Pub. Mat. UAB
Vol. 28 Nº 1 Maig 1984

A CLASS OF INVARIANT POLYNOMIALS AND AN APPLICATION IN GROUP COHOMOLOGY

G.R. Chapman

INTRODUCTION. This paper arises as part of a study of the mod 2 cohomology ring of a finite simple group G with abelian Sylow 2-subgroup G_2. In such a case, a result of Swan ([5]) lemma 1) applies, and $H^*(G,Z/2)$ consists of those elements of $H^*(G_2, Z/2)$ which are fixed under the action induced by inner automorphisms of G. Moreover, G_2 is in fact elementary abelian (see e.g. [3] p.480), so that $H^*(G_2,Z/2)$ is polynomial over GF(2), the number of indeterminates being the rank of G_2 ([4] p.558). Hence $H^*(G,Z/2)$ may be calculated as a ring of invariants in the classical sense. The results of such a calculation, with G taken to be Janko's first group, appear in [2].

The preceeding applies when G is $PSL(2,2^n)$, the projective special linear group of 2 by 2 matrices over $GF(2^n)$, the field of

2^n elements. In this case, one is led to consider the action of the multiplicative group of $GF(2^n)$ on the additive.This action has been considered recently (for arbitrary primes) by J. Aguade, and in [1] he gives a formula for the dimension of the vector space of homogeneous invariants of each degree, in terms of the number of sequences of integers which satisfy certain conditions.However, no invariant polynomials are exhibited, and the question of the multiplicative structure of the ring of invariants, which seems more difficult, remains open.

In this paper, we let $R=GF(2)[x_1,\ldots,x_n]$, and construct a class of polynomials in R which are invariant under the action of <u>any</u> degree n polynomial $s_n(t)$ in $GF(2)[t]$ which has non-zero constant term. The special case when $s_n(t)$ is irreducible and primitive then yields the situation described in the previous paragraph. The polynomials we construct are described in §2, and their invariance established in §3.

At the end of the paper, in §4, we indicate how these polynomials give rise to cohomology classes in $H^*(PSL(2,2^n),Z/2)$, and which of them in fact lie in $H^*(PSL(2,2^n),Z)$.

§2. CONSTRUCTION OF THE POLYNOMIALS.

Suppose $\underline{d} = (d_1,\ldots,d_n)$ is an n-tuple of non-negative integers. The symmetric group , S_n, acts by permuting the coordinates, and we suppose this action to be on the left. Thus for $\rho \in S_n$,

$$\rho\underline{d}=(d_{\rho^{-1}(1)},\ldots,d_{\rho^{-1}(n)}).$$

Denote by $S(\underline{d})$ the stabilizer of $\underline{d}$ under this action, and let $X(\underline{d})$ be a set of representatives for the left cosets of $S(\underline{d})$ in S_n. Given n independent variables $x_1,\ldots x_n$, we define

$$\mathrm{mon}(\underline{d})=x_1^{d_1}\ldots x_n^{d_n},$$

$$\mathrm{pol}(\underline{d})=\sum_{\rho\in X(\underline{d})}\mathrm{mon}(\rho\underline{d}),$$

where the last expression is considered as an element of R. This polynomial isindependent of the choice of representatives in $X(\underline{d})$, and is symmetric in $x_1,\ldots,x_n$.

If $\underline{d}$ has k non-zero entries ($k<n$), we wish to obtain from it a family of n-tuples, called the descendents of $\underline{d}$, each of which has k+1 non-zero entries. We say that the n-tuple $\underline{f}$ is a descendent of $\underline{d}$ (and $\underline{d}$ is an anticedent of $\underline{f}$) if $\underline{f}$ may be obtained from $\underline{d}$ by replacing two entries 2q, 0 by q,q (q a positive integer). Two descendents (and likewise two anticedents) are identified if they are equal up to order. Then, the number of distinct descendents of $\underline{d}$ is equal to the number of distinct,non-zero, even integers which occur in the entries of $\underline{d}$, while the number of distinct anticedents of $\underline{f}$ is equal to the number of integers which appear more than once in the entries of $\underline{f}$.

Let $\underline{e}=(e_1,\ldots,e_n)$ be an n-tuple of non-negative integers, let p be the number of non-zero entries in $\underline{e}$, and suppose $\underline{e}$ satisfies the following condition.

(a) The non-zero entries of $\underline{e}$ are distinct, and each is of the form 2^q ($q>n-p$).

Put $T(\underline{e},p) = \{\underline{e}\}$, and for $p+1<k<n$ let $T(\underline{e},k)$ be the set of descendents of elements of $T(\underline{e},k-1)$, again with the understanding that two n-tuples in $T(\underline{e},k)$ are identified if they are equal up to order. It is easy to see that $T(\underline{e},k-1)$ is the set of anticedents of elements of $T(\underline{e},k)$. Finally, let

$$\alpha(\underline{e}) = \sum_{k=p}^{n} \sum_{\underline{d}\in T(\underline{e},k)} pol(\underline{d}).$$

EXAMPLE. Let $n = 3$, $\underline{e} = (4,2,0)$. Then $p = 2$,

$T(\underline{e},2) = \{(4,2,0)\}$, $T(\underline{e},3) = \{(2,2,2),(4,1,1)\}$,

$pol(4,2,0) = x_1^4x_2^2 + x_2^4x_3^2 + x_3^4x_1^2 + x_1^4x_3^2 + x_2^4x_1^2 + x_3^4x_2^2$,

$pol(2,2,2) = x_1^2x_2^2x_3^2$,

$pol(4,1,1) = x_1^4x_2x_3 + x_2^4x_3x_1 + x_3^4x_1x_2$,

and $\alpha(4,2,0)$ is the sum of these three polynomials.

§ 3. PROOF THAT $\alpha(\underline{e})$ IS INVARIANT.

Let the n-tuple $\underline{e}$ satisfy condition (a). We will show that $\alpha(\underline{e})$ is invariant under the companion matrix of any degree n polynomial

$$s_n(t) = \sum_{j=0}^{n} \lambda_{j+1} t^j \in GF(2)[t] ,$$

provided $\lambda_1 = 1$.

Denote by F the transformation of R induced by

$$x_i \to x_{i+1} \quad (1<i<n-1) ,$$
$$x_n \to x_1 + \sum_{j=2}^{n} \lambda_j x_j .$$

Concerning the last expression, we have the following lemma, which we state without proof.

LEMMA 1 If θ is a power of 2, then as elements of R,

$$(x_1 + \sum_{j=2}^{n} \lambda_j x_j)^{\theta} = x_1^{\theta} + \sum_{j=2}^{n} \lambda_j x_j^{\theta} .$$

In order to show that $\alpha(\underline{e})$ is invariant under F, we make the following definitions. For an n-tuple $\underline{d}$, let

$$E(\underline{d}) = F(pol(\underline{d})) - pol(\underline{d}),$$

and for $p<k<n$ let

$$E(\underline{e},k) = \sum_{\underline{d} \in T(\underline{e},k)} E(\underline{d}) ,$$

$$AE(\underline{e},k) = \sum_{\ell=p}^{k} E(\underline{e},\ell) ,$$

where p is the number of non-zero entries in $\underline{e}$. It follows from these definitions that $\alpha(\underline{e})$ is invariant under F if and only if $AE(\underline{e},n) = 0$.

To calculate $AE(\underline{e},n)$, we must first consider $E(\underline{d})$, for $\underline{d} \in T(\underline{e},k)$ $(p<k<n)$.

PROPOSITION 1. Suppose $\underline{e}$ satisfies condition(a), and $\underline{d} \in T(\underline{e},k)$ $(p<k<n)$.

Let

$$X_1(\underline{d}) = \{\rho \in X(\underline{d});\ d_{\rho^{-1}(n)} = d_{\rho^{-1}(j-1)} \neq 0\},$$

$$X_2(\underline{d}) = \{\rho \in X(\underline{d});\ d_{\rho^{-1}(n)} \neq 0,\ d_{\rho^{-1}(j-1)} = 0\}.$$

Denote

$$\Sigma\ x_j^{d_{\rho^{-1}(n)}} x_2^{d_{\rho^{-1}(1)}} \cdots x_n^{d_{\rho^{-1}(n-1)}}$$

by $P_1(\underline{d})$ if the sum is over $X_1(\underline{d})$ and by $P_2(\underline{d})$ if it is over $X_2(\underline{d})$.

Then the coefficient of λ_j in $E(\underline{d})$ is $P_1(\underline{d}) + P_2(\underline{d})$ $(2 \leq j \leq n)$.

PROOF. For $\rho \in X(\underline{d})$, we have

$$F(\text{mon}(\rho\underline{d})) = x_2^{d_{\rho^{-1}}(1)} \cdots x_n^{d_{\rho^{-1}}(n-1)} \left(x_1 + \sum_{j=2}^{n} \lambda_j x_j\right)^{d_{\rho^{-1}}(n)}.$$

If $d_{\rho^{-1}(n)} = 0$, then the result is a monomial which appears in $\text{pol}(\underline{d})$.

Note that x_1 appears with power zero in this monomial, and distinct choices of $\rho \in X(\underline{d})$ with $d_{\rho^{-1}(n)} = 0$ yield distinct monomials.

If $d_{\rho^{-1}(n)} \neq 0$, it must be a power of 2 (this is because $\underline{e}$ satisfie (a)). Thus Lemma 1 applies, and $F(\text{mon}(\rho\underline{d}))$ may be written

$$x_1^{d_{\rho^{-1}}(n)} x_2^{d_{\rho^{-1}}(1)} \cdots x_n^{d_{\rho^{-1}}(n-1)} + \sum_{j=2}^{n} \lambda_j x_j^{d_{\rho^{-1}}(n)} x_2^{d_{\rho^{-1}}(1)} \cdots x_n^{d_{\rho^{-1}}(n-1)}.$$

The first term is a monomial which appears in $\text{pol}(\underline{d})$ and in which x_1 appears with non-zero power. Distinct $\rho \in X(\underline{d})$ with $d_{\rho^{-1}(n)} \neq 0$ yield distinct such monomials, and these monomials are distinct from those discussed in the previous paragraph. Thus, as ρ takes all values in $X(\underline{d})$, the sum of the monomials considered up to now is $\text{pol}(\underline{d})$. This means that

$$E(\underline{d}) = F(\text{pol}(\underline{d})) - \text{pol}(\underline{d})$$

$$= \Sigma \left(\sum_{j=2}^{n} \lambda_j x_j^{d_{\rho^{-1}(n)}} x_2^{d_{\rho^{-1}(1)}} \cdots x_n^{d_{\rho^{-1}(n-1)}} \right),$$

where the sum is over all $\rho \in X(\underline{d})$ with $d_{\rho^{-1}(n)} \neq 0$. For $2 \leq j \leq n$, the coefficient of λ_j is

$$\Sigma\, x_j^{d_{\rho^{-1}(n)}} x_2^{d_{\rho^{-1}(1)}} \cdots x_n^{d_{\rho^{-1}(n-1)}} \qquad (1),$$

where the sum is again over all $\rho \in X(\underline{d})$, $d_{\rho^{-1}(n)} \neq 0$. This index set may be written as the union of the disjoint subsets $X_2(\underline{d})$ and

$$Y(\underline{d}) = \{\rho \in X(\underline{d});\ d_{\rho^{-1}(n)} \neq 0,\ d_{\rho^{-1}(j-1)} \neq 0\}.$$

Thus the proposition will be proved if we can show that the expression (1), when summed over $Y(\underline{d})$ yields $P_1(\underline{d})$.

Let $\tau \in S_n$ denote the transposition $(j-1,n)$. Define $h: S_n \to S_n$ by $h(\sigma) = \tau\sigma$. Clearly h^2 is the identity map, h induces a map $\bar{h}: Y(\underline{d}) \to Y(\underline{d})$ and for $\rho \in Y(\underline{d})$ the term in (1) corresponding to $\bar{h}(\rho)$ equals the term corresponding to ρ. Thus, modulo 2 they cancel. Now $\bar{h}(\rho) = \rho$ if and only if $\rho^{-1}\tau\rho$ $S(\underline{d})$. But $\rho^{-1}\tau\rho$ is the transposition $(\rho^{-1}(j-1), \rho^{-1}(n))$, and so $\bar{h}(\rho) = \rho$ precisely when $d_{\rho^{-1}(j-1)} = d_{\rho^{-1}(n)}$. Thus the expression (1), when summed over $Y(\underline{d})$ yields $P_1(\underline{d})$, and the proposition is proved.

Note that in each monomial of $P_1(\underline{d})$ precisely (k-1) distinct x's appear with non-zero coefficient, while for monomials in $P_2(\underline{d})$ precisely k x's appear with non-zero coefficient.

We can now calculate $AE(\underline{e},k)$.

PROPOSITION 2. Let $\underline{e}$ satisfy condition (a). Then, with $P_2(\underline{d})$ as defined in Proposition 1, the coefficient of λ_j in $AE(\underline{e},k)$ is

$$\sum_{\underline{d} \in T(\underline{e},k)} P_2(\underline{d}) \qquad (2 \leq j \leq n,\ p \leq k \leq n).$$

The invariance of $\alpha(\underline{e})$ now follows from

COROLLARY 1 If $\underline{e}$ satisfied condition (a), then $AE(\underline{e},n) = 0$.

PROOF. Note that if $\underline{d} \in T(\underline{e},n)$, then no entry in $\underline{d}$ is zero, and so $X_2(\underline{d})$ is empty. Thus $P_2(\underline{d}) = 0$, and by Proposition 2, the coefficient of λ_j in $AE(\underline{e},n)$ is zero for $2 \leq j \leq n$. Hence $AE(\underline{e},n) = 0$.

PROOF OF PROPOSITION 2. We proceed by induction on k. When k=p,

$$AE(\underline{e},p) = E(\underline{e},p) = E(\underline{e}).$$

Take $\underline{d} = \underline{e}$ in Proposition 1. Since $\underline{e}$ has no non-zero entry repeated (condition (a)), it follows that $X_1(\underline{e})$ is empty. Thus the coefficient of λ_j in $E(\underline{e})$ is $P_2(\underline{e})$, which establishes the proposition when k=p.

Assume that the coefficient of λ_j in $AE(\underline{e},k-1)$ is

$$\sum_{\underline{d} \in T(\underline{e},k-1)} P_2(\underline{d}), \quad (p+1 \leq k \leq n).$$

Now $$AE(\underline{e},k) = AE(\underline{e},k-1) + E(\underline{e},k),$$

and the coefficient of λ_j on the right hand side is

$$\sum_{\underline{d} \in T(\underline{e},k-1)} P_2(\underline{d}) + \sum_{\underline{d} \in T(\underline{e},k)} (P_1(\underline{d}) + P_2(\underline{d})) \qquad (2 \leq j \leq n).$$

The induction will be established if we can prove

LEMMA 2. $$\sum_{\underline{d} \in T(\underline{e},k-1)} P_2(\underline{d}) = \sum_{\underline{d} \in T(\underline{e},k)} P_1(\underline{d}) \qquad (p+1 \leq k \leq n).$$

PROOF. A typical monomial on the left hand side is of the form

$$x_j^{d_{\rho^{-1}(n)}} x_2^{d_{\rho^{-1}(1)}} \cdots x_n^{d_{\rho^{-1}(n-1)}},$$

where $\underline{d} \in T(\underline{e},k-1)$, $\rho \in X_2(\underline{d})$. Since $\underline{e}$ satisfies (a) and $\underline{d} \in T(\underline{e},k-1)$ with $k-1<n$, it follows that each non-zero entry in $\underline{d}$ is not only a power of 2, but also not equal to 1. Let $\underline{f} = (f_1,\ldots,f_n)$ be the descendent of $\underline{d}$ obtained by replacing $d_{\rho^{-1}(n)}$ and $d_{\rho^{-1}(j-1)}$ (which is 0) by two copies of $d_{\rho^{-1}(n)}/2$.

Then $\rho \in X_1(\underline{f})$, and the monomial

$$x_j^{f_{\rho^{-1}(n)}} x_2^{f_{\rho^{-1}(1)}} \cdots x_n^{f_{\rho^{-1}(n-1)}},$$

appears on the right hand side of the equation of the Lemma.

Conversely, given a monomial on the right hand side

$$x_j^{d_{\rho^{-1}(n)}} x_2^{d_{\rho^{-1}(1)}} \cdots x_n^{d_{\rho^{-1}(n-1)}},$$

where $\underline{d} \in T(\underline{e},k)$ and $\rho \in X_1(\underline{d})$, we may reverse the above process. Let $\underline{f} = (f_1,\ldots,f_n)$ be the anticedent of $\underline{d}$ obtained by replacing $d_{\rho^{-1}(n)}$ by $2d_{\rho^{-1}(n)}$, and $d_{\rho^{-1}(j-1)}$ by 0. Then $\underline{f} \in T(\underline{e},k-1)$, $\rho \in X_2(\underline{f})$ and the monomial

$$x_j^{f_{\rho^{-1}(n)}} x_2^{f_{\rho^{-1}(1)}} \cdots x_n^{f_{\rho^{-1}(n-1)}},$$

appears on the left hand side. Thus is established a one-one correspondence between the monomials appearing on the left and on the right, and so Lemma 2 is proved.

Proposition 1, and the invariance of $\alpha(\underline{e})$ now follow.

4. AN APPLICATION IN COHOMOLOGY.

Let $G = PSL(2,2^n)$. In this section, we indicate how the polynomials constructed in $\oint 2$ give rise to cohomology classes in $H^*(G,Z/2)$ and $H^*(G,Z)$. We remark that the following holds for choices of G other than $PSL(2,2^n)$, for example $GL(2,2^n)$.

The sylow 2-subgroup G_2 of G consists of the matrices

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

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

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

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

$$1 \to G_2 \to N \to H \to 1.$$

Here, H acts on G_2 by

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & a^2b \\ 0 & 1 \end{pmatrix}.$$

Since G_2 is self centralizing and $Aut(G_2) = GL(n,2)$, we have a monomorphism $\phi: H \to GL(n,2)$. The above is discussed more fully in [3].

Let $r_n(t) = \sum_{j=0}^{n} c_{j+1}\, t^j$ be a primitive, irreducible, degree n

polynomial over GF(2), and let ξ be a root of $r_n(t)$. Then H is generated by $\begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}$, where $\mu = \xi^{2^{n-1}}$. Further as a vector space over F_2, G_2 has basis

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

Since

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

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

Turning to cohomology we note that $H^1(G_2, Z/2) = \mathrm{Hom}(G_2, Z/2)$. For $1 \leq i \leq n$, let x_i be the element of $H^1(G_2, Z/2)$ which corresponds under this isomorphism to the homomorphism which maps $\begin{pmatrix} 1 & \xi^{-1} \\ 0 & 1 \end{pmatrix}$ to 1 if $j=i-1$, and to 0 otherwise. It is well known (see e.g.[4]) that $H^*(G_2, Z/2)$ is the polynomial ring $GF(2)[x_1, \ldots, x_n]$, which in this paper has been denoted by R.

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 we may calculate $H^*(G, Z/2)$ as the ring of invariants R^M.

For integer coefficients, since $2H^m(G_2,Z) = 0$ $(m>0)$ it follows that the homology sequence arising from

$$0 \to Z \xrightarrow{j} Z \to Z/2 \to 0$$

may be decomposed into short exact sequences.

$$0 \to [H^m(G,Z)]_2 \to H^m(G,Z/2) \to [H^{m+1}(G,Z)]_2 \to 0 \quad (m>1).$$

Thus $[H^*(G,Z)]_2$ may be obtained as either the kernel of or the image of the Bockstein homomorphism Δ. Now we have $\Delta(x_i) = x_i^2$, $\Delta(x_i^2) = 0$ $(1\leq i\leq n)$.

If $\underline{e}$ satisfies (a) and all non-zero entries in $\underline{e}$ are $> 2^{n-p}$, then each $\underline{d} \in T(\underline{e},k)$ $(p\leq k\leq n)$ has all entries even. This means that in the monomials in $\mathrm{pol}(\underline{d})$, all x's appear with even power. Since $\Delta(x_i^2) = 0$, it follows that $\Delta(\mathrm{pol}(\underline{d}))$, and hence $\Delta(\alpha(\underline{e})) = 0$. An analysis of the situation when the n-tuple $\underline{e}$ satisfies condition (a) and has an entry equal to 2^{n-p} yields the following.

PROPOSITION 3. If $\underline{e}$ satisfies (a), then $\Delta(\alpha(\underline{e})) = 0$ (and so $\alpha(\underline{e}) \in H^*(G,Z)$) except in the following cases.

(i) If $\underline{e} = (2^{q_1},\ldots,2^{q_{n-1}},1)$ with $q_i > 1$ $(1\leq i\leq n-1)$, then

$$\Delta(\alpha(\underline{e})) = \alpha(2^{q_1}, \ldots ,2^{q_{n-1}},2).$$

(ii) If $\underline{e} = (2^{q_1}, \ldots, 2^{q_{n-2}},2,0)$ with $q_i > 1$ $(1\leq i\leq n-2)$, then

$$\Delta(\alpha(\underline{e})) = \alpha(2^{q_1},\ldots,2^{q_{n-2}},2,1).$$

REFERENCES

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

[2] G.R. Chapman, Generators and Relations for the cohomology of Janko's first group, Proc. Groups - St. Andrews (1981), London Math. Soc. Lecture Note Series, no.71.

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

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

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

Rebut el 6 de setembre del 1983

Department of Mathematics and Statistics,
University of Guelph,
Guelph, Ontario, N1G 2W1.
CANADA