 [7]. Consequently $H^*(G,Z/2)$ may be calculated as a ring of invariants R^H, where H is a group whose order is odd, and hence coprime to the characteristic of the base field of R.

In expository articles, Sloane [8] and Stanley [9] discuss classical invariant theory, in which the base field is the complex numbers. A canonical form is given for the ring of invariants, from which a complete set of generators and relations may be derived. In section 2 we indicate how, with minor modification, these results apply to the situation described above.

In section 3 we apply these results to $G=GL(2,2^n)$, and obtain an expression for the Poincaré Series of $H^*(GL(2,2^n),Z/2)$. The additive structure of $H^*(GL(2,2^n),Z/2)$ has been described by Aguadé [1], but the knowledge of the Poincaré Series leads, via the canonical form for the ring of invariants, to a complete set of generators and relations. For $n=2$, the results are well known [12]. For higher values of n, the calculation becomes more complicated, and the results of a machine computations are presented for $n=3$.

I would like to thank P.J. Webb for a series of enlightening correspondences, and in particular for indicated how the Brauer lift could be used to prove the version of Molien's theorem given in theorem 1.

2. MOLIEN'S THEOREM AND A BASIS OF INVARIANTS.

Let F be a field, H a finite group, V an F(H)-module with F-basis $\{x_1,\ldots,x_n\}$ and character χ. The polynomial ring $R = F[x_1,\ldots,x_n]$ is graded, with k-th component R_k having F-basis the set of monomials of degree k in $x_1,\ldots,x_n$ $(k\geq 0)$. Each $h \in H$ induces $\hat{h}:V \to V$ by $\hat{h}(v) = h.v$ $(v\in V)$, and for each $j\geq 0$ a map $\hat{h}_j:R_j \to R_j$ defined by

$$\hat{h}_j(x_1^{r_1}\ldots x_n^{r_n}) = \hat{h}(x_1)^{r_1}\ldots\hat{h}(x_n)^{r_n}, \quad (r_1+\ldots+r_n = j).$$

This makes R_j an F(H)-module, whose character we denote by χ_j. Denote by R^H the subring of R invariant under this action, and let $a_j = \dim_F(R_j^H)$.

In the classical theory, where F is taken to be the complex numbers (C) Molien's Theorem yields an explicit expression for $\Sigma\, a_j t^j$, the Poincaré Series of R^H. Moreover, R^H is a Cohen-Macauley ring which means the Poincaré Series may be written

$$\frac{\sum_{i=1}^{k} t^{u_i}}{\prod_{i=1}^{\ell}(1-t^{v_i})} .$$

Consequently, there exist free invariants $f_1,\ldots,f_\ell$ (deg $f_i = v_i$) and transient invariants $g_1,\ldots,g_k$ (deg $g_i = u_i$) such that

$$R^H = \coprod_{i=1}^{k} g_i C[f_1,\ldots,f_\ell] \quad .$$

and $f_1,\ldots,f_\ell$ are algebraically independent over C. The results sketched here are discussed more fully in [8], [9].

Now suppose that char(F)$\nmid$ H. The fact that R^H is Cohen-Macauley follows directly from [5] Propn 13 p1033, so that as in the complex case

$$R^H = \coprod_{i=1}^{k} g_i F[f_1,\ldots,f_\ell].$$

Molien's theorem may be modified by first assuming that F contains $|H|$-th roots of unity. This may be achieved by tensoring up to a suitable field if necessary, but does not effect what follows. For $h \in H$, let $B(h)$, $B(h_k)$ denote a Brauer lift of $\hat{h}$, $\hat{h}_k$ respectively, and $B(\chi)$, $B(\chi_k)$ the Brauer characters of V, R_k respectively. We have the following version of Molien's theorem.

<u>Theorem 1</u> If char $(F) \nmid |H|$, then

$$\sum_{j=0}^{\infty} a_j t^j = \frac{1}{|H|} \sum_{h \in H} \frac{\det(B(h))}{c(B(h))},$$

where $c(B(h))$ is the characteristic polynomial of $B(h)$ in the indeterminate t.

<u>PROOF</u> Let $\eta_1, \ldots, \eta_n \in C$ denote the eigenvalues of $B(h)$.

Then

$$[\det(I - B(h)t)]^{-1} = \prod_{i=1}^{n} (1-\eta_i t)^{-1}$$

$$= \sum_{j=0}^{\infty} X_j t^j , \qquad (1)$$

where $X_j = \sum_{r_1 + \ldots + r_n = j} \eta_1^{r_1} \ldots \eta_n^{r_n}$.

But $\{\eta_1^{r_1} \ldots \eta_n^{r_n} ;\ r_1 + \ldots + r_n = j\}$ is a set of eigenvalues for $B(h_k)$, so that $X_j = B(\chi_k)(h)$. (2)

Since $\mathrm{char}(F) \nmid H$, the orthogonality relations for Brauer characters [2] § 18C are similar to those for ordinary characters. In particular, it follows that

$$a_j = \frac{1}{|H|} \sum_{h \in H} B(\chi_j)(h). \qquad (3)$$

Hence by (1), (2) and (3),

$$\sum_{j=0}^{\infty} a_j t^j = \frac{1}{|H|} \sum_{h\in H} \frac{1}{\det(I-B(h)t)} ,$$

and the theorem follows.

3. THE POINCARE SERIES OF $H^*(GL(2,2^n), Z/2)$.

For $n\geq 1$, let $GF(2^n)$ denote the field of 2^n elements, and G be $GL(2,2^n)$, the group of 2×2 matrices with entries in $GF(2^n)$. A Sylow 2-subgroup G_2 of G consists of the matrices

$$\{\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix};\ \beta\in GF(2^n)\}$$

and is isomorphic to the direct product of n copies of C_2, the cyclic group of order 2. If

$$H = \{\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix};\ \ \alpha\in GF(2^n)\backslash\{0\}\},$$

then H is cyclic of order 2^n-1, and if N, C denote the normalizer of G_2 in G, and centralizer of G_2 in G respectively, we have the extension

$$1 \to C \to N \to H \to 1.$$

Here H acts on G_2 by

$$\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix}\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha^{-1} & 0\\ 0 & \alpha\end{pmatrix} = \begin{pmatrix}1 & \alpha^2\beta\\ 0 & 1\end{pmatrix} ,$$

and since $\mathrm{Aut}(G_2) = GL(n,2)$, we have a monomorphism $\emptyset: H \to GL(n,2)$. This is discussed more fully in [4].

Let $P_n(t) = \sum_{j=0}^{n} c_{j+1}t^j$ be a primitive, irreducible, degree n polynomial over $GF(2)$, and let μ be a root of $P_n(t)$. Then H is generated by $\begin{pmatrix}\delta & 0\\ 0 & \delta^{-1}\end{pmatrix}$ where $\delta = \mu^{2^{n-1}}$. Further, as a vector space over F_2, G_2 has basis

$$\{ \begin{pmatrix} 1 & \mu^i \\ 0 & 1 \end{pmatrix} ; 0 \leq i \leq n-1 \} .$$

Since

$$\begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix} \begin{pmatrix} 1 & \mu^i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \delta^{-1} & 0 \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} 1 & \mu^{i+1} \\ 0 & 1 \end{pmatrix} \quad (0 \leq i \leq n-1),$$

it follows that $\emptyset \begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix}$ is the companion matrix M of $P_n(t)$, and that $\emptyset(H) = M$, the group generated by M.

Turning to cohomology we note that $H^1(G_2, Z/2) \cong \mathrm{Hom}\,(G_2, Z/2)$. For $1 \leq i \leq n$, let x_i be the element of $H^2(G_2, Z/2)$ which corresponds under this isomorphism to the homomorphism which maps $\begin{pmatrix} 1 & \mu^j \\ 0 & 1 \end{pmatrix}$ to 1 if $j = i-1$ and 0 otherwise. It is well known (see e.g. [7]) that $H^*(G_2, Z/2)$ is the polynomial ring $R = GF(2)[x_1, \ldots, x_n]$. It follows from the definition of x_i that M induces a transformation

$$x_i \to x_{i+1} \quad (1 \leq i \leq n-1),$$

$$x_n \to \sum_{j=1}^{n} c_j x_j ,$$

so that, identifying H with its image under $\emptyset$, we may calculate $H^*(G, Z/2)$ as the ring of invariants R^H.

By theorem 1, the Poincaré series is

$$\frac{1}{2^n-1} \sum_{i=0}^{2^n-2} \frac{\det B(M^i)}{c\ B(M^i)} , \tag{4}$$

where B denotes the Brauer lift, and c the characteristic polynomial. To simplify this expression, we first note that if Q is a polynomial over $GF(2)$, then $Q(y^2) = [Q(y)]^2$. Hence if $Q(t)$ is irreducible of degree d, the roots of $Q(t)$ are of the form $\{y, y^2, \ldots, y^{2^{d-1}}\}$. Since the characteristic polynomial of M is

$P_n(t)$, it follows that M is similar to diag $(\mu,\mu^2,\dots,\mu^{2^{n-1}})$, and that M^i is similar to diag $(\mu^i,\mu^{i2},\dots,\mu^{i2^{n-1}})$.

To simplify (4), consider the action of Z/n (the integers mod. n) on $X_n = \{0,1,\dots,2^n-2\}$ given by

$\hat{z}(i)$ = residue of $2^z i$ mod. 2^n-1 $(z\in Z/n,\ i\in X_n)$.

If $\mathrm{Orb}(i)$ denotes the orbit of i and $|\mathrm{Orb}(i)| = d_i$, then d_i is the exponent of 2 mod. $e(i)$, where

$$e(i) = \frac{2^n-1}{(2^n-1,i)}$$

is the exponent of μ^i in $GF(2^n)$. Moreover, μ^i is a root of an irreducible polynomial of degree d_i over $GF(2)$. For each $d|n$, let O_d denote a set of representatives for the orbits of size d.

If η is a primitive complex (2^n-1)th root of unity corresponding to μ under the Brauer lift, we have

$$\det B(M^i) = \prod_{j=0}^{n-1} \eta^{i2^j} = 1 \quad ,$$

$$cB(M^i) = \prod_{j=0}^{n-1} (\eta^{i2^j}-t) = \prod_{j=0}^{d_i-1} (\eta^{i2^j}-t)^{n/d_i} \quad (0\leq i\leq 2^n-2) .$$

Thus from (4) we obtain

<u>Theorem</u> <u>2</u>. The Poincaré Series of $H^*(GL(2,2^n),Z/2)$ is

$$\frac{1}{2^n-1} \sum_{d|n} \Big(\sum_{i\in O_d} \frac{d}{\prod_{j=0}^{d-1}(\eta^{2^j i}-t)^{n/d}}\Big) ,$$

where η and O_d are defined above.

We exhibit the Poincaré Series for some low values of n. An explicit expression seems hard to obtain for arbitrary n.

(i) If $n = 2$, the orbits of X_2 are $\{0\}$, $\{1,2\}$ and theorem 2 gives

$$\frac{1}{3}\left[\frac{1}{(1-t)^2} + \frac{2}{(\eta-t)(\eta^2-t)}\right] \quad (\eta^3=1)$$

as the Poincaré Series. This simplifies to

$$\frac{1-t+t^2}{(1-t)(1-t^3)}$$

as is well known (see e.g. [12]).

(ii) If $n = 3$, the orbits of X_3 are $\{0\}$, $\{1,2,4\}$, $\{3,5,6\}$ so we obtain

$$\frac{1}{7}\left[\frac{1}{(1-t)^3} + \frac{3}{(\eta-t)(\eta^2-t)(\eta^4-t)} + \frac{3}{(\eta^3-t)(\eta^5-t)(\eta^6-t)}\right] \quad (\eta^7=1)$$

which can be written

$$\frac{1-2t+t^2+t^3+t^4-2t^5+t^6}{(1-t)^2(1-t^7)} .$$

(iii) For $n = 4$, the orbits of X_4 are $\{0\}$ $\{5,10\}$, $\{1,2,4,8\}$, $\{3,6,9,12\}$ and $\{7,11,13,14\}$. A lengthy calculation shows the Poincaré Series is

$$\frac{1-2t+t^2-t^3+3t^4+t^5-t^6-t^7+t^8-t^9-t^{10}+t^{11}+3t^{12}-t^{13}+t^{14}-2t^{15}+t^{16}}{(1-t)^2(1-t^3)(1-t^{15})} .$$

4. The Cohomology Rings for $n = 2,3$.

As observed in section 2, the Poincaré Series (as given by theorem 2) may be written in the form

$$\frac{\sum_{i=1}^{k} t^{u_i}}{\prod_{i=1}^{\ell}(1-t^{v_i})}$$

though not necessarily uniquely. However, if free invariants can be found in degrees $v_1,\dots,v_\ell$, and transient invariants in degrees $v_1,\dots,v_k$ then we may conclude that these generate the entire ring.

(i) When $n = 2$, (6) may be written

$$\frac{1 + t^3}{(1-t^2)(1-t^3)} .$$

Write x,y instead of x_1,x_2. Since

$$A = x^2 + xy + y^2 , \quad B = xy(x+y)$$

and $C = x^3 + x^2y + y^3$ are invariants with

$$C^2 = A^3 + B^2 + C.B,$$

it follows that these three elements generate $H^*(GL(2,2^2),Z/2)$ as a commutative ring of exponent 2 subject to the single relation given.

(ii) For $n = 3$, the Poincaré Series may be written

$$\frac{1 + 2t^4 + 3t^5 + 3t^6 + 2t^7 + t^{11}}{(1-t^3)(1-t^4)(1-t^7)}$$

Write x,y,z for x_1,x_2,x_3. Searching in the ring of invariants, we find ring generators.

$$A = x^3 + y^3 + z^3 + xz^2 + y^2z + xy^2 + xyz$$

$$B_1 = x^4 + y^4 + z^4 + x^2y^2 + y^2z^2 + z^2x^2 + xyz(x+y+z),$$

$$B_2 = x^3(y+z) + xyz(y+z) + z^3(x+y) + x^2y^2 + y^3z ,$$

$$B_3 = x^3y + x^2z^2 + xy^3 + xz^3 + y^3z + y^2z^2 ,$$

$$C_1 = x^5 + y^5 + z^5 + xyz(xy+yz+zx) + xy^4 + xz^4 + y^4z ,$$

$$C_2 = xy^4 + yz^4 + zx^4 + x^2y^3 + y^2z^3 + z^2x^3 + x^2yz(y+z) ,$$

$$C_3 = x^4y + y^4z + z^4x + x^3y^2 + y^3z^2 + z^3x^2 + xy^3(x+y) ,$$

$$D_1 = x^4y^2 + y^4z^2 + z^4x^2 + x^2y^4 + y^2z^4 + z^2x^4 + xyz(x^3+y^3+z^3) + x^2y^2z^2,$$

$$D_2 = x^5y + y^5z + z^5x + x^2y^4 + y^2z^4 + z^2x^4 + xy^2(x^3+y^3),$$

$$D_3 = x^5y + y^5z + z^5x + x^2y^2z^2 + x^5z + x^4y^2 + x^4yz + yz^5,$$

$$E_1 = xyz(x^3y + y^3z + z^3x + xy^3 + yz^3 + zx^3) ,$$

$$E_2 = x^6y + y^6z + z^6x + x^5y^2 + y^5z^2 + z^5x^2 + x^5y(x+y)$$

$$E_3 = x^6y + y^6z + z^6x + x^3y^4 + y^3z^4 + z^3x^4 + xy^3(x^3+y^3).$$

We claim that A, B_1, E_1, may be taken as free invariants, with transient invariants, B_2, B_3 in degree 4, C_1, C_2, C_3 in degree 5, D_1, D_2, D_3 in degree 6, E_2, E_3 in degree 7 and C_1D_1 in degree 11. To establish this claim we have to show that the product of any two transient invariants, and the square of each transient invariant lies in

$$S \amalg (\amalg g_i S)$$

where S is the ring generated by A, B_1, E_1, and g_i runs over the set of transient invariants. Any such relation which involves the transient C_1D_1 may be obtained from the other relations. Hence we need only consider the remaining 10 transients, which means there are 55 relations to be established. These relations have been obtained, but are not presented here, due to their quantity and complexity.

REFERENCES

[1] J. Aguadé, The cohomology of the GL_2 of a finite field, Arch Math. (Basel) 34 (1980), no. 6. 509-516.

[2] C.W. Curtis and I. Reiner, Methods of Representation Theory, Vol 1, John Wiley and Sons, New York, 1981.

[3] L. Evens, The cohomology ring of a finite group, Trans. Amer. Math.Soc. 101 (1961), 224-239. MR 25, 1191.

[4] D. Gorenstein, Finite Groups, Harper and Row, New York, Evanston and London, 1968.

[5] M. Hochster and J.A. Eagon, Cohen-Macauley rings, invariant theory, and the generic perfection of determinantal loci, Amer. J. Math. 93 (1971), 1020-1058.

[6] D.L. Johnson, On the cohomology of finite 2-groups, Inventiones Math. 7, (1969), 159-173.

[7] D. Quillen, The spectrum of an equivariant cohomology ring I, Ann. of Math. (2), 94 (1971), 549-572.

[8] N.J.A. Sloane, Error-correcting codes and invariant theory: New applications of a nineteenth century technique, Amer. Math. Monthly 84 (1977), 82-107.

[9] R.P. Stanley, Invariants of finite groups and their applications to combinatorics, Bull. A.M.S. vol 1, No 3 (1979), 475-511.

[10] R.G. Swan, The p-period of a finite group, Ill. J. Math. 4 (1960), 341-346.

[11] B.B. Venkov, Cohomology algebras for some classifying spaces, Kokl. Akad. Nauk. SSSR,, vol 127 (1959), 943-944.

[12] P.J. Webb, A local method in group cohomology, To appear.

Rebut el 3 de maig del 1985

Blaisdell House 143 E.
Tenth Street
Claremont,
California 91711
U.S.A.