Pointwise Conjugate Groups and Modules over the Steenrod Algebra

Dissertation
zur erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultäten
der Georg-August-Universität zu Göttingen

vorgelegt von
Joel Segal
aus London, Großbritannien.

Göttingen 1999

D 7
Referent: Larry Smith
Koreferent: Grant Walker
Tag der mündlichen Prüfung:

Pointwise Conjugate Groups and Modules over the Steenrod Algebra

Joel Segal

PhD Thesis, Göttingen 1999.

Abstract

This thesis is concerned with *pointwise conjugate representations* of finite groups and their rings of polynomial invariants. In particular, it will be shown that these rings are isomorphic as modules over the Steenrod algebra $\mathcal{P}^*$ if and only if the group representations are pointwise conjugate.

Contents

1 Introduction

The origins of this thesis lie in a paper by John Martino and Stuart Priddy, *Stable Homotopy Classification of* $BG^\wedge_p$ [16] from 1995. In it, they give a necessary and sufficient condition for the p-completions $BG^\wedge_p$ and $BG'^\wedge_p$ of the classifying spaces of two groups G and G' to be stably homotopy equivalent. For a finite group G, its classifying space BG is an Eilenberg-MacLane space $K(G,1)$ and thus G determines BG up to homotopy equivalence. This is however no longer true for *stable* homotopy equivalence: that is, $\Sigma^k BG \simeq \Sigma^k BG'$ for large k need not imply that $G \cong G'$. As

$$BG \simeq \bigvee_{p||G|} BG^\wedge_p,$$

stably, where $BG^\wedge_p$ is the p-completion of BG, they examined the question as to when two such p-completions for different groups are stably homotopy equivalent.

This turned out to involve the idea of *pointwise conjugacy*, the situation where there is a set bijection between two subgoups of a group, such that corresponding elements are conjugate in the larger group. This is clearly a generalisation of the notion of conjugate subgroups. Larry Smith noticed the connection with invariant theory, and suggested the project of treating this idea in an invariant theory context. Thus the beginning of the thesis was to translate some of the results of the paper [16] into a non homotopy-theoretic language and find proofs independent of the deep homotopy theory machinery used there. This is done in Section 2.

Any study of stable homotopy theory involves the *Steenrod algebra* $\mathcal{A}_p$, the algebra of all natural stable transformations of the mod p cohomology functor. The Steenrod algebra originally entered invariant theory via topology, as invariant rings occur naturally as the cohomology rings of certain spaces (see Section 6). It is a powerful tool in the study of invariants, see for example [22].

In characteristic $p \neq 2$ the invariant rings occurring as cohomology rings are naturally graded with generators in degree 2. Thus the Bockstein operator in the Steenrod algebra is identically zero on these polynomial invariant rings, as it increases degrees by 1. In this context, I follow Larry Smith in denoting the Steenrod algebra without Bockstein as $\mathcal{P}^*$, and defining it in terms of generators and relations of operators on a polynomial ring $\mathbb{F}[V]$, independently of topology.

The utility of $\mathcal{P}^*$ in invariant theory lies in the fact that the invariant ring $\mathbb{F}[V]^G$ of a finite group G has the structure of an *unstable algebra over*

$\mathcal{P}^*$, it is a module over $\mathcal{P}^*$ which satisfies the so-called *unstability conditions* (see Section 4). Thus elements of $\mathcal{P}^*$ take invariants to invariants, and can be used to manufacture new invariants from old. The existence of this $\mathcal{P}^*$-module and -algebra structure of course raises the question as to whether it is restricted, or determined, by the group G, and it is this question which the thesis treats. In particular, in the central Section 5 it is shown that two invariant rings $\mathbb{F}[V]^H$ and $\mathbb{F}[V]^K$ of finite groups H and K are isomorphic as *unstable modules* over $\mathcal{P}^*$ if and only if H and K are pointwise conjugate in $GL(n, \mathbb{F})$, and isomorphic as *unstable algebras* over $\mathcal{P}^*$ if and only if H and K are conjugate in $GL(n, \mathbb{F})$.

The topological Steenrod algebra is used only in Section 6, where applications to topology are given, namely examples of non homotopy-equivalent topological spaces with the same $\mathcal{A}_p$-module structure.

The structure of the thesis is as follows. Apart from Sections 6 and 7, we treat almost exclusively the *non-modular* case, that is, when the characteristic of the field does not divide the order of the group. Sections 1.1 and 1.2 briefly treat the invariant theory and representation theory needed in the sequel. Section 2 introduces the definition of pointwise conjugacy, giving a number of equivalent conditions which are used in an essential way in the rest of the thesis. Section 3 treats the question as to precisely when this situation arises, showing that pointwise conjugacy is in some sense equivalent to the condition of *conformality* for groups, an old term denoting that two groups have the same number of elements of each order. Some examples are given, and various group theory results are quoted which guarantee an infinite (and fairly 'common') supply of pairs of pointwise conjugate representations.

In Section 4 the Steenrod algebra and the *Dickson algebra*, a particular invariant ring, are defined. Applications to invariant rings make their first appearance in Section 5, where it is shown that, in the non-modular case, pointwise conjugacy is equivalent to the invariant rings being isomorphic as modules over $\mathcal{P}^*$. Section 6 gives a topological interpretation and examples, and Section 7 examines the *modular* case: that is, when the characteristic of the field divides the order of the group. As is often the case in invariant theory and representation theory, the nice results in the non-modular case are then no longer true.

I would like to thank the many colleagues and friends who supported me in various ways during work on this thesis, in particular my supervisor Larry Smith for always being full of ideas and suggestions for further work – much more than I could do credit to! And Miriam Seibold, thanks to whom I came to Göttingen in the first place.

1.1 Representation theory

Let $\rho : G \longrightarrow GL(n, \mathbb{F})$ be a representation of a finite group G. The G action on $V = \mathbb{F}^n$ can be extended to an action of the *group algebra* $\mathbb{F}G$, defined to be $\mathbb{F}$-linear combinations of elements of G, via

$$\left(\sum_{g \in G} \lambda_g g \right)(v) = \sum_{g \in G} \lambda_g g(v).$$

This makes V into an $\mathbb{F}G$-module, and conversely any finite dimensional $\mathbb{F}G$-module induces a representation of G by restriction to the group elements. Thus representations of G and $\mathbb{F}G$-modules are equivalent terms, and will be used interchangeably in the sequel. All modules referred to will be *left* modules, unless explicitly stated otherwise.

The *character* of the representation is a function $\chi : G \longrightarrow \mathbb{F}$, given by $\chi(g) = \text{trace}(\rho(g))$. Suppose that the characteristic of $\mathbb{F}$ does not divide the order of G. This is called the *non-modular case.* Then the character determines the representation up to conjugacy in $GL(n, \mathbb{F})$, provided that $\mathbb{F}$ is sufficiently large, i.e. contains roots of unity for all divisors of $|G|$. If however $char(\mathbb{F}) = p$ and $p \mid |G|$, then the situation is more complicated. Brauer ([6]) found a way to define a character in $\mathbb{C}$, starting from a representation in $\mathbb{F}$. This *Brauer character* has many of the properties of the non-modular case, in particular we shall use the fact that if V is a *projective* $\mathbb{F}G$-module, the Brauer character characterises the representation up to conjugacy in $GL(n, \mathbb{F})$ (see [3] or [21]).

Let H be a subgroup of G. Given a representation $\sigma : H \longrightarrow GL(n, \mathbb{F})$ and corresponding $\mathbb{F}H$-module V, we define the *induced representation* on G to be the $\mathbb{F}G$-module

$$\mathbb{F}G \otimes_{\mathbb{F}H} V,$$

denoted $Ind_H^G(\sigma)$. Equivalently, the induced representation can expressed as the G-module

$$Ind_H^G = \bigoplus_{r \in R} rV$$

where R is a set of left coset representatives of H in G. Let χ be the character of σ. If $char(\mathbb{F}) \nmid |H|$, the character χ_H^G of the induced representation can be expressed in terms of χ: to wit

$$\chi_H^G(g) = \frac{1}{|H|} \sum_{\substack{x \in G, \\ x^{-1}gx \in H}} \chi(x^{-1}gx).$$

For details, see [10] Chapter 10.

1.2 Polynomial invariants of groups

Invariant theory in this paper denotes the study of invariants of polynomial rings under the action of a (finite) group. Let $\mathbb{F}$ be a field, and let $V = \mathbb{F}^n$ be an n-dimensional vector space over $\mathbb{F}$. A subgroup $G < GL(n, \mathbb{F})$ operates on V^*, the dual space to V, as follows: for $g \in G$ and $f \in V^*$, let $(gf)(v) := f(g^{-1}v)$ for each $v \in V$. Let $\mathbb{F}[V]$ be the $\mathbb{F}$-algebra of polynomial functions on V, which may be defined as the symmetric algebra on V^*. Thus if $\{x_1, \ldots, x_n\}$ is an $\mathbb{F}$-basis for $V^* = \mathrm{Hom}_{\mathbb{F}}(V^*, \mathbb{F})$, then

$$\mathbb{F}[V] = \mathbb{F}[x_1, \ldots, x_n] = \mathbb{F} \oplus V^* \oplus S^2(V^*) \oplus S^3(V^*) \oplus \cdots .$$

Here $S^k(V^*)$ denotes the k-th symmetric power of V^*, i.e. the set of homogeneous polynomials of degree k in $x_1, \ldots, x_n$. $\mathbb{F}[V]$ is naturally graded by giving each x_i degree 1 (or degree 2 in certain cases if we are doing topology), and the action of G on V^* extends multiplicatively to a degree-preserving action on $\mathbb{F}[V]$. The *ring of invariants* $\mathbb{F}[V]^G$ is defined as

$$\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] : gf = f \quad \forall g \in G\}.$$

More generally, we are interested in the invariants of a faithful linear representation of a group $\rho : G \hookrightarrow GL(n, \mathbb{F})$. Identifying G with its image in $GL(n, \mathbb{F})$, we may talk of the ring of invariants of G when it is clear from the context which faithful representation is implied. Apart from in the last section, we shall be concerned almost exclusively with the case where $char(\mathbb{F}) \nmid |G|$.

There are one or two classical theorems which I shall make use of in this paper, the first of which was historically very important, providing part of the motivation for the beginnings of modern commutative algebra:

Theorem *(Hilbert, Noether)* $\mathbb{F}[V]^G$ *is finitely generated as an* $\mathbb{F}$*-algebra, and* $\mathbb{F}[V]$ *is an integral extension of* $\mathbb{F}[V]^G$.

Proof. Every element $x \in \mathbb{F}[V]$ is a root of the monic polynomial

$$\prod_{g \in G} (X - gx) \in \mathbb{F}[V]^G[X].$$

If A is the subalgebra of $\mathbb{F}[V]^G$ generated by the coefficients of the polynomials satisfied by the algebra generators of $\mathbb{F}[V]$, then the tower $A \subseteq \mathbb{F}[V]^G \subseteq \mathbb{F}[V]$ sandwiches $\mathbb{F}[V]^G$ between two noetherian rings, with $\mathbb{F}[V]$ integral over A. Thus $\mathbb{F}[V]$ is finitely generated as an A-module. $\mathbb{F}[V]^G$ is a submodule, hence also finitely generated over A, and thus over $\mathbb{F}$. ■

The action of G on $\mathbb{F}[V]$ can be extended to an action on the field of fractions $\mathbb{F}(V)$ of $\mathbb{F}[V]$:

$$g(f_1/f_2) := g(f_1)/g(f_2).$$

We denote the subfield of elements fixed under this action by $\mathbb{F}(V)^G$.

Proposition *$\mathbb{F}(V)$ is a Galois extension of $\mathbb{F}(V)^G$ with Galois group G. The field $\mathbb{F}(V)^G$ is the field of fractions of $\mathbb{F}[V]^G$, and $\mathbb{F}[V]^G$ is integrally closed in $\mathbb{F}(V)^G$.*

Proof. G acts as field automorphisms of $\mathbb{F}(V)$, so the first statement is clear. It is also clear that $FF(\mathbb{F}[V]^G) \subseteq \mathbb{F}(V)^G$. Any element of $\mathbb{F}(V)^G$ can be written as f_1/f_2 where $f_2 \in \mathbb{F}[V]^G$, by multiplying numerator and denominator by the distinct images of the numerator under the G-action. Then f_1 must also be G-invariant, giving the other inclusion.

Any $f \in \mathbb{F}(V)^G$ integral over $\mathbb{F}[V]^G$ is also integral over $\mathbb{F}[V]$. As $\mathbb{F}[V]$ is integrally closed over $\mathbb{F}(V)$, it follows that $f \in \mathbb{F}[V]$, and hence that $f \in \mathbb{F}[V]^G$. ■

The *Poincaré series* for the algebra $\mathbb{F}[V]^G$ is a way of encoding the vector space dimensions of the homogeneous components $\mathbb{F}[V]^G_k$: it is defined by

$$P(\mathbb{F}[V]^G, t) := \sum_{k=0}^{\infty} \dim_{\mathbb{F}}(\mathbb{F}[V]^G_k) t^k.$$

A first indication that pointwise conjugacy might have implications for invariant rings is given by the theorem of Molien (see e.g. [22]):

Theorem *(Molien) Let $\rho : G \hookrightarrow GL(n, \mathbb{F})$ be a representation of a finite group G over a field $\mathbb{F}$ of characteristic zero. Then the Poincaré series of the ring of invariants is given by*

$$P(\mathbb{F}[V]^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - \rho(g)^{-1} t)}.$$

The result is also true in positive characteristic p for $p \nmid |G|$. In this case one must use a 'Brauer Lift', lifting the eigenvalues to characteristic zero and defining trace and determinant by addition and multiplication.

Suppose that the elements of two groups H, K can be paired off so that for two representations $\rho : H \hookrightarrow GL(n, \mathbb{F})$ and $\sigma : K \hookrightarrow GL(n, \mathbb{F})$ corresponding elements h, k have images $\rho(h)$ and $\sigma(k)$ which are conjugate in

$GL(n, \mathbb{F})$; in other words, that $\rho(H)$ and $\sigma(K)$ are pointwise conjugate in $GL(n, \mathbb{F})$. (Pointwise conjugacy will be properly defined in the next Section). Then Molien's Theorem implies that $P(\mathbb{F}[V]^H, t) = P(\mathbb{F}[V]^K, t)$, as the determinants of $(1 - At)$ and $(1 - Bt)$ are equal if A and B are conjugate matrices.

Thus pointwise conjugate representations of groups evidently have invariant rings which are related in some way, in particular having the same structure as graded vector spaces. The rest of the thesis examines this in more detail.

2 Pointwise Conjugacy

In this section we introduce the basic notation and present the first main theorem.

Definition Let $\rho : H \hookrightarrow GL(n, \mathbb{F})$ and $\sigma : K \hookrightarrow GL(n, \mathbb{F})$ be faithful representations of finite groups over the field $\mathbb{F}$. We say ρ and σ are **pointwise conjugate** or PC if there is a set bijection $\gamma : H \longrightarrow K$ such that, for all $h \in H$, $\rho(h)$ is conjugate to $\sigma(\gamma(h))$ in $GL(n, \mathbb{F})$.

More generally, consider the following

Definition Let G be a finite group and $H, K < G$ subgroups. We say H and K are **pointwise conjugate in** G, or simply pointwise conjugate if G is clear from context, if there is a bijection between them such that corresponding elements are conjugate in G.

Clearly, as ρ and σ are faithful representations, when we identify the groups H and K with their images in $GL(n, \mathbb{F})$ the definitions coincide.

The following easy observation is often useful:

Lemma 1 *$H, K < G$ are pointwise conjugate if and only if $|H \cap C| = |K \cap C|$ for every conjugacy class C in G.*

For the next theorem, we need a preparatory Lemma:

Lemma 2 *Let S be the $\mathbb{F}$-vector subspace of the group algebra $\mathbb{F}(G)$ consisting of those $\sum_{g \in G} \lambda_g g$ which satisfy the following condition: $\sum_{g \in C} \lambda_g = 0$ for every conjugacy class C in G. Let $[\mathbb{F}(G), \mathbb{F}(G)]$ be the vector subspace of $\mathbb{F}(G)$ spanned by all commutators of elements of G. Then $S = [\mathbb{F}(G), \mathbb{F}(G)]$.*

Proof. It is clear that S is in fact a subspace. Suppose x, $y \in G$. Then the commutator

$$\begin{aligned} xy - yx &= xy - x^{-1}(xy)x \\ &= 1(xy) + (-1)(xy)^x, \end{aligned}$$

(where $g^x := x^{-1}gx$), which is in S. Thus every commutator is in S, hence the subspace generated by commutators is contained in S. Next, suppose $\{g^{x_1}, \ldots, g^{x_r}\}$ is a conjugacy class in G, and $w = \sum \lambda_i g^{x_i}$ with $\sum \lambda_i = 0$. Then $w = \sum \lambda_i (g^{x_i} - g) = \sum \lambda_i (h_i x_i - x_i h_i)$, where $h_i = x_i^{-1} g$, is a linear combination of commutators and so in $[\mathbb{F}(G), \mathbb{F}(G)]$. But every element of S can be written as a sum of such w, and we are finished. ∎

Theorem 3 *Let G be a finite group and $H, K < G$ subgroups such that $|H| \cdot |K| \in \mathbb{F}^\times$ (i.e. the characteristic of the field does not divide the orders of H or K). Then the following conditions are equivalent:*

(a) $H, K < G$ *are pointwise conjugate*

(b) $Ind_H^G(1_H) \cong Ind_K^G(1_K)$ *as* $\mathbb{F}(G)$*-modules*

(c) the idempotents

$$e_H = \frac{1}{|H|} \sum_{h \in H} h$$
$$e_K = \frac{1}{|K|} \sum_{k \in K} k$$

are conjugate in the group ring $\mathbb{F}(G)$.

Furthermore for char($\mathbb{F}$)$\neq$ 2, the following are also equivalent to the above:

(d) there are elements ζ *and* ξ *in* $\mathbb{F}(G)$ *such that:* $e_H = \zeta e_K \xi e_H$ *and* $e_K = \xi e_H \zeta e_K$

(e) $e_H - e_K \in [\mathbb{F}(G), \mathbb{F}(G)]$ *, where* $[\mathbb{F}(G), \mathbb{F}(G)]$ *denotes the vector space generated by all commutators in* $\mathbb{F}(G)$.

Proof. $(a) \Leftrightarrow (b)$: We claim that the $\mathbb{F}(G)$-modules $Ind_H^G(1_H)$ and $Ind_K^G(1_K)$ have the same (Brauer) character (see [21] Chapter 18), where 1_H is the trivial $\mathbb{F}(H)$-module, 1_K the trivial $\mathbb{F}(K)$-module. Let χ_H^G be the character of $Ind_H^G(1_H)$, χ_{1_H} that of 1_H, and similarly for χ_K^G, χ_{1_K}. For $g \in G$, with conjugacy class (g) in G, the following calculation

$$\begin{aligned}
\chi_H^G(g) &= \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} \chi_{1_H}(x^{-1}gx) \\
&= \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} 1 \\
&= \frac{1}{|H|} |(g) \cap H| \cdot |C_G(g)| \\
&= \frac{1}{|K|} |(g) \cap K| \cdot |C_G(g)| \qquad (*) \\
&= \chi_K^G(g)
\end{aligned}$$

where $C_G(g)$ denotes the centraliser of g in G, shows that $\chi_H^G(g) = \chi_K^G(g)$ if and only if $\frac{1}{|H|}|(g) \cap H| = \frac{1}{|K|}|(g) \cap K|$. This holds for all $g \in G$ if H is pointwise conjugate to K by Lemma 1. Conversely, if $\chi_H^G(g) = \chi_K^G(g)$, then

$$\frac{|G|}{|H|} = \chi_H^G(id) = \chi_K^G(id) = \frac{|G|}{|K|},$$

so $|H| = |K|$ and thus $|(g) \cap H| = |(g) \cap K|$, so H is pointwise conjugate to K in G by Lemma 1. Note that even in the characteristic p case, the Brauer character is defined over a finite extension of $\mathbb{Q}$, thus the equalities are not just modulo p.

Observe that $1_H \cong \langle e_H \rangle$, the $\mathbb{F}(H)$-submodule of $\mathbb{F}(H)$ generated by the element e_H. It follows that

$$Ind_H^G(1_H) = \mathbb{F}(G) \otimes_{\mathbb{F}(H)} \langle e_H \rangle \cong \mathbb{F}(G) \cdot e_H, \qquad (\dagger)$$

and similarly for K, so the $\mathbb{F}(G)$-modules are projective (being direct summands of $\mathbb{F}(G)$). Projective modules are isomorphic if and only if they have the same Brauer character ([21] or [3] Cor. 5.3.6), and we are done.

$(b) \Rightarrow (c)$: Let e, f be idempotents in $\mathbb{F}(G)$. We shall show that $\mathbb{F}(G) \cdot e \cong \mathbb{F}(G) \cdot f$ as $\mathbb{F}(G)$-modules implies that e is conjugate to f. Using the isomorphism $(\dagger)$ above, applying this to e_H, e_K completes the proof.

Let $\phi' : \mathbb{F}(G) \cdot e \longrightarrow \mathbb{F}(G) \cdot f$ be the given isomorphism. Then $(1-e)(1-e) = 1 - 2e + e^2 = 1 - e$, so $(1-e)$ is also an idempotent and there are direct sum decompositions

$$\mathbb{F}(G) = \mathbb{F}(G) \cdot e \ \oplus \ \mathbb{F}(G) \cdot (1-e)$$
$$\mathbb{F}(G) = \mathbb{F}(G) \cdot f \ \oplus \ \mathbb{F}(G) \cdot (1-f)$$

Let us first deal with the case when $\mathbb{F}(G)$ is semisimple. Then $\mathbb{F}(G) \cdot e \cong \mathbb{F}(G) \cdot f$ implies that

$$\mathbb{F}(G) \cdot (1-e) \cong \frac{\mathbb{F}(G)}{\mathbb{F}(G) \cdot e} \cong \frac{\mathbb{F}(G)}{\mathbb{F}(G) \cdot f} \cong \mathbb{F}(G) \cdot (1-f),$$

as $\mathbb{F}(G)/\mathbb{F}(G) \cdot e$ and $\mathbb{F}(G)/\mathbb{F}(G) \cdot f$ are uniquely determined by their composition factors.

In the case when $\mathbb{F}(G)$ is not semisimple, it has a non-zero radical R, and $\overline{\mathbb{F}(G)/R}$ is semisimple. Let reduction modulo R be denoted by bars. Then $\overline{\mathbb{F}(G) \cdot e} = \overline{\mathbb{F}(G)} \cdot \overline{e}$, and the argument above tells us that $\overline{\mathbb{F}(G)} \cdot \overline{(1-e)} \cong \overline{\mathbb{F}(G)} \cdot \overline{(1-f)}$. From [10] Thm 6.8, 'lifting idempotents', it follows that the lifts must be isomorphic, and so

$$\mathbb{F}(G) \cdot (1-e) \cong \mathbb{F}(G) \cdot (1-f),$$

also in this case. Call the induced isomorphism $\phi'' : \mathbb{F}(G) \cdot (1-e) \longrightarrow \mathbb{F}(G) \cdot (1-f)$.

Define a map $\phi : \mathbb{F}(G) \longrightarrow \mathbb{F}(G)$ by $\phi(a) = \phi'(ae) + \phi''(a(1-e))$. Then $\phi|_{\mathbb{F}(G)\cdot e} = \phi'$ and $\phi|_{\mathbb{F}(G)\cdot(1-e)} = \phi''$, so ϕ is an isomorphism being so on each of the direct summands.

$$\begin{array}{ccccc} \mathbb{F}(G) & \cong & \mathbb{F}(G)\cdot e & \oplus & \mathbb{F}(G)\cdot(1-e) \\ \phi\downarrow & & \phi'\downarrow & & \phi'\downarrow \\ \mathbb{F}(G) & \cong & \mathbb{F}(G)\cdot f & \oplus & \mathbb{F}(G)\cdot(1-f) \end{array}$$

Consider the identity element $1 \in \mathbb{F}(G)$, and let $\phi(1) = \zeta$. For all $a \in \mathbb{F}(G)$ we have $\phi(a) = \phi(a \cdot 1) = a \cdot \phi(1) = a \cdot \zeta$, as ϕ is a $\mathbb{F}(G)$-homomorphism. Since ϕ is also surjective, there exists $b \in \mathbb{F}(G)$ such that $1 = \phi(b) = b \cdot \zeta$, hence ζ is invertible.

Finally, in $\mathbb{F}(G) = \mathbb{F}(G) \cdot f \oplus \mathbb{F}(G) \cdot (1-f)$, we have

$$\begin{aligned} f + (1-f) &= \zeta^{-1} \cdot 1 \cdot \zeta \\ &= \zeta^{-1}(e + (1-e))\zeta \\ &= \zeta^{-1}e\zeta + \zeta^{-1}(1-e)\zeta. \end{aligned}$$

But $e\zeta = \phi(e)$, so $\zeta^{-1}e\zeta \in \mathbb{F}(G)\cdot f$, and similarly $\zeta^{-1}(1-e)\zeta \in \mathbb{F}(G)\cdot(1-f)$. Taking components gives $f = \zeta^{-1}e\zeta$ as required. As noted, this yields $(b) \Rightarrow (c)$.

$(c) \Rightarrow (b)$: Suppose $e_H = ae_Ka^{-1}$. Define a map $\psi : \mathbb{F}(G) \cdot e_H \longrightarrow \mathbb{F}(G) \cdot e_K$ by $\psi(xe_H) = xe_Ha = xa^{-1}e_K$. Clearly, this is a left $\mathbb{F}(G)$-module homomorphism, as it is simply right multiplication by an element of $\mathbb{F}(G)$. Surjectivity is immediate: given $ye_K \in \mathbb{F}(G)\cdot e_K$, $\psi(yae_H) = yaa^{-1}e_K = ye_K$. Injectivity is equally easy: $\psi(xe_H) = \psi(ye_H) \Leftrightarrow xe_Ha = ye_Ha \Leftrightarrow xe_H = ye_H$, as a is invertible in $\mathbb{F}(G)$. Thus $\mathbb{F}(G) \cdot e_H \cong \mathbb{F}(G) \cdot e_K$. As noted above,

$$Ind_H^G(1_H) \cong \mathbb{F}(G) \otimes_{\mathbb{F}(H)} \langle e_H \rangle \cong \mathbb{F}(G) \cdot e_H$$

and similarly for e_K. So

$$Ind_H^G(1_H) \cong \mathbb{F}(G) \cdot e_H \cong \mathbb{F}(G) \cdot e_K \cong Ind_K^G(1_K)$$

as required.

$(c) \Rightarrow (d)$: Suppose $e_H = a^{-1}e_Ka$. Then $e_H = a^{-1}e_Kae_H$, as e_H is an idempotent. Similarly, we have $e_K = ae_Ka^{-1}e_H$, and with $a^{-1} = \zeta$ and $a = \xi$ we are done.

$(d) \Rightarrow (e)$: $e_H - e_K = (\zeta e_K)(\xi e_H) - (\xi e_H)(\zeta e_H)$ is a linear combination of commutators. (ζ, ξ, e_H and e_K are sums of elements of G, and addition is associative over the group operation).

$(e) \Rightarrow (a)$: $e_H - e_K \in [\mathbb{F}(G), \mathbb{F}(G)] = S$, by Lemma 2. Consider the coefficient of id in this sum: $1/|H| - 1/|K|$. The identity is a complete conjugacy class, so $1/|H| - 1/|K| = 0$ by our characterisation of S. Thus $|H| = |K|$. Elements s of S can be written as $s = \sum_{a,d \in G} \lambda_{ab}(ab - ba)$. Setting $x = ab$, $y = a$, we have

$$s = \sum_{x,y \in G} \lambda_{xy}(x - y^{-1}xy). \qquad (**)$$

Consider $s = |H|(e_H - e_K) \in S$. Then

$$s = \sum_{h \in H} h - \sum_{k \in K} k.$$

Comparing this expression to (**), we see that for each $h \in H$, there is a conjugate $y_h^{-1} h y_h$ as summand in s with coefficient -1 for some $y_h \in G$. Assuming we are not in characteristic 2, this element must be in the second sum; i.e. $y_h^{-1} h y_h = k$ for some $k \in K$. But this holds for each element of H, and similarly with signs swapped for each element of K, so H and K are pointwise conjugate as required. ■

3 Finding Examples

3.1 Conformal groups

This is all very well. However, the construction can only be of interest if examples actually exist. How can we find some? Clearly, for two groups to be pointwise conjugate in a parent group it is necessary that they have the same number of elements of a given order, as conjugate elements have the same order. In fact in the case of linear representations this is in the following sense also sufficient:

Proposition 4 *For two finite groups H and K and any field $\mathbb{F}$ the following are equivalent:*

(a) H has the same number of elements of order n as K for each n,

(b) the regular representations of H and K over the field $\mathbb{F}$ are pointwise conjugate,

(c) there exist faithful representations of H and K which are pointwise conjugate.

Proof. (c) $\Rightarrow$ (a) as noted above, and (b) $\Rightarrow$ (c) is clear.

(a) $\Rightarrow$ (b): In the regular representation $reg(H)$, elements of H act as permutations, and $reg(H)$ is a subgroup of S_m, expressed as the group of permutation matrices in $GL(m, \mathbb{F})$. ($m = |H|$). Suppose $h \in H$ has order n. Let R be a set of right coset representatives for $< h >$, the cyclic subgroup generated by h. Then each repeated left multiplication by h on an element $r \in R$ gives a cycle c_r of length n

$$r \mapsto hr \mapsto \cdots \mapsto h^{n-1}r \mapsto r.$$

Each element $h \in H$ appears exactly once in a cycle in $\{c_r\}_{r \in R}$, so we see that h, as a permutation, has cycle shape $|H|/n$ cycles each of length n.

The same holds for any element k of order n in K. But in S_m, two elements are conjugate if and only if they have the same cycle shape. So $reg(h) \sim reg(k)$ in $S_m < GL(m, \mathbb{F})$, where $\sim$ denotes conjugacy. As H and K have the same number of elements of order n for each n, it follows that the regular representation of H is pointwise conjugate to that of K in S_m, and thus in $GL(m, \mathbb{F})$. ■

Two non-isomorphic groups are said to be *conformal* if they have the same number of elements of each order. Such group pairs have been studied,

and to some extent classified. We are interested in finite conformal groups. In particular, it is easy to see by the Structure Theorem for abelian groups that no two non-isomorphic abelian groups can be conformal. However, almost all abelian groups are conformal to at least one non-abelian group; more precisely, an abelian group is conformal to some other group if and only if

1. for p an odd prime, at least one of its Sylow p-subgroups is non-cyclic of order $> p^2$, or

2. if its Sylow 2-subgroups is of order $> p^3$ and not elementary abelian

([17] pages 107-109). For a given natural number $n = p_1^{a_1} \dots p_r^{a_r}$, n odd or squarefree, R. Scapellato [19] has determined exactly when there exist conformal pairs of groups of order n. Say $n \in C$ if this is the case.

For n odd,

a) some $a_i > 2$ implies $n \in C$; if no $a_i > 2$, then

b) $n \notin C$ if and only if for all p_i, p_j, p_k, $(p_k | p_i - 1, p_j - 1) \Rightarrow (p_i = p_j$ and $p_i^2 \nmid n$.

For n squarefree, $n \in C$ if and only if there exist p_i, p_j, p_k, with $p_k \neq 2$, such that $p_k | p_i - 1$ and $p_k | p_j - 1$.

For p-groups, we have ([8] p. 53):

Let p be a prime number. If H, K are groups of order p^s and neither has an element of order p^2, then H is conformal with K.

In view of Proposition 4, these results guarantee an infinite supply of groups with pointwise conjugate representations. In the Appendix there is a table of groups of order up to 190, showing how many conformal pairs, triples etc of each order there are.

Having found pointwise conjugate representations of two groups (e.g. their regular representations), one can often reduce the dimension of the representations using the following Lemma:

Lemma 5 *Let $\rho(H)$, $\sigma(K) < GL(n, \mathbb{F})$ be pointwise conjugate representations of the finite groups H, K over a field $\mathbb{F}$ of characteristic not dividing $|H| = |K|$, which is sufficiently large (i.e. which contains a primitive r-th root of unity, where r is the least common multiple of the orders of the elements of the groups). Let the representations ρ and σ be reducible, $\rho = \bigoplus_i \rho_i$,*

$\sigma = \bigoplus_j \sigma_j$ with $\rho_1, \ldots, \rho_s$ and $\sigma_1, \ldots, \sigma_s$ (not necessarily all of the) representations of degree one, which take the same value on corresponding elements of H and K. Then the representations

$$\bigoplus_{i \neq 1 \ldots s} \rho_i(H) \text{ and } \bigoplus_{j \neq 1 \ldots s} \sigma_j(K)$$

are also pointwise conjugate.

Proof. As $\mathbb{F}$ is sufficiently large, by Maschke's Theorem we can find a basis of $\mathbb{F}^n$ such that for each $h \in H$ and corresponding $k \in K$, $\rho(h) := P$ and $\sigma(k) := Q$ have the form

$$P = \begin{pmatrix} \lambda & 0 \\ 0 & P' \end{pmatrix}, \quad Q = \begin{pmatrix} \lambda & 0 \\ 0 & Q' \end{pmatrix}$$

where λ is $\rho_1(h) = \sigma_1(k)$. We know that P and Q are conjugate, and claim that P' and Q' are also. Consider the Jordan normal form of the matrices, with the diagonal entry corresponding to the eigenvalue λ in the top left corner. As the matrices are conjugate, they have the same normal form. Thus P' and Q' also have the same normal form, and are thus conjugate as claimed.

P' and Q' also have an eigenvalue $\rho_2(h) = \sigma_2(k)$ in common, so repeating the argument s times completes the proof. ■

3.2 Examples

The smallest non-isomorphic pairs of groups to satisfy the conditions of Proposition 4 are of order 16, where there are 3 sets of conformal groups, two sets of which consist of three groups. For example, $C_4 \times C_4 := H$ and $Q_8 \times C_2 := K$ have PC representations, where Q_8 is the quaternion group of order 8, and C_n the cyclic group of order n. $Q_8 \times C_2$ has 2 irreducible representations of degree 2, the rest being of degree 1. $C_4 \times C_4$ is abelian, so all its irreducible representations are of degree 1. Examining these representations, we find that Proposition 4 and Lemma 5 imply that the 12-dimensional (faithful) representation of K obtained from its regular representation by 'leaving out' four of the 1-dimensional irreducible summands is pointwise conjugate to some 12-dimensional representation of H.

The next smallest example is due to Stuart Priddy:

Example: For this example, define $K := C_3 \times C_3 \times C_3$, a direct product of 3 cyclic groups of order 3; and $H := \{$upper triangular matrices in $GL(3, \mathbb{F}_3)$

with 1's on the diagonal}.

$$H = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in GL(3, \mathbb{F}_3) \right\}$$

H and K both have order 27, but are not isomorphic, as K is abelian and H is not.

Consider the regular representations $reg(H)$, $reg(K) < GL(3^3, \mathbb{F}_2)$ of H and K over the field $\mathbb{F}_2$. Every non-identity element of H and K has order 3, and Proposition 4 implies that these representations are pointwise conjugate. Adjoining a primitive third root of unity, ω, to the field does not change this, so we can take $\mathbb{F}$ to be sufficiently large.

This example generalises immediately to $C_p \times C_p \times C_p$ and $\left\{ \left(\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{smallmatrix} \right) \in GL(3, \mathbb{F}_p) \right\}$. These groups have p^3 elements, which act as p^2 disjoint p-cycles in S_{p^3}, and are thus PC. Similarly we do not have to take $GL(p^3, \mathbb{F}_2)$; any finite field of characteristic $\neq p$ works just as well.

Going back to the case $p = 3$, we can say more. As the situation is non-modular and the field $\mathbb{F}$ is large enough with respect to H and K, we know (Brauer) that the character and representation theories for these groups are 'the same' over $\mathbb{F}$ as over $\mathbb{C}$. This means that if we identify ω with a primitive third root of unity Ω say in $\mathbb{C}$, then the lifts of representations decompose the same as in characteristic p.

In fact, we know exactly how the regular representations of H and K decompose (see e.g. [12], p.298):

$$reg(K) \cong \bigoplus_{i,j,k=1}^{3} \rho_{i,j,k}, \quad reg(H) \cong \bigoplus_{l,m=1}^{3} \sigma_{l,m} \bigoplus 3\mu_1 \bigoplus 3\mu_2,$$

where $\rho_{i,j,k}$ $i, j, k = 1 \ldots 3$ and $\sigma_{l,m}$, $l, m = 1 \ldots 3$ are one-dimensional representations. If we write elements of K as triples (a_1, a_2, a_3), with $a_m \in \mathbb{Z}/3\mathbb{Z}$, then we can take

$$\rho_{i,j,k}(a_1, a_2, a_3) = \Omega^{ia_1 + ja_2 + ka_3 \pmod 3}.$$

What about the σ_j ? Matrix multiplication gives

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & b+y+az \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}$$

so we can express H as the set of triples (a, b, c), with entries in $\mathbb{Z}/3\mathbb{Z}$ and composition rule $(a, b, c) \cdot (x, y, z) = (a + x, b + y + az, c + z)$. With this

notation it is easy to see that the 9 one-dimensional representations are $\sigma_{r,s}(a,b,c) = \Omega^{ra+sc}$.

Comparing this with the values of $\rho_{i,j,k}$ and using Lemma 5 we see that, renumbering so that $\{\rho_1 \dots \rho_9\} = \{\rho_{i,1,k} : i,k = 1 \dots 3\}$, and $\{\rho_{10} \dots \rho_{27}\} = \{\rho_{i,j,k} : j \neq 1\}$, the following matrix representations are also pointwise conjugate:

$$rep(k) = \begin{pmatrix} \rho_{10}(k) & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \rho_{27}(k) \end{pmatrix}$$

for $k \in K$ and

$$rep'(h) = \begin{pmatrix} \mu_1(h) & 0 & \cdots & & \cdots & 0 \\ 0 & \mu_1(h) & 0 & & & \vdots \\ \vdots & 0 & \mu_1(h) & \ddots & & \\ & & \ddots & \mu_2(h) & \ddots & \vdots \\ \vdots & & & \ddots & \mu_2(h) & 0 \\ 0 & \cdots & & \cdots & 0 & \mu_2(h) \end{pmatrix}$$

for $h \in H$. Thus we obtain an explicit example of two pointwise conjugate representations of non-isomorphic groups.

How can we find more examples? A useful tool, in the non-modular case, is the *character table:*

Proposition 6 *Let $\rho : H \hookrightarrow GL(n,\mathbb{F})$, $\sigma : K \hookrightarrow GL(n,\mathbb{F})$ be (faithful) representations of the finite groups H and K over the field $\mathbb{F}$, sufficiently large and of characteristic not dividing $|H|$, $|K|$. Let $\{C_i\}$ and $\{D_j\}$ be the conjugacy classes of elements of H respectively K, and suppose there is a bijection $\{C_i\} \longrightarrow \{D_j\}$, where $C_k \mapsto D_k$, and*

1) $|C_k| = |D_k|$,

2) $\chi_\rho(C_k) = \chi_\sigma(D_k)$, *with χ denoting (Brauer) character,*

3) *for $x \in C_k$, $y \in D_k$, $ord(x) = ord(y)$, and this order is either* prime, *or in the case $n = 2$, odd.*

Then the representations are pointwise conjugate. Furthermore, if $H = K$, condition (3) need only hold for those $C_k \neq D_k$.

In fact $\{C_i\}$ and $\{D_j\}$ do not actually have to be conjugacy classes; any sets of elements of the same order on which the characters are constant will do - for example single group elements.

Proof. Over $\mathbb{F}$, every matrix $\rho(h)$ (or $\sigma(k)$) is diagonalisable, with diagonal entries $ord(h)$-th roots of unity whose sum gives the character of h. Suppose that $\{\omega_i\}$ are those for $\rho(x)$, $\{\nu_j\}$ those for $\sigma(y)$ with x and y as in (3). Then from (2),

$$\sum_{i=1}^{n} \omega_i = \chi_\rho(x) = \chi_\sigma(y) = \sum_{j=1}^{n} \nu_j. \qquad (*)$$

If there is a renumbering such that $\omega_k = \nu_k$ for all k, then $\rho(x)$ is conjugate to $\sigma(y)$ in $GL(n, \mathbb{F})$, as a permutation of basis is a conjugacy operation:

$$A \sim \begin{pmatrix} \omega_1 & & \\ & \ddots & \\ & & \omega_n \end{pmatrix} \sim \begin{pmatrix} \omega_{i_1} & & \\ & \ddots & \\ & & \omega_{i_n} \end{pmatrix} \sim B \quad \Rightarrow A \sim B.$$

When is there such a renumbering?

i) Take the case $ord(x) = ord(y) = p$, prime. Let ζ be a primitive p-th root; each ω_i and ν_j is a p-th root of unity, and is thus some power (between 0 and $p-1$) of ζ. So we can rewrite equation (*) as follows, noting that $1 + \zeta + \cdots + \zeta^{p-1} = 0$:

$$\sum_{i=1}^{n} \omega_i = \sum_{k=0}^{p-1} a_k \zeta^k, \quad \sum_{j=1}^{n} \nu_j = \sum_{k=0}^{p-1} b_k \zeta^k,$$

$$\Rightarrow \sum_{k=0}^{p-1} a_k \zeta^k = \sum_{k=0}^{p-1} b_k \zeta^k$$

$$\Rightarrow \sum_{k=0}^{p-1} (a_k - b_k)\zeta^k = 0$$

$$\Rightarrow \sum_{k=0}^{p-1} (a_k - b_k)\zeta^k - (a_{p-1} - b_{p-1})(1 + \zeta + \cdots + \zeta^{p-1}) = 0$$

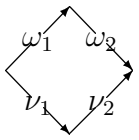
$$\Rightarrow \sum_{k=0}^{p-2} ((a_k - b_k) - (a_{p-1} - b_{p-1}))\zeta^k = 0$$

$$\Rightarrow (a_k - b_k) - (a_{p-1} - b_{p-1}) = 0, \quad \forall\, k$$

as the minimum polynomial of ζ is $1+x+\cdots+x^{p-1}$, which has degree $p-1$. So $(a_k - b_k) = (a_{p-1} - b_{p-1}) = r$, say, for each k. However, $\sum_k a_k = n = \sum_k b_k$,

so $\sum_k (a_k - b_k) = (p-1)r = 0$, and $r = 0$. So $a_k = b_k \quad \forall k$, and $\{\omega_i\} = \{\nu_j\}$ as required.

ii) Take the case $n = 2$ and $ord(x) = ord(y)$ is odd. Then ω is an $ord(x)$-th root of unity $\Rightarrow -\omega$ is not. Lifting the characters to $\mathbb{C}$, the equality of $\chi_\rho(x) = \omega_1 + \omega_2$ and $\chi_\sigma(y) = \nu_1 + \nu_2$ gives us the following picture:



$\Rightarrow \{\omega_1, \omega_2\} = \{\nu_1, \nu_2\}$.

■

Examples:

The 2-dimensional irreducible representations of D_{2p} over $\mathbb{C}$ are PC;
the 2-dimensional irreducible representations of $SL(2, \mathbb{F}_3)$ over $\mathbb{C}$ are PC;
the 3-dimensional irreducible representations of A_5 over $\mathbb{C}$ are PC; and so on.
(see e.g. [12] for a collection of character tables of small groups).

4 Rings of Polynomial Invariants

In the sequel, we shall apply the group-theoretical results of the last sections to invariant theory. For this, we need to introduce two important algebras which are specific to the characteristic p case. A brief general introduction to polynomial invariants is given in Section 1.2 at the beginning of the paper.

4.1 The Dickson algebra

The *Dickson algebra* $\mathcal{D}^*(n)$ is the invariant ring $\mathbb{F}[V]^{GL(n,\mathbb{F})}$, where $\mathbb{F}$ is a *finite* field. Note that, for a finite field $\mathbb{F}$, $GL(n,\mathbb{F})$ is a finite group. As p divides the order of this group we are in the modular case. $\mathcal{D}^*(n)$ is in fact a polynomial subalgebra of $\mathbb{F}[V]$, generated by elements denoted by $d_{n,n-1},\ldots,d_{n,0}$ and called the Dickson polynomials (see [11]). It is clear that $\mathcal{D}^*(n) \subset \mathbb{F}[V]^G$ for any subgroup $G < GL(n,\mathbb{F})$, as any polynomial invariant under all of $GL(n,\mathbb{F})$ is certainly invariant under a subgroup. It follows further from Galois theory that $FF(\mathcal{D}^*(n)) \subset FF(\mathbb{F}[V]^G)$ is in fact a finite extension of fields, where FF– denotes field of fractions, and that $\mathbb{F}[V]^G$ is a finitely generated $\mathcal{D}^*(n)$-module with respect to polynomial multiplication. See [22] for more details.

4.2 The Steenrod algebra

Let $\mathbb{F}$ be the finite field with $q = p^\nu$ elements and define

$$P(\zeta) : \mathbb{F}[V] \longrightarrow \mathbb{F}[V][[\zeta]]$$

via

(a) $P(\zeta)$ is $\mathbb{F}$-linear,

(b) $P(\zeta)(v) = v + v^q\zeta$ for $v \in V^*$,

(c) $P(\zeta)(f \cdot g) = P(\zeta)(f) \cdot P(\zeta)(g)$ for $f, g \in \mathbb{F}[V]$,

(d) $P(\zeta)(1) = 1$.

Giving ζ degree $(1-q)$, $P(\zeta)$ is a graded ring homomorphism of degree zero. If we define P^i by requiring

$$P(\zeta)(f) = \sum_{i=1}^{\infty} P^i(f)\zeta^i$$

then each P^i is an $\mathbb{F}$-linear map $\mathbb{F}[V] \longrightarrow \mathbb{F}[V]$.

The operations P^i are called the *Steenrod reduced power operations over* $\mathbb{F}$. (For $q = 2$, the P^i are denoted Sq^i, and are called the *Steenrod squaring operations*). We define the *Steenrod algebra*, denoted $\mathcal{P}^*$, to be the subalgebra of the graded algebra of endomorphisms of the functor $V \mapsto \mathbb{F}[V]$ generated by the Steenrod operations. Note that the subalgebra is not free: the operations satisfy various relations such as the identity

$$P^1 P^1 = 2P^2.$$

A graded algebra which is also a module over $\mathcal{P}^*$ is said to be an *unstable algebra* if it satisfies the *unstability conditions:*

$$P^i(u) = \begin{cases} u^q & \text{if } \deg(u) = i \\ 0 & \text{if } \deg(u) < i. \end{cases}$$

We are also interested in certain elements of $\mathcal{P}^*$ which act as derivations and are denoted P^{Δ_i}. They are defined inductively by:

$$\begin{aligned} P^{\Delta_1} &:= P^1, \\ P^{\Delta_i} &:= [P^{\Delta_{i-1}}, P^{q^{i-1}}],\ i \geq 2 \end{aligned}$$

where $[-,-]$ denotes commutator.

For an unstable algebra A over $\mathcal{P}^*$, define $\Delta(A)$ to be the A-module of endomorphisms of A generated by $\{P^{\Delta_i} \mid i = 0, 1, \dots\}$, where $P^{\Delta_0}(a) := \deg(a)a$. Suppose[1] that $\mathcal{D}^*(n) \leq A \leq \mathbb{F}[V]$. Then $\Delta(A)$ is finitely generated over A by $\{P^{\Delta_0}, \dots, P^{\Delta_{n-1}}\}$, and the relation

$$(-1)^n d_{n,0} P^{\Delta_0} + \cdots + (-1) d_{n,n-1} P^{\Delta_{n-1}} + P^{\Delta_n} = 0 \qquad (\Delta)$$

is minimal with respect to the P^{Δ_i} appearing in it: that is, any other linear dependance in $\Delta(A)$ involves P^{Δ_i} with i larger than n, or is a multiple of Δ. We can give $\Delta(A)$ a $\mathcal{P}^*$-module structure by linearly extending the definition

$$P^i(aP^{\Delta_j}) := P^i(a)P^{\Delta_j}$$

(see [18] Chapter 1).

If a finite group G acts on $\mathbb{F}[V]$ via a linear representation, then the G-action commutes with the Steenrod operations. Thus $\mathbb{F}[V]^G$ is mapped into itself by the Steenrod algebra, and is in fact an unstable algebra over $\mathcal{P}^*$. See for example [22] Chapter 10 for a more complete treatment of the subject.

[1]Note that $n = \dim_{\mathbb{F}}(V)$, so $\mathcal{D}^*(n) \leq A \leq \mathbb{F}[V]$ are finite extensions.

5 Modules over $\mathcal{P}^*$

In this section we prove the central results, namely that, in the non-modular case, two invariant rings are isomorphic as modules over $\mathcal{P}^*$ if and only if the corresponding groups are pointwise conjugate in $GL(n,\mathbb{F})$. As preparation, we need a couple of Lemmas:

Lemma 7 *Suppose that $\mathbb{F}[V]^H \xrightarrow{\phi} \mathbb{F}[V]^K$ is an isomorphism of unstable $\mathcal{P}^*$-algebras. Then $\phi(d)$ is scalar multiplication by an element λ of $\mathbb{F}$ for all $d \in \mathcal{D}^*(n)$.*

Proof. There is an obvious extension of ϕ to $\widetilde{\phi} : \Delta(\mathbb{F}[V]^H) \longrightarrow \Delta(\mathbb{F}[V]^K)$ via

$$\widetilde{\phi}\left(\sum f_i P^{\Delta_i}\right) = \sum \phi(f_i) P^{\Delta_i}.$$

This is a $\mathcal{P}^*$-module isomorphism, as ϕ is. Thus

$$\begin{aligned} -P^{\Delta_n} &= \widetilde{\phi}(-P^{\Delta_n}) \\ &= \widetilde{\phi}((-1)^n d_{n,0} P^{\Delta_0} + \cdots + (-1) d_{n,n-1} P^{\Delta_{n-1}}) \\ &= (-1)^n \phi(d_{n,0}) P^{\Delta_0} + \cdots + (-1)\phi(d_{n,n-1}) P^{\Delta_{n-1}} \end{aligned}$$

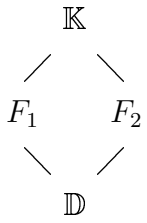
and the uniqueness of Δ implies $\phi(d_{n,i}) = \lambda d_{n,i}$ for all i, for a fixed $\lambda \in \mathbb{F}$. As $\mathcal{D}^*(n)$ is generated as an algebra by the $d_{n,i}$, the claim follows. ■

For two subgroups H and K of $GL(n,\mathbb{F})$, consider their rings of invariants $\mathbb{F}[V]^H$, $\mathbb{F}[V]^K$. If $FF(-)$ denotes the field of fractions functor, then $FF(\mathbb{F}[V]) = \mathbb{F}(V)$ is a Galois extension of the field $FF(\mathbb{F}[V]^H) = \mathbb{F}(V)^H$ with Galois group H, and similarly for K (see [22]).

Proposition 8 *Let $\mathbb{F}$ be a finite field of characteristic p, and let $V = \mathbb{F}^n$ be an n-dimensional vector space over $\mathbb{F}$. Suppose that for the subgroups H, $K < GL(n,\mathbb{F})$ there is an algebra isomorphism $\phi : \mathbb{F}[V]^H \cong \mathbb{F}[V]^K$ fixing $\mathcal{D}^*(n)$. Then H is conjugate to K in $GL(n,\mathbb{F})$.*

Proof. We can extend ϕ to an isomorphism of field extensions $\mathbb{F}(V)^H \cong \mathbb{F}(V)^K$ of $FF(\mathcal{D}^*(n))$. The result now follows from the next lemma, taking $\mathbb{D} = FF(\mathcal{D}^*(n))$, $\mathbb{K} = \mathbb{F}(V)$: ■

Lemma 9 *Suppose there is a lattice of field extensions*



such that $\mathbb{K}$ *is a finite Galois extension of each of the other three fields. Suppose there is a field isomorphism* $\sigma : F_1 \longrightarrow F_2$ *fixing* $\mathbb{D}$*. Then* $Gal(\mathbb{K}/F_1)$ *is conjugate to* $Gal(\mathbb{K}/F_2)$ *in* $Gal(\mathbb{K}/\mathbb{D})$*.*

Proof. Let $Gal(\mathbb{K}/F_i) = G_i$ for each i. $\mathbb{K}$ is a finite Galois extension of $\mathbb{D}$, so there is a primitive element $\alpha \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{D}(\alpha) = \mathbb{D}[\alpha]$. Since $\mathbb{D}$ is contained in F_i for $i = 1, 2$ it follows that $\mathbb{K} = F_i(\alpha) = F_i[\alpha]$ for each i. Thus every element a of $\mathbb{K}$ can be written as a polynomial in α with coefficients in F_1, $a = \sum_{j=0}^{|G_1|} a_j \alpha^j$, $a_j \in F_1$ for all j. We extend σ to a $\mathbb{K}$-automorphism via

$$\sigma : a = \sum a_j \alpha^j \mapsto \sum \sigma(a_j)\alpha^j,$$

calling this map σ also by abuse of notation. (This is a $\mathbb{K}-$automorphism as $|G_1| = [\mathbb{K}/F_1] = [\mathbb{K}/F_2] = |G_2|$ by the tower law). As σ fixes $\mathbb{D}$, it is an element of $Gal(\mathbb{K}/\mathbb{D})$. Then G_1 is conjugate to G_2 via the map

$$g_1 \mapsto \sigma^{-1} g_1 \sigma$$

for all $g_1 \in G_1$, which has inverse $g_2 \mapsto \sigma g_2 \sigma^{-1}$. ■

It follows from Lemma 7 that a $\mathcal{P}^*$-algebra isomorphism automatically fulfills the condition of Proposition 8, taking if necessary a scalar multiple so that the $\lambda \in \mathbb{F}$ occurring in the proof of 8 is 1. Thus the unstable $\mathcal{P}^*$-algebra structure of $\mathbb{F}[V]^G$ determines the representation of the group G, up to conjugate representations.

Suppose that we have two groups, G_1 and G_2 say, with the property that $\mathbb{F}[V]^{G_1} \cong \mathbb{F}[V]^{G_2}$ as *modules* over $\mathcal{D}^*(n)$ and over $\mathcal{P}^*$. One might then expect this to imply $\mathbb{F}[V]^{G_1} \cong \mathbb{F}[V]^{G_2}$ as graded algebras, and thus there to be an isomorphism of groups, as $\mathcal{D}^*(n)$ is 'large' in $\mathbb{F}[V]^{G_i}$, and the $\mathcal{P}^*$-module structure is restrictive, determining the q-th powers; in other words that the structure of $\mathbb{F}[V]^G$ over $\mathcal{D}^*(n)$ and $\mathcal{P}^*$ determines the group representation. Surprisingly, this is not true, even in the non-modular case:

Proposition 10 *Let $\mathbb{F}$ be a finite field of characteristic p, and let $V = \mathbb{F}^n$ be an n-dimensional vector space over $\mathbb{F}$. Suppose H, $K < GL(n, \mathbb{F})$ are pointwise conjugate subgroups such that $p \nmid |H|, |K|$. Then*

$$\mathbb{F}[V]^H \cong \mathbb{F}[V]^K$$

as modules over $\mathcal{D}^*(n)$ and over $\mathcal{P}^*$.

Proof. Note that we are in the non-modular case, where the image of the transfer map is surjective (see e.g. [22] Chapter 2, [14]). In other words,

$$\mathbb{F}[V]^H = e_H\mathbb{F}[V] \quad \text{and} \quad \mathbb{F}[V]^K = e_K\mathbb{F}[V]$$

From part (c) of Theorem 3 we know that there is some element a of $\mathbb{F}(GL(n, \mathbb{F}))$ such that $e_H = a^{-1}e_K a$, i.e. $ae_H = e_K a$. Define

$$\phi : \mathbb{F}[V]^H \longrightarrow \mathbb{F}[V]^K$$

by $y \longmapsto ay$. We claim this is the required $\mathcal{D}^*(n)$- and $\mathcal{P}^*$-module isomorphism.

First, if $y \in \mathbb{F}[V]^H$, then $y = e_H x$ for some $x \in \mathbb{F}[V]$. Thus

$$\phi(y) = ay = ae_H x = e_K ax \in e_K\mathbb{F}[V] = \mathbb{F}[V]^K.$$

Now suppose $d \in \mathcal{D}^*(n)$. d commutes with every element of $GL(n, \mathbb{F})$, so it also commutes with a, a linear combination of such elements. So

$$\phi(dy) = ady = day = d\phi(y).$$

Furthermore ϕ is clearly additive, so it is a $\mathcal{D}^*(n)$-module homomorphism. Elements of $\mathcal{P}^*$ commute with a just as the elements of $\mathcal{D}^*(n)$; replace $d \in \mathcal{D}^*(n)$ with $d \in \mathcal{P}^*$ and it follows that ϕ is also a $\mathcal{P}^*$-module homomorphism. Finally ϕ is invertible via $z \longmapsto a^{-1}z$, so it is in fact an isomorphism. ∎

Thus if we have two groups which are pointwise conjugate but not isomorphic, then their invariant rings are isomorphic as modules over $\mathcal{P}^*$ and $\mathcal{D}^*(n)$, but *not* as algebras over $\mathcal{D}^*(n)$. Furthermore, the converse is also true:

Theorem 11 *Let $\mathbb{F}$ be a field of characteristic p, and let $V = \mathbb{F}^n$ be an n-dimensional vector space over $\mathbb{F}$. Let H, $K < GL(n, \mathbb{F})$ be subgroups such that $p \nmid |H|, |K|$. Suppose that $\mathbb{F}[V]^K$ is isomorphic to $\mathbb{F}[V]^H$ as $\mathcal{P}^*$-modules. Then K is pointwise conjugate to H.*

Proof. Consider the direct sum decomposition of $\mathbb{F}[V]$:

$$\mathbb{F}[V] \cong e_H \cdot \mathbb{F}[V] \oplus (1 - e_H) \cdot \mathbb{F}[V], \qquad (\#)$$

where $e_H = \frac{1}{|H|} \sum_{h \in H} h$ is the group idempotent defined in Section 2. This is a direct sum of unstable $\mathcal{P}^*$-modules, as the Steenrod operations commute with elements of the group ring $\mathbb{F}(H)$. Furthermore,

$$e_H \cdot \mathbb{F}[V] = \mathbb{F}[V]^H$$

as noted in the proof of Theorem 3, so if $\phi : \mathbb{F}[V]^H \longrightarrow \mathbb{F}[V]^K$ is the module isomorphism, ϕ maps $e_H \cdot \mathbb{F}[V]$ to $e_K \cdot \mathbb{F}[V]$ where e_K is the group idempotent for K. $\mathbb{F}[V]$ is an injective object in the category $\mathcal{U}'$ of unstable modules over $\mathcal{P}^*$ (see [13]), and the Krull-Schmidt-Azumaya Theorem ([4] Theorem 3, p.22) states that an injective object in a locally noetherian category is a unique direct sum of (injective) indecomposibles, that is, of objects not expressible as a non-trivial direct sum. The category $\mathcal{U}'$ is locally noetherian ([20] Theorem 1.8.1), so

$$\mathbb{F}[V] \cong \bigoplus_{E \in \mathcal{I}} E^{\oplus a_E}$$

where $\mathcal{I}$ is a set of isomorphism class representatives of indecomposible injective $\mathcal{P}^*$-modules, and the a_E are cardinals. As $\mathbb{F}[V]$ is finite dimensional in each degree, each a_E is in fact an integer, so the isomorphism $\phi : e_H \cdot \mathbb{F}[V] \cong e_K \cdot \mathbb{F}[V]$ and the decomposition $(\#)$ imply that $(1-e_H) \cdot \mathbb{F}[V] \cong (1-e_K) \cdot \mathbb{F}[V]$. Call this map ϕ', and let $\chi : \mathbb{F}[V] \longrightarrow \mathbb{F}[V]$ be the isomorphism induced by the sum of ϕ and ϕ' on the direct summands of $\mathbb{F}[V]$. Thus χ is invertible, $\chi|_{\mathbb{F}[V]^H} = \phi$, and $\chi^{-1}|_{\mathbb{F}[V]^K} = \phi^{-1}$.

An endomorphism of unstable $\mathcal{P}^*$-algebras from $\mathbb{F}[V]$ to itself is determined by its behaviour in degree 1. At this degree, any map is the dual to a linear map $V \longrightarrow V$, so the map $End(V) \longrightarrow End_{\mathcal{K}'}(\mathbb{F}[V])$, $\alpha \longmapsto \alpha^*$ is a bijection, where $\mathcal{K}'$ denotes the category of unstable algebras over $\mathcal{P}^*$. Note that $End(V) = M_n(\mathbb{F})$, the multiplicative semi-group of $n \times n$ matrices over $\mathbb{F}$.

Theorem 6.4 in the paper [13] and the remark above show that there are natural equivalences

$$End_{\mathcal{U}'}(\mathbb{F}[V]) \cong \mathbb{F}[End_{\mathcal{K}'}(\mathbb{F}[V])] \cong \mathbb{F}[End(V)].$$

Thus we can consider $\chi \in End_{\mathcal{U}'}(\mathbb{F}[V])$ as an element of the semi-group ring $\mathbb{F}[M_n(\mathbb{F})]$, acting on $\mathbb{F}[V]$ naturally. Let $\beta = e_K\chi - \chi e_H$, which is

also in $End_{\mathcal{U}'}(\mathbb{F}[V])$. We shall calculate the value of β on each of the direct summands in the decomposition (#), thus giving its value on $\mathbb{F}[V]$.

Suppose $x \in e_H\mathbb{F}[V]$, i.e. $x = e_H y$ for some $y \in \mathbb{F}[V]$. Then

$$\begin{aligned} \beta x &= (e_K\chi - \chi e_H)e_H y \\ &= e_K\chi e_H y - \chi e_H e_H y \\ &= \chi e_H y - \chi e_H y \\ &= 0, \end{aligned}$$

as $e_H^2 = e_{H,}$ and $\chi e_H y \in \mathbb{F}[V]^K$ is fixed by e_K (recall that $\chi|_{\mathbb{F}[V]^H} = \phi : \mathbb{F}[V]^H \longrightarrow \mathbb{F}[V]^K$).

For the other summand, let $x \in (1 - e_H)\mathbb{F}[V]$, $x = (1 - e_H)y$ for some $y \in \mathbb{F}[V]$. Then

$$\begin{aligned} \beta x &= (e_K\chi - \chi e_H)(1 - e_H)y \\ &= e_K\chi(1 - e_H)y - \chi e_H(1 - e_H)y \\ &= e_K(1 - e_K)z - 0 \qquad \text{for some } z \in \mathbb{F}[V], \\ &= 0, \end{aligned}$$

as $e_H(1 - e_H) = 0 = e_K(1 - e_K)$, and $\chi|_{(1-e_H)\mathbb{F}[V]} : (1 - e_H)\mathbb{F}[V] \longrightarrow (1 - e_K)\mathbb{F}[V]$. Thus $\beta \equiv 0$ on each summand, hence on the whole of $\mathbb{F}[V]$. As β corresponds to the zero map in $End_{\mathcal{U}'}(\mathbb{F}[V])$, it must correspond to the zero map in $\mathbb{F}[End(V)] = \mathbb{F}[M_n(\mathbb{F})]$. So as a formula in $\mathbb{F}[M_n(\mathbb{F})]$,

$$\beta = e_K\chi - \chi e_H = 0,$$

so $e_K\chi = \chi e_H$, and $\chi^{-1}e_K\chi = e_H$.

The claim of the Theorem now follows either from the following Lemma, or by returning to the proof of Theorem 3. Examining the proof of (c) $\Longrightarrow$ (b), we see that it is not necessary for e_H and e_K to be conjugate in $\mathbb{F}[GL(n, \mathbb{F})]$; it is sufficient for them to be conjugate in $\mathbb{F}[M_n(\mathbb{F})]$, as the map $\psi : \mathbb{F}(G) \cdot e_H \longrightarrow \mathbb{F}(G) \cdot e_K$ given by $\psi(xe_H) = xe_H\chi = x\chi^{-1}e_K$ is a left $\mathbb{F}(G)$-module isomorphism for $\chi \in \mathbb{F}[M_n(\mathbb{F})]$ as long as $\chi^{-1}e_K\chi = e_H$. Thus part (b) of Theorem 3 holds, and H and K are pointwise conjugate in $GL(n, \mathbb{F})$ as claimed. ■

Thus two invariant rings are isomorphic as modules over $\mathcal{P}^*$ precisely when the corresponding groups are pointwise conjugate in $GL(n, \mathbb{F})$.

Note that the last step in the above proof gives a special case of the following Lemma, due to Larry Smith, which I cannot resist including:

Lemma 12 *Suppose two elements* $\alpha, \beta \in \mathbb{F}[GL(n,\mathbb{F})]$ *are conjugate in* $\mathbb{F}[M_n(\mathbb{F})]$. *Then they are conjugate in* $\mathbb{F}[GL(n,\mathbb{F})]$.

Proof. Consider the map $\eta : M_n(\mathbb{F}) \to GL(n,\mathbb{F})$ given by

$$\eta(M) = \begin{cases} M & \text{if } M \in GL(n,\mathbb{F}) \\ 0 & \text{otherwise.} \end{cases}$$

This is in fact a homomorphism of semi-groups, as if M is not invertible neither are MN or NM for any matrix N. We shall call the ring homomorphism induced on the semi-group algebras η also, by abuse of notation.

$$\eta : \mathbb{F}[M_n(\mathbb{F})] \to \mathbb{F}[GL(n,\mathbb{F})].$$

Suppose that for $\chi \in \mathbb{F}[M_n(\mathbb{F})]$,

$$\chi\alpha\chi^{-1} = \beta.$$

Then applying η,

$$\eta(\chi)\eta(\alpha)\eta(\chi)^{-1} = \eta(\beta).$$

But $\eta(\alpha) = \alpha$, $\eta(\beta) = \beta$, and $\eta(\chi) \in \mathbb{F}[GL(n,\mathbb{F})]$, so

$$\eta(\chi)\alpha\eta(\chi)^{-1} = \beta$$

shows that α and β are conjugate in $\mathbb{F}[GL(n,\mathbb{F})]$ as claimed. ■

6 Cohomology

In this section we shall give general constructions of topological spaces which have cohomology rings isomorphic as modules over the *topological* Steenrod algebra $\mathcal{A}_p$, but not as algebras over $\mathcal{A}_p$. In order to do this, we shall apply the results of the previous sections to cohomology rings which have the structure of rings of invariants.

Note that the results mostly stated here for $\mathcal{A}_p$ also hold for it's natural extension $\mathcal{A}_q$, where q is a power of p. See [5] for details.

6.1 Examples

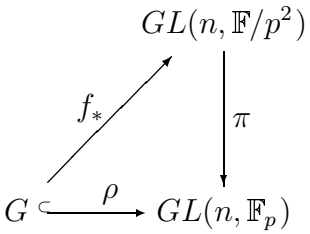
Let $G \overset{\rho}{\hookrightarrow} GL(n, \mathbb{F}_p)$ be a faithful representation of the finite group G over the field $\mathbb{F}_p = \mathbb{Z}/p$, whereby $p \nmid |G|$. We want to lift ρ to a representation of G over the p-adic integers $\mathbb{Z}_p$. We shall proceed step by step, lifting ρ to $GL(n, \mathbb{F}_{p^r})$ for successive values of r.

For a group H let BH denote the classifying space of H. $B-$ is a functor, so applying it to our representation we get $BG \overset{B\rho}{\hookrightarrow} BGL(n, \mathbb{F}_p)$. Consider the following lifting problem:

$$\begin{array}{ccc} & & BGL(n, \mathbb{F}/p^2) \\ & \overset{?f}{\nearrow} & \Big\downarrow B\pi \\ BG & \xrightarrow{B\rho} & BGL(n, \mathbb{F}_p) \end{array}$$

where $B\pi$ is the map induced from $\pi : GL(n, \mathbb{Z}/p^2) \longrightarrow GL(n, \mathbb{F}_p)$, reduction mod p. The kernel of π is a finite p-group K, and the map $B\pi$ is a fibration with fibre BK. According to obstruction theory, there is a lift f if and only if a series of elements in $H^i(BG; \pi_{i-1}(BK))$ vanish. As $\pi_j(BK) = \begin{cases} K & \text{if } k = 1 \\ 0 & \text{otherwise,} \end{cases}$ the only obstruction can be in $H^2(BG; K)$. From the cohomology of groups, we know that $H^*(BG; K) = H^*(G; K)$ is annihilated by $|G|$. On the other hand, K is a finite p-group, so some power of p annihilates $H^*(BG; K)$ for $* > 0$. As $(p, |G|) = 1$ it follows that $H^2(BG; K) = 0$, and there is no obstruction. Consider the map f induces

on fundamental groups:



This shows that $f_* := \rho_2$ lifts ρ to $GL(n, \mathbb{Z}/p^2)$.

We can repeat this argument inductively; suppose given $\rho_k : G \hookrightarrow GL(n, \mathbb{Z}/p^k)$ lifting ρ. The map $\pi_k : GL(n, \mathbb{Z}/p^{k+1}) \longrightarrow GL(n, \mathbb{Z}/p^k)$ has as kernel a finite p-group, and the rest of the steps are carried out exactly as above, lifting ρ_k to $\rho_{k+1} : G \hookrightarrow GL(n, \mathbb{Z}/p^{k+1})$.

Taking the limit of this construction, we obtain a lift of ρ into the p-adic integers $\rho_\infty : G \hookrightarrow GL(n, \mathbb{Z}_p)$ as required.

From [9] we know that

$$H^*(K(\mathbb{Z}_p^n, 2); \mathbb{F}_p) = \mathbb{F}_p[x_1, \cdots, x_n]$$

where $K(\mathbb{Z}_p^n, 2)$ denotes the Eilenberg-MacLane space, and $\mathbb{F}_p[x_1, \cdots, x_n]$ is the $\mathbb{F}_p$-algebra of polynomials in generators x_i of degree 2. Identifying G with its image in $GL(n, \mathbb{Z}_p)$ we have an action of G on $\mathbb{Z}_p^n$, hence on $K(\mathbb{Z}_p^n, 2)$, which passes to its cohomology ring. This action is natural, and so coincides with our usual action of G on the polynomial ring, except for the doubling of degrees. Following Clark and Ewing, define

$$X = X(G, p, n) := K(\mathbb{Z}_p^n, 2) \times_G EG,$$

where EG is the total space of a universal bundle for G.

Proposition 13 *[9] If p does not divide the order of G, $H^*(X; \mathbb{F}_p)$ is the subalgebra of invariants of $H^*(K(\mathbb{Z}_p^n, 2); \mathbb{F}_p)$ under the action of G. In other words, $H^*(X; \mathbb{F}_p) \cong \mathbb{F}_p[x_1, \cdots, x_n]^G$.*

Equally, we can easily extend this result to $\mathbb{F}_q$, where $q = p^s$, as

$$\begin{aligned} H^*(K(\mathbb{Z}_p^n, 2); \mathbb{F}_q) &= \mathbb{F}_q \otimes_{\mathbb{F}_p} H^*(K(\mathbb{Z}_p^n, 2); \mathbb{F}_p) \\ &= \mathbb{F}_q \otimes_{\mathbb{F}_p} \mathbb{F}_p[x_1, \cdots, x_n] \\ &= \mathbb{F}_q[x_1, \cdots, x_n], \end{aligned}$$

and from [2] p.95

$$\mathbb{F}_q \otimes_{\mathbb{F}_p} \mathbb{F}_p[V]^G \cong \mathbb{F}_q[V]^G.$$

Thus for pointwise conjugate representations of groups G_1, G_2 in $GL(n, \mathbb{F}_q)$, the topological spaces $X_1 = X(G_1, p, n)$ and $X_2 = X(G_2, p, n)$ have $\mathbb{F}_q$-cohomology rings which are isomorphic as modules over $\mathcal{A}_p$. If $G_1 \ncong G_2$, their invariant rings are not isomorphic as algebras over $\mathcal{A}_p$, so the cohomology of X_1 and X_2 are not the same.

6.2 Polynomial tensor exterior algebras

Let $\mathbb{F}$ be a Galois field of characteristic p, and consider the n-dimensional vector space $V = \mathbb{F}^n$ as an additive group. Then the (topological) classifying space BV has mod p cohomology ring $H^*(BV) \cong \mathbb{F}[V] \otimes \Lambda(V)$, where $\mathbb{F}[V]$ is the polynomial ring defined above (with algebra generators $x_1, \ldots, x_n$ in degree 2 dual to a basis of V) and $\Lambda(V)$ is an exterior algebra on generators $dx_1, \ldots, dx_n$ in degree 1. (See [7]). Considering $H,\ K \subset GL(n, \mathbb{F}) = Aut(V)$, we obtain $\mathbb{F}[V]^H$ and $\mathbb{F}[V]^K$ as subalgebras of $\mathbb{F}[V] \subset H^*(BV)$, and H and K act naturally on $H^*(BV)$, the action commuting with that of $\mathcal{A}_q$. We can extend Proposition 10 to this case:

Corollary 14 *Let $\mathbb{F}$ be a finite field of characteristic p, with $q = p^s$ elements, and let $V = \mathbb{F}^n$ be an n-dimensional vector space over $\mathbb{F}$. Suppose $H,\ K < GL(n, \mathbb{F})$ are pointwise conjugate subgroups such that $p \nmid |H|, |K|$. Then*

$$H^*(BV)^H \cong H^*(BV)^K$$

as modules over $\mathcal{A}_q$.

Proof. In the same way as for $\mathbb{F}[V]^H$, the image of the transfer is surjective for $(\mathbb{F}[V] \otimes \Lambda(V))^H$, i.e.

$$(\mathbb{F}[V] \otimes \Lambda(V))^H \cong e_H \cdot (\mathbb{F}[V] \otimes \Lambda(V)).$$

The map $\phi : \mathbb{F}[V]^H \to \mathbb{F}[V]^K$ defined in the proof of 10 by $y \longmapsto ay$ where $a^{-1} e_K a = e_H$ extends to a map $\phi' : (\mathbb{F}[V] \otimes \Lambda(V))^H \to (\mathbb{F}[V] \otimes \Lambda(V))^K$, and the rest of the proof is identical. ■

From [15] and its extension [5] $H^*(BV)$ is an injective object in the category $\mathcal{U}$ of unstable modules over $\mathcal{A}_q$, and in the paper [1] it is shown that

$$End_{\mathcal{U}}(H^*(BV)) \cong \mathbb{F}[End_{\mathcal{K}}(H^*(BV))] \cong \mathbb{F}[End(V)],$$

where $\mathcal{K}$ denotes the category of unstable algebras over $\mathcal{A}_q$. The Krull-Schmitt-Azumaya Theorem also holds in $\mathcal{U}$ ([20] Thm. 3.11.7), so we can recycle the proof of Theorem 11 to get a 'topological' version:

Corollary 15 *Let $\mathbb{F}$ be a field of characteristic p, and let $V = \mathbb{F}^n$ be an n-dimensional vector space over $\mathbb{F}$. Let H, $K < GL(n, \mathbb{F})$ be subgroups such that $p \nmid |H|, |K|$. Suppose that $H^*(BV)^K$ is isomorphic to $H^*(BV)^H$ as $\mathcal{A}_q$-modules. Then K is pointwise conjugate to H.*

Using the following Theorem, number III.10.4 in [7], we can construct pairs of classifying spaces which are not homotopy equivalent, but which have mod p cohomology rings isomorphic as modules over the Steenrod algebra:

Theorem 16 *[7] Let G be an arbitrary group, M a G-module and K a subgroup of finite index such that $(G : K)$ is invertible in M. Then res^*, the map in cohomology induced by the restriction map, maps $H^*(G; M)$ isomorphically onto the G-invariants of $H^*(K; M)$. In particular, if K is a normal subgroup,*

$$res^* : H^*(G; M) \cong H^*(K; M)^{G/K}.$$

Let K be the abelian group $\mathbb{F}_p^n$, and G_i be a subgroup of $GL(n, \mathbb{F}_p)$, acting on the vector space $M = \mathbb{F}_p^n = V$ naturally with $p \nmid |G_i|$. Let $\tilde{G}_i$ be the semidirect product of K and G_i. Then $H^*(K; \mathbb{F}_p) \cong \mathbb{F}_p[V] \otimes \Lambda[V]$, a polynomial tensor exterior algebra, and $H^*(K; \mathbb{F}_p)^{\tilde{G}_i/K} \cong H^*(K; \mathbb{F}_p)^{G_i} \cong (\mathbb{F}_p[V] \otimes \Lambda[V])^{G_i}$. Thus taking the classifying space $B\tilde{G}_i$, we have

$$\begin{aligned} H^*(B\tilde{G}_i; \mathbb{F}_p) &\cong H^*(\tilde{G}_i; \mathbb{F}_p) \\ &\cong H^*(K; \mathbb{F}_p)^{G_i} \\ &\cong (\mathbb{F}_p[V] \otimes \Lambda[V])^{G_i}. \end{aligned}$$

As mentioned above, it is clear that $(\mathbb{F}_p[V] \otimes \Lambda[V])^{G_i} = e_{G_i} \cdot (\mathbb{F}_p[V] \otimes \Lambda[V])$ where $e_{G_i} = \frac{1}{|G_i|} \sum_{g \in G_i} g$, precisely as in the polynomial case. (In fact, res^* acts on $H^*(\tilde{G}_i; M)$ as $\sum_{g \in G_i} g$). Thus Corollary 14 implies that, given two pointwise conjugate groups G_1, $G_2 < GL(n, \mathbb{F}_q)$, the topological spaces $B\tilde{G}_1$ and $B\tilde{G}_2$ constructed above have cohomology rings isomorphic as modules over $\mathcal{A}_p$. If they were isomorphic as *algebras* over $\mathcal{A}_p$, then the subalgebras $(\mathbb{F}_q[V] \otimes 1)^{G_i} \cong \mathbb{F}_q[V]^{G_i}$ would be isomorphic as algebras, as an $\mathcal{A}_p$-algebra map preserves the natural gradings of $\mathbb{F}_q[V]$ and $\Lambda[V]$. Then 8 would imply that G_1 is conjugate to G_2 in $GL(n, \mathbb{F}_q)$, as the $\mathcal{A}_p$ action on the polynomial invariant ring is the same as that of $\mathcal{P}^*$. Thus choosing G_1 not conjugate to G_2 produces spaces $B\tilde{G}_1$ and $B\tilde{G}_2$ which have mod p cohomology not isomorphic as algebras over $\mathcal{A}_p$, (and which are hence not homotopy equivalent).

7 Modular Representations

7.1 Pointwise conjugacy

Let us finally turn to a more difficult situation, namely that when the characteristic of the field over which the representations are defined divides the order of the group. Let H be a finite group, and $\mathbb{F}$ a field of characteristic $p \neq 0$ such that $p \,|\, |H|$ (usually $\mathbb{F}$ will be taken to be a finite field). Let $\rho : H \hookrightarrow GL(n, \mathbb{F})$ be a faithful representation, and let us identify H with its image in $GL(n, \mathbb{F})$. This is called the *modular case*, and much of the machinery we used in the non-modular case can no longer be applied. In particular, the elements $e_H \in \mathbb{F}(H)$ introduced in Section 2 can no longer be defined, for:

$$e_H := \frac{1}{|H|} \sum_{h \in H} h$$

is not allowed, as $|H| = 0$ in $\mathbb{F}$. The transfer map $Tr^H : \mathbb{F}[V] \longrightarrow \mathbb{F}[V]^H$ defined by

$$Tr^H(x) := \sum_{h \in H} hx$$

is no longer surjective - in fact it never hits a power of one of the Dickson polynomials (see [14]). It is also however never identically zero (see [22] Lemma 11.5.2 and [14]), so it is natural to ask whether there is at least a connection between the images of the transfer for pointwise conjugate modular representations of groups, analog to that in the non-modular situation.

Let us thus examine the element $\widetilde{e}_H \in \mathbb{F}(H)$ defined by

$$\widetilde{e}_H := \sum_{h \in H} h,$$

as the image of the transfer is $\widetilde{e}_H \cdot \mathbb{F}[V] \subset \mathbb{F}[V]^H$. Unlike e_H, $\widetilde{e}_H$ is not an idempotent; in fact $\widetilde{e}_H \cdot \widetilde{e}_H = 0$! How much of Theorem 3 can be translated into this context?

Unfortunately, almost nothing. Recall the five conditions, equivalent in the non-modular case with $char(\mathbb{F}) \neq 2$, expressed for $\widetilde{e}_H$ and $\widetilde{e}_K$:

(a) $H, K < G$ are pointwise conjugate,

(b) $Ind_H^G(1_H) \cong Ind_K^G(1_K)$ as $\mathbb{F}(G)$-modules,

(c) the idempotents $\widetilde{e}_H = \sum_{h\in H} h$, $\widetilde{e}_K = \sum_{k\in K} k$ are conjugate in the group ring $\mathbb{F}(G)$,

(d) there are elements ζ and ξ in $\mathbb{F}(G)$ such that: $\widetilde{e}_H = \zeta\widetilde{e}_K\xi\widetilde{e}_H$ and $\widetilde{e}_K = \xi\widetilde{e}_H\zeta\widetilde{e}_K$,

(e) $\widetilde{e}_H - \widetilde{e}_K \in [\mathbb{F}(G), \mathbb{F}(G)]$, where $[\mathbb{F}(G), \mathbb{F}(G)]$ denotes the vector space generated by all commutators in $\mathbb{F}(G)$.

Condition (e) is still equivalent to condition (a), as an easy modification of the proof in Chapter 1 shows:

Proof. (a)$\Longrightarrow$(e): As H and K are pointwise conjugate, for each $h \in H$ there is a $g_h \in G$ and $k \in K$ with

$$k = g_h h g_h^{-1}.$$

Thus

$$\widetilde{e}_H - \widetilde{e}_K = \sum_{h\in H} h - \sum_{k\in K} k = \sum_{h\in H}(h - g_h h g_h^{-1}),$$

which is clearly in the vector subspace S defined in Lemma 2, which is equal to $[\mathbb{F}(G), \mathbb{F}(G)]$.

(e)$\Longrightarrow$(a): Effectively the identical proof as in the non-modular case. ■

Condition (d) can immediately be seen never to hold, independently of the other conditions: for suppose there exist ζ and ξ in $\mathbb{F}(G)$ such that $\widetilde{e}_H = \zeta\widetilde{e}_K\xi\widetilde{e}_H$ and $\widetilde{e}_K = \xi\widetilde{e}_H\zeta\widetilde{e}_K$. Then

$$0 = \zeta\widetilde{e}_K\widetilde{e}_K = (\zeta\widetilde{e}_K)\widetilde{e}_K = (\zeta\widetilde{e}_K)\xi\widetilde{e}_H\zeta\widetilde{e}_K = (\zeta\widetilde{e}_K\xi\widetilde{e}_H)\zeta\widetilde{e}_K = \widetilde{e}_H\zeta\widetilde{e}_K,$$

so $\xi\widetilde{e}_H\zeta\widetilde{e}_K = \xi 0 = 0 \neq \widetilde{e}_K$, a contradiction.

Suppose that (a) holds. Then there is a counterexample to (b) for a pair of conformal groups in [10] p.255.

Finally consider condition (c), the most relevant, as it was the key to the important results in Section 5. Suppose that (c) does follow from (a). Examining the proof of Proposition 10, we see that it would then imply that $\widetilde{e}_H \cdot \mathbb{F}[V]$ is isomorphic to $\widetilde{e}_K \cdot \mathbb{F}[V]$ as modules over $\mathcal{P}^*$. This is *not* in general true, as the counterexample in the next section shows.

7.2 The image of the transfer: two examples

Let $\mathbb{F}$ be a field of characteristic 3. Define H to be the subgroup of $GL(3,\mathbb{F})$ generated by the matrices

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

These have order 3 and commute, so H is isomorphic to $C_3 \times C_3$, the direct product of two cyclic groups of order 3. Let $\langle A \rangle$ be the subgroup generated by A, and $Tr^{\langle A \rangle}$ the transfer map of this subgroup. H acts on $\mathbb{F}[x,y,z]$, which has an additive $\mathbb{F}-$basis consisting of monomials $x^a y^b z^c$ with $a,b,c \in \mathbb{Z}$. The image of such a monomial under $Tr^{\langle A \rangle}$ is as follows:

$$\begin{aligned} Tr^{\langle A \rangle}(x^a y^b z^c) &= \sum_{i=0}^{2} A^i(x^a y^b z^c) \\ &= \sum_{i=0}^{2} A^i(x)^a A^i(y)^b A^i(z)^c \\ &= x^a y^b z^c + x^a (y+z)^b z^c + x^a (y-z)^b z^c \\ &= x^a z^c (y^b + (y+z)^b + (y-z)^b) \\ &= x^a z^c \left(3y^b + \sum_{i=0,\ldots,b-1:\ b-i \text{ even}} 2\binom{b}{i} y^i z^{b-i} \right) \\ &= -x^a z^c \left(\sum_{i=0,\ldots,b-1:\ b-i \text{ even}} \binom{b}{i} y^i z^{b-i} \right) \end{aligned}$$

as $char(\mathbb{F})$ =3, and when $b-i$ is odd, the terms containing z^{b-i} and $(-z)^{b-i}$ cancel each other out. When $b = 0$ or 1, this is 0; when $b = 2$, the image is $-x^a z^c (z^2)$, so the ideal of $\mathbb{F}[x,y,z]^{\langle A \rangle}$ generated by z^2 is contained in $im(Tr^{\langle A \rangle})$, as for any group G Tr^G is an $\mathbb{F}[V]^G$-module homomorphism.

As $b-i$ is always nonzero and even in the expression above, we see that z^2 divides $Tr^{\langle A \rangle}(x^a y^b z^c)$ for any monomial; thus $im(Tr^{\langle A \rangle}) = (z^2)$, the principal ideal of $\mathbb{F}[x,y,z]^{\langle A \rangle}$ generated by z^2. It is easy to calculate the invariant ring of $\langle A \rangle$: to wit

$$\mathbb{F}[x,y,z]^{\langle A \rangle} = \mathbb{F}[x, y(y^2 - z^2), z].$$

Recall that the transfer can also be defined relative to a subgroup: $Tr^G_K : \mathbb{F}[V]^K \longrightarrow \mathbb{F}[V]^G$, for $K < G$, via

$$Tr^G_K(f) := \sum_{g \in G/K} g(f),$$

where g runs over a set of representatives for left cosets of K in G. Thus $Tr^{\langle A\rangle} = Tr^{\langle A\rangle}_{id}$ in this terminology, and further

$$Tr^G(f) = Tr^G_K \cdot Tr^K(f)$$

for all $f \in \mathbb{F}[V]$. Applying this to our group H it follows that

$$im(Tr^H) = Tr^H_{\langle A\rangle}(im(Tr^{\langle A\rangle})).$$

Now $im(Tr^{\langle A\rangle}) = (z^2)$ and $\{id,\ B,\ B^2\}$ is a set of coset representatives, so any element of $im(Tr^H)$ is a linear combination of elements of the form

$$\begin{aligned} Tr^H_A(x^a y^b z^c z^2) &= \sum_{j=0}^{2} B^j(x^a y^b z^{c+2}) \\ &= y^b z^{c+2} \sum_{j=0}^{2} B^j(x)^a \quad \text{as } y, z \in \mathbb{F}[V]^H, \\ &= y^b z^{c+2}(x^a + (x+z)^a + (x-z)^a) \\ &= -y^b z^{c+2} \left(\sum_{i=0,\ldots,a-1:\ a-i \text{ even}} \binom{a}{i} x^i z^{a-i} \right) \end{aligned}$$

by the same calculation as above; thus $im(Tr^H) \subseteq (z^4)$, the principal ideal in $\mathbb{F}[V]^H$ generated by z^4. In fact,

$$Tr^H(x^2y^2) = Tr^H_{\langle A\rangle} \cdot Tr^{\langle A\rangle}(x^2y^2) = Tr^H_{\langle A\rangle}(x^2z^2) = z^4,$$

so $im(Tr^H) = \langle z^4 \rangle$. It is known that $\mathbb{F}[V]^H = \mathbb{F}[x^3 - xz^2,\ y^3 - yz^2,\ z]$ (see [22] Chap. 8), so we see that $im(Tr^H)$ is very thin in $\mathbb{F}[V]^H$.

Let K be the subgroup of $GL(n, \mathbb{F})$ generated by the matrices

$$T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

As

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \pm 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \pm 1 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \pm 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & \pm 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

we see that H and K are pointwise conjugate in $GL(n, \mathbb{F})$. However, the invariant ring of $\mathbb{F}[V]^K = \mathbb{F}[x, y, f]$, where $f = \prod_{g \in K} gz$ is a polynomial of degree 9 ([22] Chap. 8), so $\mathbb{F}[V]^K \ncong \mathbb{F}[V]^H$ even as graded $\mathbb{Z}$-modules. What about the images of the transfer?

Using brute force, we calculate the image of a monomial under the transfer for K:

$$\begin{aligned} Tr^K(x^a y^b z^c) &= \sum_{g \in K} g(x^a y^b z^c) \\ &= x^a y^b \sum_{i=0}^{2} g(z)^c \quad \text{as } x, y \in \mathbb{F}[V]^K \\ &= x^a y^b (z^c + (z+y)^c + (z-y)^c + (z+x)^c + (z-x)^c + \\ &(z+x+y)^c + (z+x-y)^c + (z-x+y)^c + (z-x-y)^c). \end{aligned}$$

Substituting for c (using a computer algebra programme!), we find that this polynomial is zero mod 3 for all $c < 8$, and equal to

$$x^a y^b (x^6 y^2 + x^4 y^4 + x^2 y^4)$$

for $c = 8$. Thus $im(Tr^K)$ contains no elements of degree less than 8, and $im(Tr^K) \ncong im(Tr^H)$ even as graded $\mathbb{Z}$-modules[2]. This example can be (fairly) easily generalised to larger characteristic, giving a family of counter-examples to (c) in Section 7.1.

The moral of all this is that pointwise conjugacy, like so many things, is only well behaved in the non-modular case.

[2]Note that these calculations correct some mistakes in [22] Chapter 11.

A Appendix: Small Conformal Groups

This is a small table giving all conformal groups of order less than 192, leaving out 128 as there are too many. On the verical axis is indicated the order of the groups, on the horizontal how many pairs, triples and so forth of conformal groups there are. Thanks to the computer algebra programme GAP:

$\lvert G\rvert$ \ n-tuples	$n=2$	3	4	5	6	7	8	9	10	Total
$\lvert G\rvert = 16$	1	2								8
27	2									4
32	2	3	4	1		1				41
48	5	3	1							23
54	3	1								9
64	4	5	3	2	2	1	1	2	2†	252
72	1									2
80	8	3	1							29
81	2	1		1						12
96	18	7	10	2	2	2	1	1	2	170
100	1									2
108	11	2								25
112	4	3	1							21
125	2									4
128	*	*	*	*	*	*	*	*	*	*
135	2									4
144	26	9	4							99
147	1									2
160	20	7	11	3	2	2	1	1	2	183
162	9	3	1	1		1				43
176	4	3	1							21
189	4	1								11

† There are also two 14-tuples, and one each of n-tuples for $n = 11, 12, 13, 16, 17, 20$ and 25 of groups of order 64.

For comparison, here is a list of the number of non-isomorphic groups of orders up to 190 (leaving out primes):

Order	Number
4	2
6	2
8	5
9	2
10	2
12	5
14	2
16	14
18	5
20	5
21	2
22	2
24	15
25	2
26	2
27	5
28	4
30	4
32	51
34	2
36	14
38	2
39	2
40	14
42	6
44	4
45	2
46	2
48	52
49	2
50	5

Order	Number
52	5
54	15
55	2
56	13
57	2
58	2
60	13
62	2
63	4
64	267
66	4
68	5
70	4
72	50
74	2
75	3
76	4
78	6
80	52
81	15
82	2
84	15
86	2
88	12
90	10
92	4
93	2
94	2
96	231
98	5
99	2

Order	Number
100	16
102	4
104	14
105	2
106	2
108	45
110	6
111	2
112	43
114	6
116	5
117	4
118	2
120	47
121	2
122	2
124	4
125	5
126	16
128	2328
129	2
130	4
132	10
134	2
135	5
136	15
138	4
140	11
142	2
144	197
146	2

Order	Number
147	6
148	5
150	13
152	12
153	2
154	4
155	2
156	18
158	2
160	238
162	55
164	5
165	2
166	2
168	57
169	2
170	4
171	5
172	4
174	4
175	2
176	42
178	2
180	37
182	4
183	2
184	12
186	6
188	4
189	13
190	4

Note e.g. that for groups of order p^3, p prime, 4 of the 5 non-isomorphic groups are pairwise conformal. The exception is of course C_{p^3}.

References

[1] J. F. Adams, J. H. Gunawardena, H. R. Miller, *The Segal conjecture for elementary abelian p-groups,* Topology 24 (1985), 435-460.

[2] A. Adem, R. J. Milgram, *Cohomology of Finite Groups,* Grundlehren der Mathematischen Wissenschaften vol. 309, Springer-Verlag, 1994.

[3] D. J. Benson, *Representations and Cohomology Vol. 1,* Cambridge Studies in Advanced Mathematics No. 30, Cambridge University Press 1991.

[4] N. Bourbaki, *Algébre,* Chapitre 10, Hermann, Paris 1980.

[5] D. Bourguiba, *Profondeur et algèbre de Steenrod,* Thèse, Université de Tunis 1997.

[6] R Brauer, *Über die Darstellung von Gruppen in Galoisschen Feldern,* Act. Sci. Ind. 195 (1935).

[7] K. S. Brown, *Cohomology of Groups,* Graduate Texts in Mathematics Vol. 87, Springer Verlag, 1982.

[8] Carmichael, *Introduction to the Theory of Groups of Finite Order*, Dover Publications, 1937.

[9] A. Clark, J. Ewing, *The realization of polynomial algebras as cohomology rings,* Pacific J. of Math. 67 (1974), 425-782.

[10] C. W. Curtis, I. Reiner, *Methods of Representation Theory - with applications to finite groups and orders* Vol. 1, Wiley-Interscience 1981.

[11] L. E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem,* Trans. of the Amer. Math. Soc. 12 (1911), 75-98.

[12] G. James, M. Liebeck, *Representations and Characters of Groups*, Cambridge University Press, 1993.

[13] N. J. Kuhn, *Generic representations of the finite general linear groups and the Steenrod algebra: 1,* Amer. J. Math. 116 (1993), 327-360.

[14] K. Kuhnick, *Der Transferhomomorphismus in modularen Invariantentheorie,* Diplomarbeit, Göttingen 1998.

[15] J. Lannes, S. Zarati, *Sur les $\mathcal{U}$-injectifs,* Ann. Scient. Ec. Norm. Sup. 19 (1987), 25-59.

[16] J. Martino, S. Priddy, *Stable homotopy classification of* $BG_p^{\hat{}}$, Topology 34 (1995), 633-649.

[17] G. A. Miller, H. F. Blichfeldt, Cooper, *Theory and Applications of Finite Groups*, Wiley, 1916.

[18] M. D. Neusel, *The inverse invariant theory problem and Steenrod operations,* Memoirs of the AMS (to appear).

[19] R. Scapellato, *Finite groups with the same number of elements of each order*, Rendiconti di Matematica, Serie VII Vol. 8, Roma (1988), 339-344.

[20] L. Schwartz, *Unstable Modules over the Steenrod Algebra and Sullivan's Fixed Point Set Conjecture,* University of Chicago Press, 1994.

[21] J.-P. Serre, *Linear Representations of Finite Groups,* Graduate Texts in Mathematics No. 42, Springer-Verlag 1977.

[22] L. Smith, *Polynomial Invariants of Finite Groups*, A. K. Peters, 1995.

[23] L. Smith, *Variations on a theorem of Haynes R. Miller and a functor of Jean Lannes,* Preprint, Göttingen 1998/1999.