BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 34, Number 3, July 1997, Pages 211–250
S 0273-0979(97)00724-6

POLYNOMIAL INVARIANTS OF FINITE GROUPS A SURVEY OF RECENT DEVELOPMENTS

LARRY SMITH

ABSTRACT. The polynomial invariants of finite groups have been studied for more than a century now and continue to find new applications and generate interesting problems. In this article we will survey some of the recent developments coming primarily from algebraic topology and the rediscovery of old open problems.

It has been almost two decades since the *Bulletin of the AMS* published the marvelous survey article [111] of R. P. Stanley. Since then the invariant theory of finite groups has taken on a central role in many problems of algebraic topology, such as e.g. [22], [2], [101], [65], [105], [84], [106] chapter 11, and the references there. It has received new impetus as a subject of study in its own right, [72]–[81], [3], [43], and several textbooks with varying viewpoints [9], [114], and [106], as well as a reprint of venerable old lecture notes [48], have recently appeared. In this survey article I will try to discuss some of these developments as seen through the eyes of one who came to the subject from algebraic topology. That means that finite groups and finite fields will play a central role, and the modular case, i.e. where the characteristic of the field divides the order of the group, will play (in contrast to [111]) an important part.

Generally speaking, invariant theory is concerned with the action of groups on rings and the *invariants* of the action, e.g. the fixed subring and related objects. Here we will restrict ourselves to the actions of finite linear groups on polynomial rings. To be more specific, fix a field $\mathbb{F}$ to serve as ground field. For a finite-dimensional vector space V over $\mathbb{F}$ we denote by $\mathbb{F}[V]$ the **algebra of homogeneous polynomial functions**[1] **on** V, which we define to be the symmetric algebra on V^*, the dual of V. In other words, the homogeneous component of $\mathbb{F}[V]$ of degree m, denoted by $\mathbb{F}[V]_m$ (see [31] §1.5 or [106] chapter 4 for a discussion of gradings) is $S^m(V^*)$, the m-th symmetric power of V^*. With this grading linear forms have degree one. If you are a topologist, you may occasionally wish to double the degrees. If $z_1, \ldots, z_n \in V^*$ is a basis, we also denote $\mathbb{F}[V]$ by $\mathbb{F}[z_1, \ldots, z_n]$. The elements of $\mathbb{F}[z_1, \ldots, z_n]$ are just homogeneous polynomials in the linear forms $z_1, \ldots, z_n$ with coefficients in $\mathbb{F}$.

It is often convenient to think of the elements of the polynomial algebra $\mathbb{F}[V]$ as being functions. There is a problem if $\mathbb{F}$ is a Galois field of characteristic p, since it

Received by the editors January 3, 1997.
1991 *Mathematics Subject Classification.* Primary 13A50; Secondary 55S10.
Key words and phrases. Polynomial invariants of finite groups.

[1]We will have no occasion in this article to work with nonhomogeneous polynomials in $\mathbb{F}[V]$. Occasionally we refer to elements of $\mathbb{F}[V]$ as **forms** to emphasize they are homogeneous.

does not contain enough elements to separate the functions x^{p^k}, $k = 0, 1, \ldots$. The remedy is to allow the functions to take values in a larger field. A simple way to do this is to let $\overline{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$ and to define $\mathbb{F}[V]$ to be the subalgebra of the algebra of polynomial functions from $\overline{V} = V \otimes_{\mathbb{F}} \overline{\mathbb{F}}$ to $\overline{\mathbb{F}}$ generated by the linear forms defined over V, i.e. obtained from V^* by field extension.

Let G be a finite group and $\varrho : G \to \mathrm{GL}(n, \mathbb{F})$ a representation of G. Then G acts on the vector space $V = \mathbb{F}^n$ through linear transformations, and this may be extended to $\mathbb{F}[V]$ by the formula $(gf)(v) := f(\varrho(g^{-1})v)\ \forall v \in V$. One of the basic objects of study in invariant theory is the set of G-invariant polynomials $\mathbb{F}[V]^G := \{f \in \mathbb{F}[V] | gf = f\ \forall g \in G\}$. It is easy to see that the product and sum of two invariant polynomials is invariant and that a polynomial is invariant if and only if all its homogeneous components are invariant. Thus $\mathbb{F}[V]^G$ is also a graded algebra over $\mathbb{F}$ called **the ring of invariants** of ϱ (or if ϱ is clear from context, we suppress ϱ from the notation and speak of the ring of invariants of G). The algebra $\mathbb{F} \otimes_{\mathbb{F}[V]^G} \mathbb{F}[V] = \mathbb{F}[V]/J$, where J is the ideal if $\mathbb{F}[V]$ generated by all the homogeneous invariants of positive degree, is called the **ring of coinvariants** and is likewise a graded $\mathbb{F}$ algebra. Since $\mathbb{F}[V]^G \subseteq \mathbb{F}[V]$ is a finite extension (see e.g. [106] corollary 2.3.2), the algebra $\mathbb{F}[V]_G$ is **totally finite** in the sense that $\bigoplus_{t=0}^{\infty}(\mathbb{F}[V]_G)_i$ is a finite-dimensional $\mathbb{F}$-vector space.

If $\varrho : G \to \mathrm{GL}(n, \mathbb{F})$ is not faithful (i.e. if ϱ has a nonzero kernel), then ϱ induces a faithful representation $\varrho : H := G/\ker(\varrho) \hookrightarrow \mathrm{GL}(n, \mathbb{F})$. Clearly $\mathbb{F}[V]^G = \mathbb{F}[V]^H$, and so it is no loss of generality, and often simplifies the statement of results, to assume that ϱ is faithful, and we will do so without further comment.

Familiar examples of rings of invariants include the invariants of the **symmetric group** Σ_n acting in its tautological representation as a permutation group of $x_1, \ldots, x_n$. As is well known

$$\mathbb{F}[x_1, \ldots, x_n]^{\Sigma_n} = \mathbb{F}[e_1, \ldots, e_n],$$

where $e_1, \ldots, e_n$ are the elementary symmetric polynomials in $x_1, \ldots, x_n$. Less familiar are perhaps the invariants of the **alternating** group A_n in its tautological representation, where $\mathbb{F}[x_1, \ldots, x_n]^{A_n}$ is generated as an algebra by $e_1, \ldots, e_n$ and the polynomial ∇ obtained by summing all the elements of the A_n orbit of the monomial $x_1 \cdot x_2^2 \cdots x_{n-1}^{n-1}$. These polynomials are not algebraically independent: ∇^2 is a polynomial in $e_1, \ldots, e_n$. (If the characteristic of $\mathbb{F}$ is not two, we could replace ∇ by Δ, the discriminant (see [106] §1.3).)

A particularly interesting family of rings of invariants is provided by the representations $\sigma_k : \mathbb{Z}/2 \hookrightarrow \mathrm{GL}(2n, \mathbb{F})$, where σ_k maps the nonzero element of $\mathbb{Z}/2$ to the block matrix

$$\begin{bmatrix} 0 & 1 & & & & & \\ 1 & 0 & & 0 & & 0 & \\ & & 0 & 1 & & & \\ & 0 & 1 & 0 & 0 & & 0 \\ & & & & & & \\ \vdots & & \vdots & & \ddots & \vdots & \\ & & & & & 0 & 1 \\ 0 & & 0 & & \cdots & 1 & 0 \end{bmatrix} \in \mathrm{GL}(2k, \mathbb{F}).$$

This is just the k-fold direct sum of the tautological representation of $\mathbb{Z}/2 = \Sigma_2$ with itself. (For $k = 1$ we write σ for σ_1.) Another way to think about the invariant theory of these actions is to think of $\mathbb{Z}/2$ as acting on the polynomial

ring $\mathbb{F}[x_1, \ldots, x_k, y_1, \ldots, y_k]$ by permuting the vector variables $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$. Even though these are permutation representations, the structure of the invariant rings is strongly dependent on the characteristic of the ground field $\mathbb{F}$. If the ground field has characteristic 2, then these examples serve to show that almost all of the nice results of §1 and §2 can fail in the modular case (see §3).

Although **we will confine ourselves to the case of finite groups**, this is not meant to imply that the invariant theory of infinite groups is not interesting. Far from it; it is most interesting (see e.g. the DMV-Seminar [59]), but including it here would burst the confines of a survey and exceed my competence. This survey is divided into sections as follows:

Sections 1, 2, 4, and 5 are primarily concerned with tools and how they are used. Sections 3 and 6 are more concerned with results. The first section discusses the classical theorems of Hilbert, Molien and Noether and sets up much of the notation we need later. These results are all proved by means of the **transfer** homomorphism and its properties in the **nonmodular case**, i.e. when the characteristic of the ground field does not divide the order of the group. In the second section we introduce **orbit Chern classes** and show how they can be used to prove some of the more modern finiteness theorems for rings of invariants. In §3 we examine some basic finiteness problems that remain open. Until quite recently (see for example the papers of M.-J. Bertin [10], [11] and H. Nakajima [72]–[81]), apart from the many papers of L. E. Dickson [29], most work in invariant theory has assumed the ground field to be of characteristic zero, often the complex numbers. What little has been done for fields of nonzero characteristic has often taken place under the silent assumption that the characteristic is not a divisor of the group order. In §4 we first show that everything, apart from Noether's finiteness theorem and Hilbert's syzygy theorem, can go wrong in the **modular case**, i.e. when the characteristic of the ground field divides the group order. There are, however, compensations that make modular invariant theory interesting and exciting, since invariant theory over Galois fields offers strikingly new features. The first of these is the **Dickson algebra**, which we also introduce in §4. It is an algebra of *universal invariants*, that is, consists of polynomials present in all rings of invariants, and provides a universal system of parameters for rings of invariants over Galois fields. We use this to give a short proof of Noether's finiteness theorem in the modular case. A second new feature[2] is the **Steenrod algebra**, which we introduce in §5. It comes from algebraic topology and is a way to organize information derived from the Frobenius homomorphism (which is a fundamental new feature[3] of algebra over finite fields). It provides among other things a means of constructing new invariants from old ones and imposes an additional, very rigid structure on modular rings of

[2]Other new features are the ideals of stable invariants [54], [83] and the higher cohomology groups $H^*(G; \mathbb{F}[V])$ [3] (after all $\mathbb{F}[V]^G = H^0(G; \mathbb{F}[V])$).

[3]See also the fundamental paper of C. Peskine and L. Szpiro [91] for another way to employ the Frobenius.

invariants. Using these two new features, P. S. Landweber and R. E. Stong [62] formulated a conjecture concerning the depth (or homological codimension) of rings of invariants, which needs the Dickson algebra to be stated. They used Steenrod operations to verify their conjecture in many cases. Recently D. Bourguiba and S. Zarati, in [13], have proven a theorem about the Steenrod algebra that includes this conjecture as a special case. We describe the essence of their proof in the last section.

I have tried throughout to indicate the many open problems remaining in invariant theory. To avoid interrupting the flow of the exposition, much of the notation[4] used will be introduced as needed and explained in footnotes.

Acknowledgment

I would like to thank the many people who have helped me with criticism and suggestions for this survey, and in particular Mara D. Neusel for reading, correcting, and commenting on the many preliminary drafts, as well as for many fruitful discussions.

1. The transfer and the classical finiteness theorems

Finiteness questions have played an important role in invariant theory from the beginnings of the subject, and several different kinds of finiteness theorems—**structural, combinatorial** and **homological**—are part of the basic theory. Structural finiteness has come to mean that rings of invariants are Noetherian: indeed much of commutative algebra was developed to prove precisely this. Combinatorial finiteness concerns the rate of growth of the sequence of integers $\dim_{\mathbb{F}}(\mathbb{F}[V]_k^G)$, i.e. of the dimension of the space of homogeneous invariant polynomials $S^k(V^*)^G$ of degree k. These integers are encoded in the **Poincaré series**, defined[5] by

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

Homological finiteness is concerned with the length of syzygy chains and the finiteness of various homological dimensions one can associate to a ring of invariants.

Let us begin by considering structural finiteness: namely that a ring of invariants is finitely generated and finitely related. This was proven by D. Hilbert in certain cases[6] in [45] in a paper that broke completely new ground in invariant theory. Contrary to a popular belief, it did not settle all aspects of the finiteness problem, not even in the case of finite groups in the nonmodular case (see the discussion of Noether's bound in §3). The finiteness of the chain of relations among the relations

[4]The following standard notation will be used: $\mathbb{Z}$ for the ring of integers, $\mathbb{N}$ for the set of positive integers, and $\mathbb{N}_0$ for the set of nonnegative integers, $\mathbb{Q}$ for the rational numbers, $\mathbb{R}$ for the reals, and $\mathbb{C}$ for the complexes. If $f_1, \ldots, f_s \in \mathbb{F}[V]$, then perhaps less standard is the notation $\mathbb{F}[f_1, \ldots, f_s]$ to indicate that the subalgebra generated by $f_1, \ldots, f_s$ is a **polynomial algebra** in the elements $f_1, \ldots, f_s$, i.e. that $f_1, \ldots, f_s$ are algebraically independent.

[5]If M is a graded vector space over $\mathbb{F}$, we say M has **finite type** if each homogeneous component M_k, $k \in \mathbb{Z}$, is a finite-dimensional $\mathbb{F}$-vector space. We say M is **positively graded** if $M_k = 0$ for $k \notin \mathbb{N}_0$. The **Poincaré series** (also called the **Hilbert series** in much of the literature) of a graded vector space of finite type is defined to be the formal power series $P(M,t) = \sum \dim_{\mathbb{F}}(M_k) t^k$.

[6]It should perhaps be noted that Hilbert's proof precedes the introduction of vector spaces and *linear* representations. Much of nineteenth-century invariant theory was concerned with *projective* representations, because projective space was a familiar object, from complex analysis for example, and vector spaces, much less linear representations, had not yet been defined.

among...is a homological finiteness property and the start of homological algebra proper. This is also in Hilbert's paper.

That something really needs to be proved can be seen by considering the subalgebra of $\mathbb{F}[x, y]$ generated by the elements

$$1, xy, xy^2, \ldots, xy^n, \ldots .$$

Clearly no generator xy^n can be in the subalgebra generated by the remaining generators, since the product of any two other generators, and hence any polynomial in the other generators, that is divisible by y^n must be divisible by x^2. So there are subalgebras of $\mathbb{F}[x, y]$ that are not finitely generated.

D. Hilbert's proof [45] depends on a certain amount of commutative algebra that he developed[7] ad hoc. This was systematically expanded by E. Noether into the theory of commutative Noetherian rings and modules. There are many references for this material, e.g. [24], [31], [5], [6], [7] or the classic [115]. The proof of the finiteness theorem that follows is due to E. Noether [89]. It has been reworked many times; see e.g. [116] pp. 175–176, [96] and [109]. The basic tool we need is the **transfer**. If H is a subgroup of a finite group G and V is a finite-dimensional G-representation, the **relative transfer from H to G**, denoted by

$$\mathrm{Tr}_H^G : \mathbb{F}[V]^H \to \mathbb{F}[V]^G,$$

is defined by the formula

$$\mathrm{Tr}_H^G(f)(x) = \sum_{gH \in G/H} g(f)(x) = \sum_{gH \in G/H} f(g^{-1}(x)) \quad \forall x \in V.$$

The notation means that the sum runs over a set of left coset representatives of H in G. It is an easy calculation to show that for $f \in \mathbb{F}[V]^H$ and $g'H = g''H \in G/H$ that $g'f = g''f \in \mathbb{F}[V]^G$, so the right-hand side makes sense independent of the choice of elements in G representing the cosets G/H. Since

$$g' \cdot \mathrm{Tr}_H^G(f) = \sum_{g''H \in G/H} g'g''(f) = \sum_{g'g''H \in G/H} g'g''(f) = \mathrm{Tr}_H^G(f),$$

(if $\{g''H\}$ runs through all cosets exactly once, so does $\{g'g''H\}$ for a fixed g'), we see that $\mathrm{Tr}_H^G(f) \in \mathbb{F}[V]^G$. In general the transfer behaves badly with respect to products in $\mathbb{F}[V]^H$. However, $\mathbb{F}[V]^H$ is an $\mathbb{F}[V]^G$-module since $\mathbb{F}[V]^G$ is a subalgebra of $\mathbb{F}[V]^H$. Moreover[8],

$$\left.\begin{array}{l} \mathrm{Tr}_H^G(f) = |G : H| \cdot f \\ \mathrm{Tr}_H^G(f \cdot h) = f \cdot \mathrm{Tr}_H^G(h) \end{array}\right\} \quad f \in \mathbb{F}[V]^G, h \in \mathbb{F}[V]^H, \deg(h) > 0,$$

and therefore Tr_H^G is an $\mathbb{F}[V]^G$-module homomorphism.

The composite

$$\mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]^H \xrightarrow{\mathrm{Tr}_H^G} \mathbb{F}[V]^G$$

[7] Hilbert's **Basis Theorem**, *If A is a commutative Noetherian ring, then so is the polynomial ring $A[x]$*, with $A = \mathbb{C}$ appears as *Hilfssatz 1* (see also [48] lecture XXXV) and Hilbert's **Syzygy Theorem** as *Hilfssatz 2* in [45] (see also [48] lecture XLVII). These are the key to everything, but also the source of the **nonconstructive** nature of much of the theory.

[8] If X is any finite set, then $|X|$ denotes its cardinality. For a group G, and a subgroup $H \leq G$, $|G : H|$ denotes the index of H in G, i.e. the number of left cosets of H in G.

is equal to multiplication by $|G:H|$. In particular, if $|G:H|$ is invertible in $\mathbb{F}$, then the transfer is surjective, and the map

$$\pi_H^G = \frac{1}{|G:H|}\operatorname{Tr}_H^G : \mathbb{F}[V]^H \to \mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]^H,$$

called the **Reynolds operator**, is an idempotent projection[9] whose image is equal to $\mathbb{F}[V]^G$. In this case $\mathbb{F}[V]^H$ is a module direct summand of $\mathbb{F}[V]^G$ and the kernel of π_H^G. By contrast, the transfer is never surjective if the characteristic of $\mathbb{F}$ divides the order of G (see 4.1).

To summarize: the transfer has good properties almost exclusively when $|G:H|$ is invertible in $\mathbb{F}$. In particular, even in well-studied examples where the characteristic of $\mathbb{F}$ divides the order of G, it is only recently [36] (and the appendix to [37]) and [19] that the image of the transfer map $\operatorname{Tr}^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$ is beginning to be understood. We will return to this in sections §4 and §5.

Here is the first of the classical finiteness theorems [89]. Since the proof is so short and lovely, I cannot resist giving it in full.

Theorem 1.1 (D. Hilbert - E. Noether)**.** *Let V be a finite-dimensional representation of a finite group G and suppose that $|G|$ is invertible in $\mathbb{F}$. Then $\mathbb{F}[V]^G$ is finitely generated as an algebra.*

Proof. Consider the ideal $J \subset \mathbb{F}[V]$ generated by all the invariant polynomials of positive degree. Since the ring $\mathbb{F}[V]$ is Noetherian, the ideal J is finitely generated, and therefore we may choose finitely many invariant polynomials $h_1, \dots, h_m$ such that $J = (h_1, \dots, h_m)$. We are going to show that these polynomials generate $\mathbb{F}[V]^G$ as an $\mathbb{F}$-algebra.

So let $f \in \mathbb{F}[V]^G$. As always, f is homogeneous, and without loss of generality of positive degree. Then of course $f \in J$, so we may find polynomials $f_1, \dots, f_m \in \mathbb{F}[V]$ such that

$$f = f_1 h_1 + \cdots + f_m h_m.$$

The coefficients $f_1, \dots, f_m$ all have degree strictly smaller than the degree of f. If f is an element in $\mathbb{F}[V]^G$ of minimal positive degree, then the coefficients must be scalars, and f is a linear combination of $h_1, \dots, h_m$, so belongs to the subalgebra they generate. This allows us to proceed inductively and assume that all invariant polynomials of degree strictly smaller than that of f lie in the subalgebra of $\mathbb{F}[V]^G$ generated by $h_1, \dots, h_m$. The Reynolds operator applied to the preceding equation gives

$$f = \pi^G f = \pi^G(f_1 h_1 + \cdots + f_m h_m) = \pi^G(f_1)h_1 + \cdots + \pi^G(f_m)h_m,$$

since f and $h_1, \dots, h_m$ are invariant. By construction the polynomials $\pi^G(h_1), \dots, \pi^G(h_m)$ are also invariant, and of strictly lower degree than the degree of f, so all lie in the subalgebra of $\mathbb{F}[V]^G$ generated by $h_1, \dots, h_m$. Hence so does f, completing the inductive step. □

The theorem of Hilbert - Noether and its proof just presented are unsatisfactory for two reasons:

— the proof is *nonconstructive*; i.e. it provides no algorithm to compute a generating system of invariants, and

[9] If $H = 1$, we suppress it from the notation for the transfer and the associated projection when it is defined, i.e. if $|G| \in \mathbb{F}^\times$ (the nonzero elements of $\mathbb{F}$).

— it is *nonmodular* in character; i.e. it provides no information about the rings of invariants of finite groups when the characteristic of the ground field divides the order of the group.

Indeed, the proof does not extend to the modular case, and, moreover, invariant generators for the ideal J generated by the invariants of positive degree need not be generators for the ring of invariants [85].

There is also an enhancement due to E. Noether [89] (it is one of two proofs of the basic finiteness theorem in this remarkable paper) that is constructive in nature, offering an upper bound on the number and degrees of the generators required. In addition, when it applies, it yields an algorithm to compute a complete system of generating invariants. It has the disadvantage that it works only if the characteristic of the ground field is zero or strictly greater than the order of the group. Here is the relative form of the theorem: the proof of Barbara Schmid [96] theorem 1.1 easily extends to this case.

Theorem 1.2 (E. Noether)**.** *Let V be a finite-dimensional representation of a finite group G and $H \leq G$ a subgroup of G. If $|G:H|!$ is invertible in $\mathbb{F}$ and $\mathbb{F}[V]^H$ is generated by elements of degree at most m, then $\mathbb{F}[V]^G$ is generated by elements of degree at most $m \cdot |G:H|$.*

A proof of this result along with a discussion of the algorithm it uses can be found in [96] or [106] §2.4. The algorithm is not very efficient: it consists of computing degreewise all transfers up to degree $|G|$ and using these polynomials to generate the invariants. If you are wondering if the ! in the statement of the theorem is a misprint, it is not. Hidden in the proof is the symmetric group $\Sigma_{|G:H|}$, and it is the order of this group that needs to be inverted at a crucial point in the proof.

The upper bound on the degrees of a set of generating polynomials for the ring of invariants given by this theorem is known as **Noether's bound**. We discuss it in more detail in §3.

The basic combinatorial finiteness theorem for $\mathbb{F} = \mathbb{C}$ was established[10] one hundred years ago by T. Molien [71]. The proof again depends on the transfer and associated Reynolds operator.

Theorem 1.3 (T. Molien)**.** *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{C})$ be a representation of a finite group. Then the Poincaré series of the ring of invariants is given by*

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

and is a rational function of t. □

The formula says that the Poincaré series of $\mathbb{C}[V]^G$ is the average of the reciprocals of the characteristic polynomials of the elements of G. If $|G| \in \mathbb{F}^\times$ and we choose a Brauer lift of $\mathbb{F}^\times$ to identify the nonzero element of $\mathbb{F}$ with roots of unity, then the formula continues to hold and provides a means to compute the Poincaré series of rings of invariants in the nonmodular case.

Example 1. Consider the complex representation σ_2 of $\mathbb{Z}/2$ described in the introduction. The nontrivial element of $\mathbb{Z}/2$ has characteristic polynomial $(1 - t^2)^2$,

[10] Proofs of this result can be found in [9] §2.5, [49] §II.2, and [106] §4.4. They differ hardly at all from Molien's original proof.

so Molien's theorem tells us

$$P(\mathbb{C}[x_1,x_2,y_1,y_2]^{\mathbb{Z}/2},t) = \frac{1}{(1-t)^4} + \frac{1}{(1-t^2)^2} = \frac{1+t^2}{(1-t^2)^2(1-t)^2}$$
$$= 1 + 2t + 5t^2 + \cdots .$$

In particular the space of invariant quadratic polynomials is 5-dimensional. Clearly the polynomials $x_1y_1, x_2y_2, (x_1+y_1)^2, (x_2+y_2)^2$ are invariant, but to span $\mathbb{C}[x_1,x_2,y_1,y_2]_2^{\mathbb{Z}/2}$ over $\mathbb{C}$ we need the additional polynomial $x_1x_2 + y_1y_2$.

The representation σ_2 is just the direct sum $\sigma \oplus \sigma$, and the invariants $\mathbb{C}[x,y]^{\mathbb{Z}/2}$ of the representation σ are $\mathbb{C}[x+y, xy]$. Thus, knowing the invariants of the factors of a representation that decomposes into a direct sum does not yield the invariants of the direct sum in an obvious way. If the ground field is of characteristic zero, then **polarization** (see [116] chapter II, [96] §6, [106] §3.4, or the article by Kraft in [59]) leads to a construction of $\mathbb{F}[V_1 \oplus \cdots \oplus V_k]^G$ from the invariants of the factors.

In the modular case no analogous formula to 1.3 is known (see, however, [4] for a special case). Put another way, one can write down Molien's formula in the modular case using the regular elements in G and a Brauer lift; however, the resulting formula does not compute the Poincaré series of the ring of invariants, rather (see [100], §18.1 ix) the Poincaré series of the fixed point set in the projective cover of $\mathbb{F}[V]$.

For permutation representations the combinatorial situation can be developed in a characteristic free way. This conforms to the often-used paradigm that a permutation representation is a linear representation over the field with one element.

Suppose that G is a finite group and X a finite G-set, i.e. a finite set upon which G acts through permutations. Identifying the elements of X with a basis for the linear forms on the corresponding dual linear representation, we obtain an action of G on $\mathbb{F}[X]$ which sends monomials to monomials. The monomials of degree k are a basis for $\mathbb{F}[X]_k$, and hence $\mathbb{F}[X]_k$ is itself the linear representation associated to the permutation representation of G on the monomial basis. The elements of the monomial basis for $\mathbb{F}[X]_k$ may be identified with the elements in $\mathbb{SP}^k(X)$, the **k-th symmetric power** of the set X, which is defined to be the orbit space of the operation of the symmetric group Σ_k on the k-fold cartesian product $\times_k X$ of X with itself given by permuting coordinates. The action of G on X extends componentwise to $\times_k X$ where it commutes with the action of Σ_k. Hence G acts on $\mathbb{SP}^k(X)$, and we may identify $\mathbb{F}[X]_k$ with the linear representation associated to the permutation representation $\mathbb{SP}^k(X)$. For a permutation module V, the dimension of the fixed point set is given by the number of orbits of G on the set Y of elements being permuted, and the number of such orbits is given by the formula[11] of Burnside

$$|Y/G| = \frac{1}{|G|}\sum_{g\in G} |Y^g|.$$

If we replace Y by $\mathbb{SP}^k(X)$ in this formula, we see:

[11] In [106] page 89, the remark in the middle of the page: a TEX coding error led to a most unfortunate misprint in this formula.

Theorem 1.4. *Let G be a finite group acting on the finite set X and $\mathbb{F}$ a field. Then*

$$P(\mathbb{F}[X]^G, t) = \frac{1}{|G|} \sum_{n=0}^{\infty} \sum_{g \in G} |\mathbb{SP}^n(X)^g| t^n.$$

This formula is independent of the field $\mathbb{F}$. □

The first homological finiteness theorem, the syzygy theorem, was established by Hilbert loc. cit. (See for example [106] chapter 6 for a discussion of the syzygy theorem and its converse.) The more modern homological finiteness theorems had to wait upon the developments of commutative and homological algebra for their formulation. Recall that a sequence of elements $a_1, \ldots, a_n$ in a graded connected commutative algebra over $\mathbb{F}$ is called a **homogeneous system of parameters** if the quotient algebra $A/(a_1, \ldots, a_n)$ is totally finite, but none of the quotient algebras[12] $A/(a_1, \ldots, a_{i-1}, \widehat{a_i}, a_{i+1}, \ldots, a_n)$ are totally finite. A system of parameters[13] is always algebraically independent; and hence if A has a system of parameters, then it is a finite extension of a polynomial algebra. As references for systems of parameters we note [31] chapter 8, [69] chapter 5, or [106] chapter 5. These and other standard sources contain a proof of the following fundamental result. (See also §2 for a construction of a system of parameters for rings of invariants.)

Theorem 1.5 (Noether Normalization Theorem)**.** *Let A be a finitely generated graded connected algebra over a field $\mathbb{F}$. Then there exists a system of parameters for A, and the following integers are equal*:

(i) *the smallest integer r such that there exist r elements $a_1, \ldots, a_r \in A$ with $A/(a_1, \ldots, a_r)$ totally finite,*
(ii) *the largest integer s such that there exist s algebraically independent elements in A,*
(iii) *the length t of the longest strictly increasing chain*

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_t \subset A$$

of prime ideals in A.

The common value of the integer in (i), (ii), (iii) *is the Krull dimension of A.* □

If A is a finitely generated graded connected algebra over a field, we say that A is a **Cohen-Macaulay algebra** if there is a system of parameters $a_1, \ldots, a_n \in A$ such that A is a free $\mathbb{F}[a_1, \ldots, a_n]$-module. Luckily, Macaulay's theorem ([7] theorem 3.3.5 or [106] corollary 6.7.7) assures us that if one system of parameters has this property, then all systems of parameters do, and any system of parameters is a **regular sequence**[14] in A. Systems of parameters behave well vis a vis finite ring extensions, but regular sequences do not; see e.g. [106] §6.2 example 2.

---

[12] Using standard conventions from algebraic topology, a $\widehat{\ }$ over an element means that it is omitted from the list.

[13] Since we will have no occasion to deal with nonhomogeneous systems of parameters, we drop the adjective *homogeneous* in the sequel.

[14] If M is an A module and $a_1, \ldots, a_m$ belong to the augmentation ideal $\overline{A}$ of A, we say they are a **regular sequence** on M if a_1 is not a zero divisor on M and a_i is not a zero divisor on $M/a_1 \cdot M + \cdots a_{i-1} \cdot M$ for $i = 2, \ldots, m$. For properties of regular sequences see e.g. [31] §17, [98], chapter IV or [106] chapter 6.

If A is Cohen-Macaulay and $a_1, \ldots, a_n \in A$ is a system of parameters, then a basis for A as a module over $\mathbb{F}[a_1, \ldots, a_n]$ projects bijectively via the natural map

$$A \to \mathbb{F} \otimes_{\mathbb{F}[a_1,\ldots,a_n]} A =: QA$$

to a vector space basis for the **module of indecomposables** QA. The module QA is totally finite, and so there is an integer k such that all the homogeneous components $(QA)_i = 0$ if $i > k$. Therefore, if we can find such a k, then we obtain an upper bound for the degrees of a set of algebra generators for A by taking $\max\{\deg(a_1), \ldots, \deg(a_n), k\}$.

The following homological finiteness theorem not only will be of use in discussing permutation groups but is a major tool in the theory. Again, the Reynolds operator is the decisive tool.

Theorem 1.6 (J. A. Eagon and M. Hochster [51])**.** *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation of a finite group G over a field $\mathbb{F}$. If $|G|$ is prime to the characteristic of $\mathbb{F}$, then $\mathbb{F}[V]^G$ is a Cohen-Macaulay algebra.*

Proof. $\mathbb{F}[V]^G$ is Noetherian by 1.1. Let $f_1, \ldots, f_n \in \mathbb{F}[V]^G$ be a system of parameters. Then

$$\mathbb{F}[f_1, \ldots, f_n] \subseteq \mathbb{F}[V]^G \subseteq \mathbb{F}[V]$$

are finite extensions ([106] corollary 2.3.2 or [5] chapter 5 exercise 12 and corollary 5.4), so $f_1, \ldots, f_n \in \mathbb{F}[V]$ is a system of parameters. $\mathbb{F}[V]$ is Cohen-Macaulay, so by Macaulay's theorem $\mathbb{F}[V]$ is a free $\mathbb{F}[f_1, \ldots, f_n]$-module. The projection $\pi^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$ derived from the transfer is an $\mathbb{F}[V]^G$-module homomorphism and a fortiori an $\mathbb{F}[f_1, \ldots, f_n]$-module homomorphism. It splits the inclusion $\mathbb{F}[V]^G \subseteq \mathbb{F}[V]$, so $\mathbb{F}[V]^G$ is an $\mathbb{F}[f_1, \ldots, f_n]$-module direct summand in $\mathbb{F}[V]$ and therefore a projective $\mathbb{F}[f_1, \ldots, f_n]$-module. Since flat, projective and free agree for graded connected algebras over a field ([7] (appendix) theorem A.5.4 or [106] proposition 6.1.1), $\mathbb{F}[V]^G$ is a Cohen-Macaulay. □

The homological finiteness theorem 1.6 allows us to apply a divide-and-conquer strategy to describing a ring of invariants in the nonmodular case: namely

STEP 1 Choose a system of parameters $f_1, \ldots, f_n \in \mathbb{F}[V]^G$. These are called **primary generators** of $\mathbb{F}[V]^G$.

STEP 2 Find a basis $h_1, \ldots, h_m$ for $\mathbb{F}[V]^G$ as a module (it is free, remember) over $\mathbb{F}[f_1, \ldots, f_n]$. These are called **secondary generators**.

From the point of view of efficiency of computation it is important to minimize the number of secondary generators. For an excellent example of how the choice of a system of parameters can affect the outcome of a computation see [32] example 4.2.

In §4 we will see examples to show that 1.6 is false in the modular case, which leads to some of the most interesting new developments in modular invariant theory (see [13] and the discussion of the depth conjecture in §5).

2. Orbit Chern classes and finiteness theorems

In this section we will introduce a tool, the **orbit Chern classes**, based on a reworking[15] of Noether's [89] proof, motivated by the needs of [104] and using the language of algebraic topology [109]. With its help we take another look at the

[15] It is remarkable how many times this paper has been reworked, and how it continues to yield new and interesting results and problems. See e.g. [96], [8], and of course [116] chapter VIII §15.

structural finiteness theorems and the practical problem of computing generating polynomials for rings of invariants.

Let V be a finite-dimensional G-representation, G a finite group. For an orbit $B \subseteq V^*$ set

$$\varphi_B(X) = \prod_{b \in B} (X + b) \tag{2.1}$$

which we regard as an element of the ring $\mathbb{F}[V][X]$, with X a new variable. The polynomial $\varphi_B(X)$ is called the **orbit polynomial** of B. Since the product is taken over an invariant subset of V^*, $\varphi_B(X)$ regarded as a polynomial in X has coefficients in $\mathbb{F}[V]^G[X]$, i.e. $\varphi_B(X) \in \mathbb{F}[V]^G[X]$. More generally the formula (2.1) makes sense for any finite subset $B \subseteq V$ and defines an element of $\mathbb{F}[V][X]$. If the subset B is G-invariant, then $\varphi_B(X) \in \mathbb{F}[V]^G[X]$. If $B', B'' \subset V$ are disjoint, then $\varphi_{B'}(X) \cdot \varphi_{B''}(X) = \varphi_{B' \cup B''}(X)$. Since any G-invariant subset is a disjoint union of orbits we may, for the most part, restrict attention to subsets B that are orbits.

If we expand $\varphi_B(X)$ to a polynomial of degree $|B|$ in X, we obtain

$$\varphi_B(X) = \sum_{i+j=|B|} c_i(B) \cdot X^j,$$

defining homogeneous polynomials $c_i(B) \in \mathbb{F}[V]^G_i$, $i = 1, \ldots, |B|$ called the **orbit Chern classes** of the orbit B. Note that $\mathbb{F}[V]$ is integral over $\mathbb{F}[V]^G$ of finite type and for $v \in V^*$ the orbit polynomial $\varphi_{G \cdot v}(X)$ is the minimal polynomial of the element v over $\mathbb{F}[V]^G$.

The first orbit Chern class $c_1(B)$ is the sum of the orbit elements, and hence $c_1(B) = \mathrm{Tr}^{G/G_b}(b)$ where $b \in B$ is arbitrary and G_b the isotropy subgroup of b. If $|B| = k$, then $c_k(B)$ is the product of all the elements in the orbit B and is referred to as the **top Chern class of the orbit**, or the **norm** of $b \in B$. The first Chern class is additive and the norm is multiplicative, and all together they satisfy the **Whitney sum formula**

$$c_k(B' \sqcup B'') = \sum_{i+j=k} c_i(B') \cdot c_j(B'')$$

when B', B'' are disjoint G-invariant sets.

Here are some examples[16] to illustrate how Chern classes can be used to compute rings of invariants.

Example 1 (L. E. Dickson)**.** Consider the tautological representation of $\mathrm{GL}(2, \mathbb{F}_p)$ on $V = \mathbb{F}_p^2$. Let $\{x, y\}$ be a basis for the dual vector space V^*. The only orbits of $\mathrm{GL}(2, \mathbb{F}_p)$ on V^* are $\{0\}$ and $\widetilde{V} = V^* \setminus \{0\}$. To compute the Chern classes of the orbit $\widetilde{V}^*$, it is convenient to consider instead the orbit polynomial of V^*

$$\varphi_{V^*}(t) = t\varphi_{\widetilde{V}^*}(t) = \prod_{v \in V^*} (t + v).$$

This polynomial has the advantage that it is additive in t, and a short computation yields (see [106] §5.6 example 4)

$$\varphi_{V^*}(t) = t^{p^2} - (x^{p(p-1)} + y^{p-1}(y^{p-1} - x^{p-1})^{p-1})t^p - (xy^p - x^p y)^{p-1} t.$$

[16] If $z \in V^*$, we denote by $[z]$ the orbit of z, and by $c_i([z])$ or $c_i(z)$ the i-th Chern class of this orbit.

Hence the only nonzero orbit Chern classes are

$$\begin{aligned} c_{p^2-1}(\widetilde{V}) &= (xy^p - x^p y)^{p-1} \\ c_{p^2-p}(\widetilde{V}) &= (x^{p(p-1)} + y^{p-1}(y^{p-1} - x^{p-1})^{p-1}) \\ &= \frac{xy^{p^2} - x^{p^2}y}{xy^p - x^p y}. \end{aligned}$$

These polynomials are algebraically independent, and the product of their degrees is $(p^2-1)(p^2-p) = |\operatorname{GL}(2,\mathbb{F}_p)|$, so by a result of G. Kemper [55] it follows that they generate $\mathbb{F}_p[x,y]^{\operatorname{GL}(2,\mathbb{F}_p)}$. Hence $\mathbb{F}_p[x,y]^{\operatorname{GL}(2,\mathbb{F}_p)} = \mathbb{F}[c_{p^2-1}(\widetilde{V}), c_{p^2-p}(\widetilde{V})]$.

Example 2 (N. J. A. Sloane [103])**.** Consider the task of finding all the polynomials $f(x,y)$ that satisfy the identities

$$\begin{gathered} f\left(\frac{X+Y}{\sqrt{q}}, \frac{(q-1)X - Y}{\sqrt{q}}\right) = f(X,Y) \\ f(-X,-Y) = f(X,Y) \end{gathered}$$

where q is a fixed positive real number. This is a problem of invariant theory that arises in connection with binary codes. Note that we are demanding that the polynomial be invariant under the linear change of variables given by the matrices

$$\mathbf{A} = \frac{1}{\sqrt{q}}\begin{bmatrix} 1 & q-1 \\ 1 & -1 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

These matrices are each of order two and commute with each other, so generate a subgroup of $\operatorname{GL}(2,\mathbb{R})$ isomorphic to the Klein 4-group K (i.e. $\mathbb{Z}/2 \oplus \mathbb{Z}/2$). The group K acts via these matrices on the polynomial functions $\mathbb{R}[x,y]$ in two variables by linear change of variables, and we require a description of $\mathbb{R}[x,y]^K$.

If x, y denote the standard dual basis for $\mathbb{R}^2$, then the action[17] of $\mathbf{A}$ on x and y is:

$$\begin{aligned} \mathbf{A}(x) &= \frac{1}{\sqrt{q}}(x + (q-1)y) \\ \mathbf{A}(y) &= \frac{1}{\sqrt{q}}(x - y). \end{aligned}$$

The $\mathbf{A}$ orbits are therefore:

$$\begin{aligned} [x] &= \left\{x, \frac{1}{\sqrt{q}}(x + (q-1)y)\right\} \\ [y] &= \left\{y, \frac{1}{\sqrt{q}}(x - y)\right\}. \end{aligned}$$

[17]Remember, in the dual space the action is given by the transposed matrix.

The Chern classes of these orbits are:

$$\begin{aligned} c_1(x) &= x + \frac{1}{\sqrt{q}}(x + (q-1)y) \\ c_1(y) &= \frac{1}{\sqrt{q}}x + \left(1 - \frac{1}{\sqrt{q}}\right) y \\ c_2(x) &= \frac{x}{\sqrt{q}}(x + (q-1)y) \\ c_2(y) &= \frac{1}{\sqrt{q}}y(x-y). \end{aligned}$$

The two linear invariants are linearly dependent, as the following matrix computation shows:

$$\det \begin{bmatrix} 1 + \frac{1}{\sqrt{q}} & \frac{q-1}{\sqrt{q}} \\ \frac{1}{\sqrt{q}} & 1 - \frac{1}{\sqrt{q}} \end{bmatrix} = 1 - \frac{1}{q} - \frac{q-1}{q} = 1 - \frac{1}{q} - 1 + \frac{1}{q} = 0.$$

Let $f = \sqrt{q}c_1(y) = x + (\sqrt{q} - 1)y$ and $h = \sqrt{q}c_2(y) = y(x-y)$. The matrix $\mathbf{B}$ acts on $\mathbb{R}[x, y]$ by changing the signs of x and y simultaneously. The polynomial h is invariant under $\mathbf{B}$, whereas f is not, but its square is, and there are no algebraic relations between f^2 and h, i.e. $\mathbb{R}[f^2, h] \subseteq \mathbb{R}[x, y]^K$. A bit of linear algebra and Noether's bound, or some homological algebra ([106] theorem 5.5.5), show that indeed we have equality.

Orbit Chern classes are also a useful theoretical tool, as the following result taken from [109] (see also [106] §3.3) illustrates.

Theorem 2.1 (L. Smith and R. E. Stong)**.** *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation of a finite group G over a field $\mathbb{F}$. Suppose either the field $\mathbb{F}$ is of characteristic zero or that the order of G is less than the characteristic of $\mathbb{F}$. Then $\mathbb{F}[V]^G$ is generated by orbit Chern classes. If b is the size of the largest orbit of G acting on V^*, then $\mathbb{F}[V]^G$ is generated by homogeneous polynomials of degree at most b.*

Since $|G|$ is an upper bound for orbit sizes, this result also proves that Noether's bound holds under the same conditions as in theorem 1.2. Again, $\Sigma_{|G|}$ enters in the proof in such a way that its order must be invertible in the ground field.

Using the basic properties of Noetherian rings and modules (*sic*!) and the fundamental idea of a system of parameters, E. Noether extended the basic structural finiteness theorem 1.1 to arbitrary ground fields in [90]. For rings of invariants there is an algorithm to construct a system of parameters that R. Stanley [111] attributes to E. Dade (private correspondence) when the ground field has characteristic zero. We begin by describing the basic ideas (see also [93]) in a characteristic free way.

Proposition 2.2. *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation of a finite group G over the field $\mathbb{F}$, and set $V = \mathbb{F}^n$. Suppose that there is a basis $z_1, \ldots, z_n$ for the dual representation V^* that satisfies the condition*

$$z_i \notin \bigcup_{g_1, \ldots, g_{i-1} \in G} \mathrm{Span}_{\mathbb{F}}\{g_1 \cdot z_1, \ldots, g_{i-1} \cdot z_{i-1}\} \quad i = 2, \ldots, n. \tag{2.2}$$

Then the top Chern classes

$$c_{t_1}([z_1]), \ldots, c_{t_n}([z_n]) \in \mathbb{F}[V]^G$$

of the orbits $[z_1], \ldots, [z_n]$ of the basis elements are a system of parameters for $\mathbb{F}[V]$. (Here t_i denotes the cardinality $|[z_i]|$ of the G-orbit $[z_i]$ of z_i for $i = 1, \ldots, n$).

Proof. Since the extension of rings $\mathbb{F}[V]^G \subseteq \mathbb{F}[V]$ is finite and integral, it is equivalent to show $c_{t_1}([z_1]), \ldots, c_{t_n}([z_n]) \in \mathbb{F}[V]$ are a system of parameters. Passing to an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$, we need to show that the variety defined by the ideal $(c_{t_1}([z_1]), \ldots, c_{t_n}([z_n])) \subset \mathbb{F}[V]$ consists of the origin $0 \in \overline{V} = \overline{\mathbb{F}}^n$ alone. Note that the variety $V(c_{t_i}([z_i]))$ consists of the union of the hyperplanes $\ker\{g \cdot z_i\}$ where g ranges over all the elements of G. Since $z_1, \ldots, z_n$ satisfy condition (2.2), the linear forms $g_1 z_1, \ldots, g_n z_n$ are linearly independent for any $g_1, \ldots, g_n \in G$, and therefore the intersection of their kernels is zero. Hence for the variety $V(c_{t_1}([z_1]), \ldots, c_{t_n}([z_n]))$ defined by the ideal $(c_{t_1}([z_1]), \ldots, c_{t_n}([z_n])) \subset \mathbb{F}[V]$ we have

$$\begin{aligned} V(c_{t_1}([z_1]), \ldots, c_{t_n}([z_n])) &= \bigcap_{j=1}^{n} V(c_{t_j}([z_j])) = \bigcap_{j=1}^{n} \bigcup_{g_j \in G} \ker\{g_j \cdot z_j\} \\ &= \bigcup_{g_1, \ldots, g_n \in G} \ker\{g_1 z_1\} \cap \cdots \cap \ker\{g_n z_n\} = \{0\} \end{aligned}$$

as required. □

Given a representation $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$, a basis $z_1, \ldots, z_n \in V^*$ (where $V = \mathbb{F}^n$) that satisfies the condition (2.2) of proposition 2.2 will be called a **Dade basis** for V^*, and we refer to (2.2) as **Dade's condition**. If the ground field contains enough elements, then a sort of general position argument shows that a Dade basis always exists.

Proposition 2.3. *Let G be a finite group, $n \in \mathbb{N}$ and $\mathbb{F}$ a field. If $|G|^{n-1} < |\mathbb{F}|$, then for any representation $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ of G the dual representation V^* of $V = \mathbb{F}^n$ admits a Dade basis.* □

From this we can prove the finiteness theorem of E. Noether.

Theorem 2.4 (E. Noether [90])**.** *Let V be a finite-dimensional representation of a finite group G; then $\mathbb{F}[V]^G$ is finitely generated as an algebra.*

Proof. Without loss of generality we may suppose that $\mathbb{F}$ is algebraically closed, and therefore by proposition 2.3 V contains a Dade basis $z_1, \ldots, z_n$. The top Chern classes $c_{t_1}(z_1), \ldots, c_{t_n}(z_n) \in \mathbb{F}[V]$ are a system of parameters and therefore algebraically independent, so we have the inclusions

$$\mathbb{F}[c_{t_1}(z_1), \ldots, c_{t_n}(z_n)] \subseteq \mathbb{F}[V]^G \subseteq \mathbb{F}[V].$$

Since $\mathbb{F}[V]$ is a finitely generated $\mathbb{F}[c_{t_1}(z_1), \ldots, c_{t_n}(z_n)]$-module and $\mathbb{F}[V]^G$ is an $\mathbb{F}[c_{t_1}(z_1), \ldots, c_{t_n}(z_n)]$-submodule, it too is finitely generated as an $\mathbb{F}[c_{t_1}(z_1), \ldots, c_{t_n}(z_n)]$-module. If $h_1, \ldots, h_m \in \mathbb{F}[V]^G$ is a system of $\mathbb{F}[c_{t_1}(z_1), \ldots, c_{t_n}(z_n)]$-module generators, then $\mathbb{F}[V]^G$ is generated as an algebra by $c_{t_1}(z_1), \ldots, c_{t_n}(z_n), h_1, \ldots, h_m$. □

This result can be applied to deduce an upper bound, although larger than Noether's bound, for the degrees of a set of algebra generators for $\mathbb{F}[V]^G$ in the nonmodular case that improves on the bound obtained by H. E. A. Campbell, I. G. Hughes and R. D. Pollack in [18] using vector invariants. The following is part of joint work with V. Reiner [93] (see also [38]).

Corollary 2.5. *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation of a finite group G over the field $\mathbb{F}$, and suppose that $|G| \in \mathbb{F}^\times$. Then $\mathbb{F}[V]^G$ is generated as an algebra by homogeneous polynomials of degree at most* $\max\{|G|, n(|G| - 1)\}$.

Proof. Passing to an algebraic closure, proposition 2.3 implies there is a system of parameters[18] $h_1, \ldots, h_n \in \mathbb{F}[V]^G$ such that $\deg(h_1) = \cdots = \deg(h_n) = |G|$. The Poincaré series of $\mathbb{F} \otimes_{\mathbb{F}[h_1,\ldots,h_n]} \mathbb{F}[V]$ is

$$P(\mathbb{F} \otimes_{\mathbb{F}[h_1,\ldots,h_n]} \mathbb{F}[V], t) = (1 + t + \cdots + t^{|G|-1})^n$$

and therefore has degree $n(|G| - 1)$. Since $|G| \in \mathbb{F}^\times$, the transfer homomorphism[19] $\mathrm{Tr}^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$ provides a splitting as $\mathbb{F}[V]^G$-module, and hence a fortiori as $\mathbb{F}[h_1, \ldots, h_n]$-module, to the inclusion $\mathbb{F}[V]^G \subseteq \mathbb{F}[V]$. Hence the induced map

$$\mathbb{F} \otimes_{\mathbb{F}[h_1,\ldots,h_n]} \mathbb{F}[V]^G \to \mathbb{F} \otimes_{\mathbb{F}[h_1,\ldots,h_n]} \mathbb{F}[V]$$

is a monomorphism, so $n(|G| - 1)$ is also an upper bound for the degree of the Poincaré series $P(\mathbb{F} \otimes_{\mathbb{F}[h_1,\ldots,h_n]} \mathbb{F}[V]^G, t)$, and thus $\mathbb{F}[V]^G$ is generated by homogeneous polynomials of degree at most $\max\{|G|, n(|G| - 1)\}$, as $h_1, \ldots, h_n$ together with polynomials that project to a basis for $\mathbb{F} \otimes_{\mathbb{F}[h_1,\ldots,h_n]} \mathbb{F}[V]^G$ certainly generate $\mathbb{F}[V]^G$ as an algebra. □

Note that this bound is of a fundamentally different character than Noether's bound, as it depends on the group order **and** the dimension of the representation.

In addition to bounds for the degrees of generators, bounds on their number are also interesting. If $f_1, \ldots, f_m \in \mathbb{F}[V]^G$ generate $\mathbb{F}[V]^G$, then $m \geq n$. If $m = n$, then $\mathbb{F}[V]^G = \mathbb{F}[f_1, \ldots, f_n]$ is a polynomial algebra. If $|G| \in \mathbb{F}^\times$, then this is the case if and only if G is generated by pseudoreflections[20] (see e.g. [106], §7.4). In fact, independent of the characteristic, G and all the pointwise stabilizers G_v, $v \in V$, are generated by pseudoreflections[21] [12] chapter 5 §6 exercise 8. Examples show [56] that the converse is false. A lot remains to be done, e.g.

Problem 2.6 (M. Göbel)**.** *Characterize the representations* $G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ *whose rings of invariants are generated by* $n + 1$ *elements.*

Geometrically this amounts to asking for a classification of **hypersurface groups**, i.e. groups whose orbit space V/G is a hypersurface, because the map

$$f : V/G \to \mathbb{F}^m \quad f([v]) = (f_1(v), \ldots, f_m(v))$$

provides an affine embedding[22] of the orbit space V/G (see e.g. [20] or [24] chapter 7 §4, particularly theorem 10 (2) for the case $\mathbb{F} = \mathbb{C}$). Therefore the difference $m - n$ is called the **embedding codimension** of $\mathbb{F}[V]^G$. Geometric invariant theory provides ([44] §4.4 corollary 4) the following lower bound for the embedding dimension.

Theorem 2.7 (N. L. Gordeev)**.** *Let* $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ *be a representation of a finite group over an algebraically closed field of characteristic* 0*. Then the embedding dimension of* $\mathbb{F}[V]^G$ *is at least* $\min\{\mathrm{codim}_{\mathbb{F}}(V^g) | 1 \neq g \in G\} - 1$. □

---

[18] Suitable powers of the top Chern classes of the orbits of a Dade basis.

[19] So this argument will **not** work if we just assume that $\mathbb{F}[V]^G$ is Cohen-Macaulay.

[20] A **pseudoreflection** $s \in \mathrm{GL}(n, \mathbb{F})$ is an element with 1 as an eigenvalue of multiplicity exactly $n - 1$.

[21] For finite real reflection groups this is elementary, and in the complex case this is a theorem of R. Steinberg [112].

[22] For arbitrary ground fields this is the key to defining an orbit space of an algebraic group acting on an algebraic variety. See for example [58] and the references there.

It would be nice to have a direct proof for finite groups and an estimate valid over arbitrary ground fields. Counting the minimal number of generators for $\mathbb{F}[V]^G$ seems to be a very difficult problem, even for abelian groups in characteristic zero. For the special case of the regular representation of a cyclic group see [34], [53], and [67], and for certain other representations of abelian groups [16]. The special class of hypersurface groups $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ where $\mathbb{F}[V]^G$ is of the form $\mathbb{F}[h_1, \ldots, h_n][f]/(f^s - h)$ for some $h \in \mathbb{F}[h_1, \ldots, h_n]$ is classified for $\mathbb{F} = \mathbb{F}_p$ in [50] when certain nonmodular conditions[23] hold (see also [79]).

The combinatorial finiteness theorem 1.3 was generalized by Serre (see e.g. [9] §2.1 or [106] §2.1), and for rings of invariants it reads:

Theorem 2.8 (J.-P. Serre)**.** *If $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ is a representation of a finite group, then the Poincaré series of $\mathbb{F}[V]^G$ is of the form*

$$\frac{f(t)}{\prod_{i=1}^{n}(1 - t^{k_n})},$$

where $k_1, \ldots, k_n \in \mathbb{N}$ and $f(t)$ is a polynomial with integral coefficients with $f(1) \neq 0$. □

In particular $P(\mathbb{F}[V]^G, t)$ is a rational function with a pole of order $n = \dim_{\mathbb{F}}(V)$ at $t = 1$. The leading coefficient of the Laurent expansion about $t = 1$ is $\frac{1}{|G|}$ (see e.g. [2] (the correction), [9] §2.4 or [106] §5.5). An interpretation for the next coefficient was conjectured by D. Carlisle and P. Kropholler (unpublished) and verified by W. Crawley-Bovey and D. Benson (see [9]). A nice discussion from the geometric viewpoint has also been given by A. Neeman [82].

The direct generalization of the homological finiteness theorem of Hochster-Eagon (see 1.6) fails in the modular case. This will be discussed in section §4.

3. Noether's bound: A forgotten old problem

Finiteness problems continue to be one of the most interesting aspects of invariant theory. In this section we will take a look at the problems connected with the structural finiteness theorem, particularly bounds on the degrees of generators, e.g. Noether's bound. The upper bound on the degrees of a set of generating polynomials for the ring of invariants given by theorem 1.2, Noether's bound, leads to a number of basic open problems in the invariant theory of finite groups.

If $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ is a representation, then following B. J. Schmid [96] we write $\beta(\varrho)$ for the smallest integer such that $\mathbb{F}[V]^G$ is generated as an algebra by homogeneous polynomials of degree $\leq \beta(\varrho)$. Write $\beta_{\mathbb{F}}(G)$ for the maximum, or infinity, of $\beta(\varrho)$ for ϱ a representation over $\mathbb{F}$. For example $\beta_{\mathbb{F}}(G) \leq |G|$ if $|G|! \in \mathbb{F}^{\times}$.

Problem 3.1. *Does Noether's bound hold under the assumption that $|G| \in \mathbb{F}^{\times}$?*

Until we know the answer to this question, the invariant theory of finite groups seems to divide into a number of different cases:

The nonmodular case: $|G| \in \mathbb{F}^{\times}$.

The strong nonmodular case: $|G|! \in \mathbb{F}^{\times}$; i.e. $|G|$ is strictly smaller than the characteristic of $\mathbb{F}$. In this case $\beta_{\mathbb{F}}(G) \leq |G|$ (see theorem 1.2).

[23] The nonmodularity condition takes the form $p \nmid \det(h_1) \cdots \deg(h_n)$ and $s|(p-1)$. The proof makes essential use of Steenrod operations.

The weak nonmodular case: $|G|$ is relatively prime to, but larger than, the characteristic of $\mathbb{F}$. In this case $\beta_{\mathbb{F}}(G)$ is largely unknown.

The modular case: $|G| \equiv 0 \in \mathbb{F}$. In this case Noether's bound need not hold, e.g. §4 example 2, and $\beta_{\mathbb{F}}(G)$ is infinite in all known cases.

Good test candidates for this problem are the Suzuki groups[24] in characteristic 3, or the alternating groups A_n in characteristic p, where $n < p < \frac{n!}{2}$. We will see in §4 that Noether's bound is definitely false in the modular case.

A family of groups for which Noether's bound is known to hold in all nonmodular cases are the solvable groups [107], [52]. Here is the relative version of the result.

Theorem 3.2. *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation of the finite group G over the field $\mathbb{F}$ and $H \leq G$ a subgroup. Suppose*:

(1) *$\mathbb{F}[V]^H$ is generated as an algebra by elements of degree at most d_H.*
(2) *$|G : H| \in \mathbb{F}^\times$.*
(3) *There is a subnormal series*

$$H = G_0 \lhd G_1 \lhd \cdots \lhd G_s = G$$

whose composition factors G_i/G_{i-1} are finite cyclic groups for $i = 1, \ldots, s$.

Then $\mathbb{F}[V]^G$ is generated as an algebra by elements of degree at most $d_H \cdot |G : H|$.

The proof is not really difficult and leads to an interesting question in algebraic combinatorics. It begins with the simplest case, namely that of a cyclic group.

Lemma 3.3. *Let $m \in \mathbb{N}$ and $\varrho : \mathbb{Z}/m \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of the finite cyclic group $\mathbb{Z}/m$ over the field $\mathbb{F}$. If the characteristic of $\mathbb{F}$ does not divide m, then $\mathbb{F}[V]^{\mathbb{Z}/m}$ is generated by elements of degree at most m.*

Proof. By flat base change we may suppose that $\mathbb{F}$ contains a primitive m-th root of unity λ. The representation ϱ is then implemented by a diagonal matrix

$$T = \begin{bmatrix} \lambda^{a_1} & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & \cdots & \lambda^{a_n} \end{bmatrix} \in \mathrm{GL}(n, \mathbb{F}),$$

where $0 \leq a_i \leq m-1$ for $i = 1, \ldots, n$. By splitting off the fixed point set of T we may also suppose that $a_i \neq 0$ for $i = 1, \ldots, n$. The action of T on a monomial $z^b = z_1^{b_1} \cdots z_n^{b_n}$ is given by

$$T(z^b) = \lambda^{a_1 b_1 + \cdots + a_n b_n} z^b.$$

Hence $f \in \mathbb{F}[V]^{\mathbb{Z}/m}$ if and only if f is a sum of monomials satisfying

$$a_1 b_1 + \cdots + a_n b_n \equiv 0 \bmod m.$$

The multiplicative semigroup of monomials $\{z^b | a_1 b_1 + \cdots + a_n b_n \equiv 0 \bmod m\}$ is isomorphic to the subsemigroup B of $\underset{\longleftarrow}{\mathbb{N}} \times \underset{n}{\cdots} \times \underset{\longrightarrow}{\mathbb{N}}$ consisting of those n-tuples $(b_1, \ldots, b_n)$ such that $a_1 b_1 + \cdots + a_n b_n \equiv 0 \bmod m$. The result then follows from the congruence semigroup lemma, [96] lemma 2.1, of B. J. Schmid. □

For the sake of completeness we include the statement of the congruence semigroup lemma loc. cit. in the form in which we have used it. A proof of this formulation can be found in [107]. It would be nice to have a better proof, one that generalizes to simultaneous congruences (see problem 3.8).

[24] These are finite simple groups whose order is not divisible by, but greater than, 3.

Lemma 3.4 (B. J. Schmid)**.** *Let $m, n \in \mathbb{N}$. Suppose one is given $a_1, \ldots, a_n \in \mathbb{N}$ satisfying $a_i \not\equiv 0 \bmod m$ and let $B \subseteq \underset{\longleftarrow}{\mathbb{N}} \times \underset{n}{\cdots} \times \underset{\longrightarrow}{\mathbb{N}}$ be the congruence semigroup defined by*

$$b = (b_1, \ldots, b_n) \in B \text{ if and only if } a_1 b_1 + \cdots + a_n b_n \equiv 0 \bmod m.$$

Then B is generated as a semigroup by the elements $b \in B$ satisfying $b_1 + \cdots + b_n \leq m$. □

It is now an easy matter to establish what we need to show to prove that Noether's bound holds for solvable groups in the nonmodular case.

Proposition 3.5. *Let A be a graded connected commutative algebra over a field $\mathbb{F}$ and $m \in \mathbb{N}$. Let $\mathbb{Z}/m \leq \mathrm{Aut}(A)$ be a finite cyclic group of grading preserving automorphisms of A. Assume that*

1. *A is generated as an algebra by elements of degree at most d, and*
2. *the characteristic of $\mathbb{F}$ does not divide m.*

Then $A^{\mathbb{Z}/m}$ is generated by elements of degree at most dm.

Proof. Define the graded vector space V by requiring

$$V_i = \begin{cases} A_i & \text{for } i = 1, \ldots, d \\ 0 & \text{otherwise.} \end{cases}$$

Then $V \subseteq A$ is closed under the action of $\mathbb{Z}/m$ on A. Hence the induced map

$$\varphi : S(V) \to A$$

is a $\mathbb{Z}/m$-equivariant map, where $S(—)$ denotes the symmetric algebra functor. Since V generates A as an algebra, the map φ is an epimorphism. Since the characteristic of $\mathbb{F}$ does not divide m, the map φ may be split by a $\mathbb{Z}/m$-equivariant map of graded vector spaces. Hence the induced map

$$\varphi : S(V)^{\mathbb{Z}/m} \to A^{\mathbb{Z}/m}$$

is also an epimorphism. Let $z_1, \ldots, z_n \in V$ be a homogeneous basis for V as a graded vector space over $\mathbb{F}$. By lemma 3.3 $S(V)^{\mathbb{Z}/m}$ is generated as an algebra by monomials $z^b = z_1^{b_1} \cdots z_n^{b_n}$ with $b_1 + \cdots + b_n \leq m$. Since each z_i has at most degree d it follows that these monomials have degree at most dm, and since their images under φ generate A the result is established. □

Proof of Theorem 3.2. If $H \lhd G$ is a normal subgroup, then $\mathbb{F}[V]^G = (\mathbb{F}[V]^H)^{G/H}$, so repeated application yields

$$\mathbb{F}[V]^G = (\cdots((\mathbb{F}[V]^{G_0})^{G_1/G_0})^{\cdots})^{G_s/G_{s-1}}$$

and the result follows from successive use of proposition 3.5. □

Corollary 3.6. *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of the finite solvable group G over the field $\mathbb{F}$ whose characteristic is prime to the order of G. Then $\mathbb{F}[V]^G$ is generated as an algebra by elements of degree at most $|G|$.* □

The Odd Order Theorem of W. Feit and J. G. Thompson [35] says groups of odd order are solvable, so Noether's bound holds for groups of odd order in characteristic 2.

Problem 3.7. *Find other classes of groups for which Noether's bound holds in the nonmodular case.*

The proof of theorem 3.2 can be modified to obtain an improvement of Noether's bound for nonabelian nilpotent groups in all nonmodular cases. By contrast B. J. Schmid shows [96] that Noether's bound is sharp for cyclic groups (proposition 1.6 loc. cit.) but not for noncyclic groups (proposition 1.7 loc. cit.) in the strong nonmodular case. Her analysis (loc. cit.) of abelian groups leads to the following problem in algebraic combinatorics, formulated as a generalization of lemma 3.4.

Problem 3.8. *Suppose one is given integers $m_1, \dots, m_k \in \mathbb{N}$ that successively divide, i.e. $m_1 | m_2 | \cdots | m_k$. Let $a_{1,j}, \dots, a_{n,j} \in \mathbb{N}$ satisfying $a_{i,j} \not\equiv 0 \bmod m_j$ for $i = 1, \dots, n$, and let $B \subseteq \underset{\longleftarrow}{\mathbb{N}} \times \underset{n}{\cdots} \times \underset{\longrightarrow}{\mathbb{N}}$ be the congruence semigroup defined by the simultaneous system of congruences*:

$$b = (b_1, \dots, b_n) \in B \text{ if and only if } a_{1,j} b_1 + \cdots + a_{n,j} b_n \equiv 0 \bmod m_j \quad \text{for } j = 1, \dots, k.$$

Find an upper bound as a function of $m_1, \dots, m_k$ on $|b| = b_1 + \cdots + b_n$ for b in a system of generators for B.

For example, when $k = 2$, B. J. Schmid notes [96] that $m_1 \cdot m_2 - 1$ serves as an upper bound, which is one less than one would expect.

If $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ is a fixed representation of the finite group G, it is natural to study how $\beta(\bigoplus^k \varrho)$ varies with k. This leads to the theory of vector invariants[25], which were much studied in characteristic zero beginning in the last century and reached a high point in chapter II of H. Weyl's book [116]. His theorem 2.5.A ([116] chapter II §5 page 44) implies for $\mathbb{F}$ of characteristic zero and any representation ϱ of a finite group G over $\mathbb{F}$ that $\beta(\bigoplus^m \varrho) \leq \beta(\bigoplus^{\dim_{\mathbb{F}}(\varrho)} \varrho)$ for all $m \in \mathbb{N}$. In characteristic zero, for $\mathbb{F} = \mathbb{C}$ any representation ϱ is a sum of irreducible representations, and each irreducible representation θ of G occurs exactly $\dim_{\mathbb{C}}(\theta)$ times. Thus we have:

Theorem 3.9 (B. J. Schmid)**.** *For any finite group G we have $\beta_{\mathbb{C}}(G) \leq \beta(\mathrm{REG}_{\mathbb{C}})$, where $\mathrm{REG}_{\mathbb{C}}$ is the complex regular representation of $\mathbb{C}$.*

As noted, her proof in [96], §6 using Weyl's theorem does not work if the characteristic of the ground field is not 0, since representations of $\mathrm{GL}(n, \mathbb{F})$ are not completely reducible in this case.

Problem 3.10. *Is $\beta_{\mathbb{F}}(G) \leq \beta(\mathrm{REG}_{\mathbb{F}})$ in the nonmodular case? In the strong nonmodular case?*

$\beta_{\mathbb{F}}(G)$ need not be finite in the modular case [95], but all the examples show that $\beta_{\mathbb{F}}(\varrho)$ might depend on just $|G|$ and the dimension of the representation; therefore the following is of basic importance for modular invariant theory.

Problem 3.11. *Is there an upper bound for $\beta(\varrho)$ in the modular case that depends only on $|G|$ and $\dim_{\mathbb{F}}(\varrho)$?*

Permutation representations form another class of representations where we have good bounds and algorithms to compute rings of invariants.

Let $|X|$ be a finite G-set, $|X| = n$, defined by $\varrho : G \hookrightarrow \Sigma_n$. We have the following relations between the rings of invariants

$$\mathbb{F}[e_1, \dots, e_n] = \mathbb{F}[X]^{\Sigma_n} \subseteq \mathbb{F}[X]^G \subseteq \mathbb{F}[X].$$

[25] See e.g. [94], [95] and [57] for a discussion in the modular case.

The elementary symmetric polynomials $e_1, \ldots, e_n \in \mathbb{F}[X]^{\Sigma^n}$ are a system of parameters and $\mathbb{F}[X]$ is a Cohen-Macaulay algebra. Therefore $\mathbb{F}[X]$ is a free finitely generated $\mathbb{F}[X]^{\Sigma_n}$-module and the Poincaré series of $\mathbb{F} \otimes_{\mathbb{F}[X]^{\Sigma_n}} \mathbb{F}[X]$ is

$$\prod_{i=1}^{n}(1 + t + \cdots + t^{i-1})$$

and has degree $0 + 1 + \cdots + (n-1) = \binom{n}{2}$. Hence $\mathbb{F}[X]_{\Sigma_n}$ is zero in homogeneous degrees larger than $\frac{n(n-1)}{2}$.

If the characteristic of the ground field $\mathbb{F}$ does not divide the order of G, the Reynolds operator (see §1)

$$\pi^G : \mathbb{F}[X] \to \mathbb{F}[X]^G$$

is a $\mathbb{F}[X]^{\Sigma_n}$-module homomorphism and splits the inclusion $\mathbb{F}[X]^G \subseteq \mathbb{F}[X]$. Hence we obtain a monomorphism of the associated indecomposable modules

$$\mathbb{F} \otimes_{\mathbb{F}[X]^{\Sigma_n}} \mathbb{F}[X]^G \hookrightarrow \mathbb{F} \otimes_{\mathbb{F}[X]^{\Sigma_n}} \mathbb{F}[X] = \mathbb{F}[X]_{\Sigma_n}.$$

It follows that $\mathbb{F} \otimes_{\mathbb{F}[X]^{\Sigma_n}} \mathbb{F}[X]^G$ is also totally finite and zero in degrees larger than $\binom{n}{2}$. Hence $e_1, \ldots, e_n$ is also a system of parameters for $\mathbb{F}[X]^G$, so $\mathbb{F}[X]^G$ is generated as an $\mathbb{F}[X]^{\Sigma_n}$-module by polynomials of degree less than or equal to $\frac{n(n-1)}{2}$ and as an algebra by polynomials of degree at most $\max\{n, \frac{n(n-1)}{2}\}$.

This bound is often better than $|G|$, which is what Noether's theorem 1.2 provides when it applies. Moreover, the bound $\max\{n, \frac{n(n-1)}{2}\}$ for transitive permutation representations of degree n is sharp because the ring of invariants of the alternating group A_n in its tautological representation[26] is generated by the elementary symmetric functions $e_1, \ldots, e_n$ and Δ, the discriminant, which has degree $n(n-1)/2$.

In characteristic zero the bound $\max\{n, \frac{n(n-1)}{2}\}$ for permutation representations was first proved by Garsia and Stanton [41]. The above nonmodular discussion is taken from [106] §6.2. The following remarkable extension was obtained by M. Göbel [43] (see also [92]).

Theorem 3.12 (M. Göbel)**.** *Let G be a finite group and X a finite G-set. If R is a commutative ring with 1 and $R[X]$ the polynomial ring over R in the variables X, then $R[X]^G$ is generated by the orbit sums of the monomials of degree less than or equal to* $\max\{|X|, \binom{|X|}{2} = \frac{|X|(|X|-1)}{2}\}$. □

The orbit sum of a polynomial is simply the sum of all the elements in the orbit, i.e. the higher degree analog of the first Chern class of an orbit of a linear form.

Problem 3.13. *Find ways to estimate $\beta_{\mathbb{F}}(G)$ based on group theoretical properties of G, or $\beta(\varrho)$ based on representational theoretic properties of ϱ.*

For example, for p-permutation representations, P. Fleischmann and W. Lempken have shown $\beta_{\mathbb{F}}(\varrho) \leq \max\{|G|, n(|G|-1)\}$ [39].

4. The Dickson algebra and modular invariant theory

Invariant theory in the modular case is not as straightforward as in the nonmodular case. In particular, apart from the basic finiteness theorem of Noether and Hilbert's syzygy theorem, all the nice features of the nonmodular case can and do

[26] Over a groundfield $\mathbb{F}$ of characteristic different from 2.

fail in the modular case. To illustrate this we make use of the family of representations $\sigma_k : \mathbb{Z}/2 \hookrightarrow \mathrm{GL}(2k, \mathbb{F})$, for $\mathbb{F}$ a field of characteristic 2, described in the introduction.

Example 1. The transfer need not be surjective in the modular case. This already occurs for the smallest possible modular example, $\sigma : \mathbb{Z}/2 \hookrightarrow \mathrm{GL}(2, \mathbb{F})$ over a field of characteristic 2. The polynomial $xy \in \mathbb{F}[x, y]$ is clearly invariant. The polynomials x^2, xy, y^2 are a basis for the homogeneous quadratic polynomials in $\mathbb{F}[x, y]$ and

$$\mathrm{Tr}^{\mathbb{Z}/2}(x^2) = x^2 + y^2 = \mathrm{Tr}^{\mathbb{Z}/2}(y^2)$$
$$\mathrm{Tr}^{\mathbb{Z}/2}(xy) = 0,$$

so $xy \in \mathbb{F}[x, y]^{\mathbb{Z}/2}$, but $xy \notin \mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/2})$.

In fact this is not an isolated example. In the last section of [37] M. Feshbach sketched a proof of the following theorem. The proof below is based on one developed by H. Derkson and the Dagstuhl Workshop on Computational Invariant Theory (May 1996).

Theorem 4.1 (M. Feshbach)**.** *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation of a finite group G over the field $\mathbb{F}$. If the characteristic of $\mathbb{F}$ is p and divides the order of G, then Tr^G is not surjective.*

Proof. Let $h \in G$ be an element of order p, $H \leq G$ the subgroup generated by h, and $g_1, \ldots, g_t \in G$ a transversal of H in G. Since h has order p, $V^H \neq \{0\}$. Choose $v \neq 0 \in V^H$. Then for any $f \in \mathbb{F}[V]$ we have

$$(\mathrm{Tr}^G(f))(v) = \sum_{\substack{i=0 \\ j=1}}^{\substack{p-1 \\ t}} f(g_j^{-1} h^{-i} v) = \sum_{j=1}^{t} p f(g_j^{-1} v) = 0. \tag{4.1}$$

Suppose to the contrary that Tr^G were surjective. Choose a system of parameters $f_1, \ldots, f_n \in \mathbb{F}[V]^G$. Then $f_1, \ldots, f_n$ is also a system of parameters for $\mathbb{F}[V]$, so for any $f \in \mathbb{F}[V]$ there exists polynomials $F_1, \ldots, F_n \in \mathbb{F}[V]$ such that

$$F = F_1 f_1 + \cdots + F_n f_n.$$

Since $f_1, \ldots, f_n \in \mathrm{Im}(\mathrm{Tr}^G)$ it follows from (4.1) that

$$F(v) = F_1(v) f_1(v) + \cdots F_n(v) f_n(v) = 0.$$

Therefore every polynomial $F \in \mathbb{F}[V]$ will vanish at $v \neq 0 \in V$, which is impossible, so Tr^G cannot be surjective. □

Remark. With a bit more care the above proof shows that the height of the ideal $\mathrm{Im}(\mathrm{Tr}^G)$ is at most equal to the codimension of the algebraic variety $\bigcup_{\substack{g \in G \\ g^p = 1}} V^g$.

Once one has seen that the transfer need not be surjective, it is not surprising that results that depend on the transfer for their proof can also fail in the modular case. The following examples show that the invariant theory of cyclic groups in the modular case presents a number of very hard problems: these examples are only the tip of an iceberg; see e.g. [10], [11], [33], [40] and [85].

Example 2 (M. D. Neusel)**.** Consider the representation $\sigma_3 : \mathbb{Z}/2 \hookrightarrow \mathrm{GL}(6,\mathbb{F})$, where $\mathbb{F}$ is a field of characteristic 2. The Poincaré series of $\mathbb{F}[x_1,x_2,x_3,y_1,y_2,y_3]^{\mathbb{Z}/2}$ can be computed by using either Molien's theorem to compute the Poincaré series over $\mathbb{C}$ and the last conclusion of theorem 1.4 or theorem 1.4 directly. In either case we obtain:

$$\begin{aligned} P(\mathbb{F}[x_1,x_2,x_3,y_1,y_2,y_3]^{\mathbb{Z}/3},t) &= \frac{1}{2}\left[\frac{(1+t)^3+(1-t)^3}{(1-t)^3(1-t^2)^3}\right] \\ &= \frac{1+3t^2}{(1-t)^3(1-t^2)^3} = 1+3t+12t^2+28t^3+\cdots . \end{aligned}$$

Therefore the space of invariant linear forms has dimension 3, the space of invariant quadratic forms dimension 12, the space of invariant cubic forms dimension 28, etc. To compute requisite bases, assume that the basis x_1,x_2,x_3,y_1,y_2,y_3 for the linear forms in $\mathbb{F}[x_1,x_2,x_3,y_1,y_2,y_3]$ is chosen so that the nontrivial element of $\mathbb{Z}/2$ simultaneously interchanges x_i with y_i for $i=1,2,3$. Then

$$l_i = x_i + y_i \quad i=1,2,3$$

is a basis for the invariant linear forms, and the 6 products

$$l_i l_j \quad 1 \le i \le j \le 3$$

together with the 6 quadratic polynomials

$$\begin{aligned} q_i &= x_i y_i \quad i=1,2,3 \\ Q_3 &= x_1x_2 + y_1y_2 \\ Q_2 &= x_1x_3 + y_1y_3 \\ Q_1 &= x_2x_3 + y_2y_3 \end{aligned}$$

form a basis for the space of invariant quadratic forms. From these, at most 28 linearly independent invariant cubic polynomials can be generated as products: 18 products of a linear and a quadratic polynomial, and 10 products of three linear polynomials, so the space of cubic forms in the subalgebra generated by these polynomials has at most dimension 28. The crucial observation made by M. D. Neusel is that

$$l_1l_2l_3 = Q_1l_1 + Q_2l_2 + Q_3l_3 + 2(x_1x_2x_3 + y_1y_2y_3)$$

and hence in characteristic 2 this space of cubic forms has dimension at most 27. (In characteristic different from 2 it has the required dimension 28, by for example 3.6). Therefore the algebra of invariants $\mathbb{F}[x_1,x_2,x_3,y_1,y_2,y_3]^{\mathbb{Z}/2}$ contains an indecomposable cubic form, and Noether's bound, $|\mathbb{Z}/2| = 2$, does not hold in this example.

For a different discussion of this example[27] see [106] §2.4 example 2, and for a more complete analysis of the entire family of examples $\sigma_k : k = 1,2,\ldots$ see [95]. In particular Richman shows that $\mathbb{F}[x_1,\ldots,y_k]^{\mathbb{Z}/2}$ contains an indecomposable form of degree k, so $\beta_{\mathbb{F}_2}(\sigma_k) \ge k$. There is therefore no analog of Noether's bound, i.e. independent of the dimension of the representation, in the modular case.

[27]The discussion in [106] contains a number of unfortunate misprints, the most irritating being that $y_iy_jy_k$, for $i,j,k \in \{1,2,3\}$ **are** invariant cubic forms, but the cubic form f contains the monomial $x_1x_2y_3$ that does **not** occur in an invariant cubic form in the subalgebra generated by the invariant linear and quadratic forms.

All the evidence in the modular case makes it plausible that the answer to the following is yes.

Problem 4.2. *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation of a finite group over the field $\mathbb{F}$. If the characteristic of $\mathbb{F}$ divides the order of G, does $\lim_{k\to\infty} \beta_{\mathbb{F}}(k\varrho) = \infty$?*

The preceding example can also be reinterpreted to show that the homological finiteness theorem 1.6, namely the Cohen-Macaulay property, can also fail in the modular case.

Example 3 (M. D. Neusel)**.** Consider again σ_3 over a field of characteristic 2. The polynomials

$$l_i, q_j \in \mathbb{F}[x_1, x_2, x_3, y_1, y_2, y_3]^{\mathbb{Z}/2} \qquad i = 1, 2, 3 \quad j = 1, 2, 3$$

is a system of parameters (l_i, q_i are the elementary symmetric functions in x_i, y_i for $i = 1, 2, 3$, and so together are a system of parameters for $\mathbb{F}[x_1, x_2, x_3, y_1, y_2, y_3]$). If $\mathbb{F}[x_1, x_2, x_3, y_1, y_2, y_3]^{\mathbb{Z}/2}$ were Cohen-Macaulay, then these polynomials would have to be a regular sequence in $\mathbb{F}[x_1, x_2, x_3, y_1, y_2, y_3]^{\mathbb{Z}/2}$. But Neusel's relation shows

$$l_1 Q_1 = l_2 Q_2 + l_3 Q_3 + l_1 l_2 l_3 \in \mathbb{F}[x_1, x_2, x_3, y_1, y_2, y_3]^{\mathbb{Z}/2}$$

and therefore $l_1 Q_1 \in (l_2, l_3) \subset \mathbb{F}[x_1, x_2, x_3, y_1, y_2, y_3]^{\mathbb{Z}/2}$. Since $Q_1 \notin (l_2, l_3) \subset \mathbb{F}[x_1, x_2, x_3, y_1, y_2, y_3]^{\mathbb{Z}/2}$ this shows that l_1 is a zero divisor modulo (l_2, l_3) and therefore $l_1, l_2, l_3 \in \mathbb{F}[x_1, x_2, x_3, y_1, y_2, y_3]^{\mathbb{Z}/2}$ is not a regular sequence, so $\mathbb{F}[x_1, x_2, x_3, y_1, y_2, y_3]^{\mathbb{Z}/2}$ is not Cohen-Macaulay.

For a different discussion of this same example see [57], [17] or [106] §6.7 example 2.

"If the property you want is important, but fails to hold in interesting examples, then the difference between what you have and what you want should be an interesting invariant." This paraphrase of a remark of J. F. Adams suggests a way to profit from the fact that rings of invariants need not be Cohen-Macaulay in the modular case, namely, introduce the length of the longest regular sequence in $\mathbb{F}[V]^G$, which is bounded above by $n = \dim_{\mathbb{F}}(V) = \dim(\mathbb{F}[V])$, with equality in the Cohen-Macaulay case, and study the difference between it and n. This length is a well-studied invariant in commutative algebra called the **homological codimension** or the **depth** of $\mathbb{F}[V]^G$ (see e.g. [14]). We prefer the term homological codimension and will work with the following definition and notation:

Definition. Let H be a graded connected commutative algebra over a field $\mathbb{F}$ and M a graded H-module. The **homological dimension**, or **projective dimension**, of M is the length of the shortest projective resolution of M as H-module and is denoted by $\text{hom-dim}_H(M)$. The **homological codimension** of M as an H-module, denoted by $\text{hom-codim}_H(M)$, is the length of the longest regular sequence in the augmentation ideal $\overline{H}$ on M.

If $M = H$, we speak of the homological codimension of H and denote it by $\text{hom-codim}(H)$. The **Auslander-Buchsbaum equality** [14] theorem 1.3.3

$$\text{hom-dim}_H(M) + \text{hom-codim}_H(M) = \text{hom-codim}(H)$$

for any graded connected commutative algebra H over a field $\mathbb{F}$ and nonzero H-module M of finite projective dimension explains the origin of the term codimension and is a useful computational tool.

What makes the study hom-codim$(\mathbb{F}[V]^G)$ in the modular case interesting and tractible is that over a Galois field there is a universal system of parameters for $\mathbb{F}[V]^G$, i.e. depending only on V and not on G or ϱ. We turn to this next.

For the rest of this section, unless stated to the contrary, $\mathbb{F}$ denotes the Galois field $\mathbb{F}_q$ of characteristic p with $q = p^\nu$ elements. The group $\mathrm{GL}(n, \mathbb{F})$ is then a **finite** group of order $(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$ (the classic reference here is [28]). Therefore the ring of invariants of the full linear group, $\mathbb{F}[V]^{\mathrm{GL}(n,\mathbb{F})}$, fits into the context of the polynomial invariants of finite groups. These rings were computed by L. E. Dickson [25] ([29] vol. VI pp. 381–404).

Theorem 4.3 (L. E. Dickson)**.** *Suppose $n \in \mathbb{N}$, p a prime, $q = p^\nu$, $\mathbb{F} = \mathbb{F}_q$ and $V = \mathbb{F}^n$. Then*

$$\mathbb{F}[V]^{\mathrm{GL}(n,\mathbb{F}_q)} = \mathbb{F}_q[V]^{\mathrm{GL}(n,\mathbb{F}_q)} \cong \mathbb{F}_q[\mathbf{d}_{n,0}, \ldots, \mathbf{d}_{n,n-1}]$$

where $\deg(\mathbf{d}_{n,n-i}) = q^n - q^{n-i}$ *for* $i = 1, \ldots, n$. □

This is not the place to present yet another proof of Dickson's remarkable theorem, as there are many modern proofs in the journals, e.g. [117], [113], [110], as well as in books [12] chapter V §5 exercise 6 (a sort of do-it-yourself kit), [9] and [106].

The polynomials $\mathbf{d}_{n,n-i}$, $i = 1, \ldots, n$, are called the **Dickson polynomials** and are unique up to a nonzero scalar. They are the nonzero Chern classes of the only orbit of interest $V^* \setminus \{0\}$ of $\mathrm{GL}(n, \mathbb{F})$ on V^*. The following formula[28]

$$\mathbf{d}_{n,k} = \sum_{\{W < V^* \mid \dim_{\mathbb{F}}(w) = k\}} \left(\prod_{z \notin W} z \right)$$

for the Dickson polynomials was shown to the author independently by R. E. Stong and T. Tamagawa. It has also made its way into the new edition of [68] (page 38 (e)). For example, the **top** Dickson polynomial, i.e. the one with maximal degree, is just the product of all the nonzero linear forms in V^*. The algebra $\mathbb{F}[V]^{\mathrm{GL}(V)}$ is called the **Dickson algebra** and is denoted by $\mathbf{D}^*(n)$, where $n = \dim_{\mathbb{F}}(V)$. Since $\mathbf{D}^*(n) \subset \mathbb{F}[V]^G$ for any representation $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$, and $\mathbf{D}^*(n) \subset \mathbb{F}[V]$ is a finite extension, it follows that the Dickson polynomials

$$\mathbf{d}_{n,n-1}, \ldots, \mathbf{d}_{n,0} \in \mathbb{F}[V]^G$$

form a **universal** system of parameters. Based on the study of cohomology of finite groups and rings of invariants, P. S. Landweber and R. E. Stong made the following very astute conjecture.

Conjecture 4.4 (P. S. Landweber and R. E. Stong)**.** *If $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ is a representation of a finite group over a Galois field, then* hom-codim$(\mathbb{F}[V]^G) \geq k$ *if and only if $\mathbf{d}_{n,n-1}, \ldots, \mathbf{d}_{n,n-k} \in \mathbb{F}[V]^G$ is a regular sequence.*

Note carefully, the order is important (the reason will become apparent in the next section): it is the order of increasing degrees. We will discuss the recent proof of this conjecture by D. Bourguiba and S. Zarati [13] in §6.

The main result of Ellingsrud and Skjelbred [33] shows that whenever the codimension of the fixed point set is at least 2, then hom-codim$(\mathbb{F}[V]^G) \geq 2 + \dim_{\mathbb{F}}(V^G)$.

[28] This formula illustrates once again the utility of the paradigm that the symmetric group is the general linear group over the field with one element, for with this interpretation the Dickson polynomials become the elementary symmetric polynomials.

It would be natural to suppose that a basis for V^{*G} could be extended to a regular sequence of maximal length. However, the example of M. D. Neusel, example 3, shows that this need not be the case. This indicates that the Dickson polynomials must have a subtle property to allow them to detect the homological codimension so accurately.

We close this section with a number of results related to Dickson's theorem and homological codimension of rings of invariants. The first of these is the not surprising result that the p-Sylow subgroup of G controls the Cohen-Macaulay property for $\mathbb{F}[V]^G$ and provides a lower bound for the homological codimension. The following basic change of rings result will be of use in the sequel (see e.g. the do-it-yourself kit [14] exercise 1.2.26).

Proposition 4.5. *Let A and B be graded connected commutative Noetherian algebras over the field $\mathbb{F}$ and $\varphi : A \to B$ a homomorphism of graded algebras. If M is a B-module that is finitely generated as an A-module, then* $\text{hom-codim}_A(M) = \text{hom-codim}_B(M)$. □

Theorem 4.6 (Folklore)**.** *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation of a finite group over a finite field of characteristic p. Then*

$$\text{hom-codim}(\mathbb{F}[V]^G) \geq \text{hom-codim}(\mathbb{F}[V]^{\mathrm{Syl}_p(G)}),$$

where $\mathrm{Syl}_p(G) \leq G$ is a p-Sylow subgroup of G.

Proof. By proposition 4.5 it is equivalent to show

$$\text{hom-codim}_{\mathbf{D}^*(n)}(\mathbb{F}[V]^G) \geq \text{hom-codim}_{\mathbf{D}^*(n)}(\mathbb{F}[V]^{\mathrm{Syl}_p(G)}).$$

Since $|G : \mathrm{Syl}_p(G)|$ is relatively prime to p, we obtain from the Reynolds operator

$$\pi^G_{\mathrm{Syl}_p(G)} = \frac{1}{|G : \mathrm{Syl}_p(G)|} \mathrm{Tr}^G_{\mathrm{Syl}_p(G)} : \mathbb{F}[V]^{\mathrm{Syl}_p(G)} \to \mathbb{F}[V]^G$$

an $\mathbb{F}[V]^G$-module, and hence a fortiori a $\mathbf{D}^*(n)$-module, splitting of the inclusion $\mathbb{F}[V]^G \subseteq \mathbb{F}[V]^{\mathrm{Syl}_p(G)}$.

Suppose that $h_1, \ldots, h_c \in \overline{\mathbf{D}^*(n)}$ is a regular sequence on $\mathbb{F}[V]^{\mathrm{Syl}_p(G)}$. Then $\mathbb{F}[V]^{\mathrm{Syl}_p(G)}$ is a free $\mathbb{F}[\overline{h}_1, \ldots, \overline{h}_c]$-module, where $\overline{h}_i$ acts via h_i on $\mathbb{F}[V]^{\mathrm{Syl}_p(G)}$ for $i = 1, \ldots, c$. The map $\pi^G_{\mathrm{Syl}_p(G)}$ is then an $\mathbb{F}[\overline{h}_1, \ldots, \overline{h}_c]$-module splitting for the inclusion $\mathbb{F}[V]^G \subseteq \mathbb{F}[V]^{\mathrm{Syl}_p(G)}$ and hence $\mathbb{F}[V]^G$ is a projective $\mathbb{F}[\overline{h}_1, \ldots, \overline{h}_c]$-module. By Koszul's theorem (see e.g. [7] appendix A.6 or [106] §6.2) it is then free as an $\mathbb{F}[\overline{h}_1, \ldots, \overline{h}_c]$-module, so $h_1, \ldots, h_c$ is also a regular sequence on $\mathbb{F}[V]^G$. □

Example 4. It can easily happen that $\mathbb{F}[V]^G$ is Cohen-Macaulay even though $\mathbb{F}[V]^{\mathrm{Syl}_p(G)}$ is not. For the symmetric group in its tautological representation, $\mathbb{F}[x_1, \ldots, x_p]^{\Sigma_p}$, p a prime, is a polynomial algebra in the elementary symmetric polynomials and hence Cohen-Macaulay, but the p-Sylow subgroup $\mathbb{Z}/p$ has Cohen-Macaulay invariants if and only if $p = 2$ or 3 [33].

Finally we note briefly another **new feature** of invariant theory in the modular case. In the nonmodular case representations of finite groups are completely reducible, and therefore the algebra of coinvariants $\mathbb{F}[V]_G$, which inherits a G-action from $\mathbb{F}[V]$ since the ideal generated by all the invariant polynomials of positive degree is a G-subspace, is fixed point free; i.e. $(\mathbb{F}[V]_G)^G = \mathbb{F}$ is nothing but the constant polynomials. This is no longer the case in the modular case and the source of a number of new and interesting problems (see e.g. [54] and [83]).

5. The Steenrod algebra and modular invariant theory

In this section we introduce the Steenrod algebra, which is a second new tool of invariant theory over Galois fields. Although the Steenrod operations arose in algebraic topology, their systematic use in invariant theory is very natural. There are several ways to introduce Steenrod operations in a completely algebraic manner, and we have chosen one appropriate to the invariant theory setting. See however [60] for a representation theory-oriented introduction and [118] for one based on differential operators and related to computational problems in algebraic topology. The Steenrod operations and the Steenrod algebra represent one way to organize information hidden in the Frobenius homomorphism. For another way of doing this see [91].

Let $\mathbb{F}$ be the Galois field with $q = p^\nu$ elements and define[29]

$$P(\xi) : \mathbb{F}[V] \to \mathbb{F}[V][[\xi]]$$

by the rules

(i) $P(\xi)$ is $\mathbb{F}$-linear,
(ii) $P(\xi)(v) = v + v^q\xi$ for $v \in V^*$,
(iii) $P(\xi)(u \cdot w) = P(\xi)(u) \cdot P(\xi)(w)$ for $u, w \in \mathbb{F}[V]$,
(iv) $P(\xi)(1) = 1$.

We consider $P(\xi)$ as a ring homomorphism of degree 0 by giving ξ the degree $(1-q)$. (Topologists may want to double the degrees when p is odd.) By separating out homogeneous components we obtain $\mathbb{F}$-linear maps

$$P^i : \mathbb{F}[V] \to \mathbb{F}[V]$$

by the requirement

$$P(\xi)(f) = \sum_{i=0}^{\infty} P^i(f)\xi^i.$$

For $q = 2$ these operations are usually denoted by $Sq^i(f)$.

As defined $P(\xi)$ depends on V, but it is easy to see that $P(\xi)$ is natural with respect to linear maps $\varphi : V' \to V''$, i.e.

$$\varphi^* P(\xi) = P(\xi)\varphi^*$$

where φ^* is the algebra homomorphism induced by φ.

The operations P^i are called the **Steenrod reduced power operations over** $\mathbb{F}$, and when $q = 2$, the operations Sq^i are referred to as **Steenrod squaring operations**. Collectively they are referred to as **Steenrod operations**. They are $\mathbb{F}$-linear maps and in addition satisfy:

$$P^i(u) = \begin{cases} u^q & i = \deg(u) \\ 0 & i > \deg(u) \end{cases}$$

which[30] are called the **unstability conditions**. By the multiplicative property of $P(\xi)$, one has

$$P^k(u \cdot w) = \sum_{i+j=k} P^i(u) \cdot P^j(w) \qquad \forall\ k \in \mathbb{N}_0$$

[29] If A is a ring, then $A[[\xi]]$ denotes the ring of formal power series over A in the variable ξ.
[30] Hence $P(\xi)(f)$ is actually a polynomial in ξ of degree equal to the degree of f.

which are called the **Cartan formulae**. For a linear polynomial $x \in \mathbb{F}[x_1, \ldots, x_n]$ these yield:

$$P^i(x^j) = \binom{j}{i} x^{j+i(q-1)}.$$

If $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ is a representation of a finite group, then the Steenrod operations and the G action on $\mathbb{F}[V]$ commute. Therefore $\mathbb{F}[V]^G$ is mapped into itself by all Steenrod operations. This can be used to produce new invariants from old ones. For example, if G leaves invariant a quadratic form such as $Q = z^2 - xy \in \mathbb{F}[x, y]$ and $\mathbb{F} = \mathbb{F}_2$, then G must also leave the cubic form $Sq^1(Q) = -(x^2y + xy^2)$ invariant, and the quintic form $Sq^2Sq^1(Q) = -(x^4y + xy^4)$ invariant, etc. (See also [102] §8 and [106] §§10.3 and 11.5.)

Clearly the Steenrod operations can be composed, and their compositions satisfy certain identities, such as

$$P^1P^1 = 2P^2,$$

which is easily verified by induction on the dimension of V using the preceding formulae. We define[31] the **Steenrod algebra over** $\mathbb{F}$, denoted by $\mathcal{P}^*$, to be the subalgebra of the graded algebra of endomorphisms of the functor $\mathbb{F}[—]$ from vector spaces to graded connected commutative $\mathbb{F}$ algebras generated by the Steenrod operations.

The Steenrod algebra contains a family of derivations[32] generalizing P^1 defined inductively by the formulae:

$$P^{\Delta_i} = \begin{cases} P^1 & \text{if } i = 1 \\ [P^{\Delta_{i-1}}, P^{p^{i-1}}] & \text{for } i > 1 \end{cases}$$

where $[—, —]$ denotes the commutator of the two arguments. These are very useful both for the theoretical side [1], [2] and for computations.

A complete set of relations between the Steenrod operations over the prime fields was found by a mixture of algebraic and topological methods, and these relations are called **Adem relations**. They were originally conjectured by Wu Wen-Tsün based on his study of the mod p cohomology of Grassmann manifolds [119]. The remarkable discovery of S. R. Bullett and I. G. Macdonald was that these seemingly complex relations could be summarized in one simple identity, the **Bullett-Macdonald identity** [15], which says

$$P(t(1-t)^{q-1}) \cdot P(1) = P((1-t)^{q-1}) \cdot P(t^q) : \mathbb{F}[V] \to \mathbb{F}[V][t].$$

The first operator arises by applying $P(\xi)$, substituting $\xi = 1$, then applying $P(\xi)$ again, substituting $\xi = t(1-t)^{q-1}$, and interpreting the result as an element in $\mathbb{F}[V][t]$. The second operator arises analogously. Given this interpretation, note that each of these operators is multiplicative, so we are required to verify only the identity on $x \in \mathbb{F}[x]$, which follows from the elementary fact that $P(\xi)(x) = x + \xi x^q$.

To obtain the Adem relations from the Bullett-Macdonald identity, one sets $s = t(1-t)^{q-1}$ and notes that the coefficient of s^a in $P(s) \cdot P(1)$ is $\sum P^a P^k$, so the homogeneous component of degree $a + b$ is $P^a \cdot P^b$. An intricate residue calculation

[31] Actually, to a topologist, this is the algebra of **reduced powers** for $q \neq 2$ since we have not included any Bockstein operators.

[32] In 1914 probably no one was aware of the Steenrod operations, but [42] introduced these primitive elements precisely to construct new invariants from old ones.

is used to compute the same component in $P((1-t)^{q-1}) \cdot P(t^q)$, and the result is then the Adem relations. For $q = 2$ they are:

$$Sq^i Sq^j = \sum_{k=0}^{[i/2]} \binom{j-k-1}{i-2k} Sq^{i+j-k} Sq^k$$

for all $i, j > 0$ such that $i < 2j$. For $q \neq 2$ they are:

$$P^i P^j = \sum_{k=0}^{[i/q]} (-1)^{i+1} \binom{(q-1)(j-k)-1}{i-qk} P^{i+j-k} P^k$$

for all $i, j > 0$ such that $i < qj$, where $[a/b]$ denotes the integral part of a/b. The remarkable thing about these relations is that the coefficients always lie in the prime subfield $\mathbb{F}_p < \mathbb{F}$.

Given a sequence $I = (i_1, i_2, \ldots, i_k)$, we write $P^I = P^{i_1} P^{i_2} \cdots P^{i_k}$. These iterations of Steenrod operations are called **basic monomials**. A basic monomial is called **admissible** if $i_s \geq q i_{s+1}$ for $s \geq 1$: they are the basic monomials to which no Adem relation can be applied. There is a surjective map from the free associative algebra with 1 generated by formal Steenrod operations $\{P^i | i \in \mathbb{N}\}$ modulo the ideal generated by the Adem relations onto the Steenrod algebra. In fact, this map is an isomorphism, and hence the Adem relations are a complete set of defining relations for the Steenrod algebra. To wit:

Theorem 5.1. *The admissible monomials are an $\mathbb{F}$-vector space basis for $\mathcal{P}^*$.* □

For a proof based on arguments of J.-P. Serre, H. Cartan and Wu Wen-Tsün see [106] §10.3.

One way in which the Steenrod algebra interacts with invariant theory is through the following remarkable theorem of J.-P. Serre [99]. The proof due to C. W. Wilkerson is short enough to include.

Proposition 5.2 (J.-P. Serre)**.** *If $\mathfrak{p} \subset \mathbb{F}[V]$ is a prime ideal that is invariant under the Steenrod operations, then $\mathfrak{p}$ is generated by $\mathfrak{p} \cap V^*$, i.e. $\mathfrak{p}$ is generated by the classes of degree one that it contains.*

Proof. Consider the quotient map

$$\pi : \mathbb{F}[V] \to \mathbb{F}[V]/\mathfrak{p},$$

and let $z_1, \ldots, z_m \in \pi(V^*)$ be a basis. Then $z_1, \ldots, z_m$ generate $\mathbb{F}[V]/\mathfrak{p}$ as an algebra. Since $\deg(z_1) = \cdots = \deg(z_m) = 1$ we have

$$P^{\Delta_i}(z_j) = z_j^{q^i} \qquad j = 1, \ldots, m \quad i = 1, \ldots$$

and hence letting $i = 0, \ldots, m-1$ and $j = 1, \ldots, m$

$$\deg(\mathcal{P}^{\Delta_i}(z_j)) = \det(z_j^{q^i}).$$

This determinant was evaluated in [26] (see also [2] lemma 5.9) by L. E. Dickson, who showed that in $\mathbb{F}[V]$ it is the product of one nonzero linear form from each line in $\mathrm{Span}_{\mathbb{F}}\{z_1, \ldots, z_m\}$, and hence not in $\mathfrak{p}$. A standard lemma on derivations ([106] lemma 5.6.1) implies that $z_1, \ldots, z_m$ are algebraically independent, and the result follows. □

It is convenient to introduce some terminology at this point. We say that a graded connected commutative algebra H is an **unstable algebra over the Steenrod algebra** when H is a graded $\mathcal{P}^*$-module that satisfies the unstability condition and the Cartan formulae. An ideal in H is called $\mathcal{P}^*$-**invariant** if it is mapped into itself by all Steenrod operations. The following theorem (see [108]) generalizes the basic overlying theorem optimally to the new context.

Theorem 5.3 (M. D. Neusel [86])**.** *Suppose that $A' \supseteq A''$ is a finite integral extension of unstable Noetherian algebras over the Steenrod algebra $\mathcal{P}^*$. If $\mathfrak{p}'' \subset A''$ is a $\mathcal{P}^*$-invariant prime ideal, then every prime ideal $\mathfrak{p}' \subset A'$ with $\mathfrak{p}' \cap A'' = \mathfrak{p}''$ is also $\mathcal{P}^*$-invariant.* □

Another basic fact from commutative algebra is the Lasker-Noether decomposition of an ideal [31] chapter 3 or [6] §2.3. If I is any ideal in a graded commutative Noetherian algebra H over a field, this theorem says there are a finite number of primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ such that

(i) $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$;
(ii) no $\mathfrak{q}_i$ contains $\bigcap_{i \neq j} \mathfrak{q}_j$;
(iii) if $j \neq i$, then $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$.

Such a representation of I as the intersection of primary ideals is called an **irredundant minimal primary decomposition** of I. If

$$\mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_{n'} = I = \mathfrak{q}''_1 \cap \cdots \cap \mathfrak{q}''_{n''}$$

are two irredundant minimal primary decompositions of I, then $n' = n''$ and, after reordering, $\sqrt{\mathfrak{q}'_i} = \sqrt{\mathfrak{q}''_i}$. The prime ideals $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ are thus independent of the choice of minimal irredundant primary decomposition of I and are called the **associated primes** of I. Minimal primes among the associated primes of I are also called **isolated primes** of I. The isolated primes of I are the minimal prime ideals among those that include I, and $\sqrt{I}$ is the intersection of the isolated primes of I. This theorem too has a $\mathcal{P}^*$-invariant analog, namely [88]:

Theorem 5.4 (M. D. Neusel and L. Smith)**.** *Let H^* be an unstable Noetherian algebra over $\mathbb{F}$ and $I \subseteq H^*$ a $\mathcal{P}^*$-invariant ideal. Then the associated prime ideals of I are $\mathcal{P}^*$-invariant and there exists a minimal irredundant primary decomposition*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

with $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ $\mathcal{P}^*$-invariant primary ideals. □

As an immediate consequence of these results we obtain an application (see [108]) to the transfer homomorphism $\mathrm{Tr}^G : \mathbb{F}[V] \to \mathbb{F}[V]^G$.

Corollary 5.5. *Let $\varrho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation of a finite group over the Galois field $\mathbb{F}$. Then some power of the top Dickson polynomial $\mathbf{d}_{n,0}$ belongs to* $\mathrm{Im}(\mathrm{Tr}^G)$.

Proof. The transfer homomorphism commutes with Steenrod operations so $\mathrm{Im}(\mathrm{Tr}^G) \subseteq \mathbb{F}[V]^G$ is a $\mathcal{P}^*$-invariant ideal. Since the radical of $\mathrm{Im}(\mathrm{Tr}^G)$ is the intersection of its minimal primes, and these are $\mathcal{P}^*$-invariant by theorem 5.4, it follows that $\sqrt{\mathrm{Im}(\mathrm{Tr}^G)}$ is a $\mathcal{P}^*$-invariant ideal. In this modular context[33] the transfer cannot

[33]This is a standard fact from field theory; see e.g. [23] volume 2 proposition 9.6.

be identically zero, so $\sqrt{\mathrm{Im}(\mathrm{Tr}^G)} \neq (0)$. If $\mathfrak{p}$ is a minimal prime of $\mathrm{Im}(\mathrm{Tr}^G)$, then lying over it is a $\mathcal{P}^*$-invariant ideal $\tilde{\mathfrak{p}}$ in $\mathbb{F}[V]$. The ideal $\tilde{\mathfrak{p}}$ is generated by nonzero linear forms by Serre's theorem, 5.2, so must contain the top Dickson class, which is the product of all nonzero linear forms in $\mathbb{F}[V]$. Since the top Dickson class is also invariant it must be in every minimal prime of $\mathrm{Im}(\mathrm{Tr}^G)$, and the result follows. □

For more information (and examples) about the transfer in the modular case see also [19], [57], and [61]. In addition to Serre's theorem on the structure of the $\mathcal{P}^*$-invariant ideals in $\mathbb{F}[V]$ Landweber has obtained a structure theorem for the $\mathcal{P}^*$-invariant ideals in the Dickson algebra. Here it is:

Theorem 5.6 (P. S. Landweber)**.** *The only $\mathcal{P}^*$-invariant prime ideals in the Dickson algebra $\mathbf{D}^*(n)$ are $(\mathbf{d}_{n,0}, \mathbf{d}_{n,1}, \ldots, \mathbf{d}_{n,i})$ $i = 0, \ldots, n-1$.* □

Note that the sequence of Dickson polynomials conjectured by P. S. Landweber and R. E. Stong to be a regular sequence in $\mathbb{F}[V]^G$ is the complement of a sequence generating a $\mathcal{P}^*$-invariant ideal. It would have been nice if $\mathbf{D}^*(n)$ were characterized by its $\mathcal{P}^*$-invariant prime ideal spectrum. This is, however, far from the case (see [86]).

6. All together now: The depth conjecture

If $\mathbb{F}[V]^G$ is a ring of invariants over the Galois field $\mathbb{F}$ with $q = p^\nu$ elements, then it supports two additional structures; viz.

— it is a module (actually an algebra) over the Dickson algebra $\mathbf{D}^*(n)$, $n = \dim_{\mathbb{F}}(V)$, and
— it is an unstable algebra over the Steenrod algebra $\mathcal{P}^*$.

Moreover, these structures are related by the Cartan formulae. We summarize this by saying[34] $\mathbb{F}[V]^G$ is an **unstable $\mathbf{D}^*(n) \odot \mathcal{P}^*$-algebra**. Proposition 4.5 tells us that the codimension of $\mathbb{F}[V]^G$ as algebra is equal to its codimension as $\mathbf{D}^*(n)$-module. It is in this context that one can best understand the conjecture 4.4 of P. S. Landweber and R. E. Stong: namely, it should be viewed as a statement about the codimension of Noetherian unstable $\mathbf{D}^*(n) \odot \mathcal{P}^*$-modules[35]. A Noetherian $\mathbf{D}^*(n)$-module has a prime filtration, i.e. a filtration by $\mathbf{D}^*(n)$-submodules

$$\{0\} = M_0 \subset M_1 \subset \cdots \subset M_k = M \tag{6.1}$$

satisfying[36]

$$M_i/M_{i-1} \cong \sum^{m_i} (\mathbf{D}^*(n)/\mathfrak{p}_i) \qquad i = 1, \ldots, k$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are prime ideals in $\mathbf{D}^*(n)$, $m_1, \ldots, m_k \in \mathbb{N}_0$. If we knew that there existed a prime filtration by $\mathbf{D}^*(n) \odot \mathcal{P}^*$-submodules, then each $\mathfrak{p}_i$ would be a $\mathcal{P}^*$-invariant prime ideal, and hence by Landweber's theorem (theorem 5.6)

$$\mathfrak{p}_i = (\mathbf{d}_{n,0}, \ldots, \mathbf{d}_{n,l_i}) \qquad i = 1, \ldots, k,$$

[34]The **semitensor product** construction was introduced by W. S. Massey and F. P. Peterson in [66] to convert an algebra with such a mixed structure into an ordinary algebra over $\mathbf{D}^*(n) \odot \mathcal{P}^*$, the semitensor product of $\mathbf{D}^*(n)$ and $\mathcal{P}^*$. We do not need the construction, but we will use the notation.

[35]See definition following.

[36]For a graded object N, $\sum^k(N)$ is the graded object defined by $\sum^k(N)_j = N_{j-k}$, for $j \in \mathbb{N}_0$.

and a simple induction argument on k would prove the depth conjecture. However, the existence of such a filtration is at present not known, so instead of using the prime filtration theorem, which is a key step in the usual proof of the Lasker-Noether theorem for modules ([31] chapter 3 or [6] §2.4), we will make use of another approach to the Lasker-Noether theorem for modules ([31] appendix 3 exercises A3.4 and A3.5) to prove the depth conjecture. An essential ingredient in this approach is the existence, and structure, of injective hulls in the category of Noetherian unstable $\mathbf{D}^*(n) \odot \mathcal{P}^*$-modules. It is, however, easier, and for our purposes equivalent, to consider Noetherian unstable $\mathbb{F}[V] \odot \mathcal{P}^*$-modules and the structure of their injective hulls. It is at this point that the Steenrod algebra enters in a decisive way into the proof of the depth conjecture. The discussion that follows is of necessity brief, and we refer to the original sources [63], [64], [13] or the fine book [97] for the missing details.

An unstable $\mathbb{F}[V] \odot \mathcal{P}^*$-module M is a module over both $\mathbb{F}[V]$ and $\mathcal{P}^*$ that satisfies the **unstability condition for $\mathcal{P}^*$-modules**, namely $P^k(x) = 0$ if $k > \deg(x)$, and the Cartan formulae

$$P^k(f \cdot x) = \sum_{i+j=k} P^i(f) \cdot P^j(x) \qquad \forall f \in \mathbb{F}[V], x \in M.$$

The category of such modules is denoted by $\mathcal{U}_{\mathbb{F}[V]}$. For an unstable $\mathbb{F}[V] \odot \mathcal{P}^*$-module M we define functors

$$\mathbf{\Upsilon}^k(M) := \mathrm{Hom}_{\mathbb{F}}(M_k, \mathbb{F}) \qquad k \in \mathbb{N}_0.$$

These are exact functors, and preserve direct sums, and therefore are representable (see e.g. [97] 2.2.1). We denote by $\mathbf{J}_{\mathbb{F}[V]\odot\mathcal{P}^*}(k)$ the representing module, so that

$$\mathrm{Hom}_{\mathbb{F}[V]\odot\mathcal{P}^*}(M_k, \mathbf{J}_{\mathbb{F}[V]\odot\mathcal{P}^*}(k)) = \mathrm{Hom}_{\mathbb{F}}(M_k, \mathbb{F}) = \mathrm{Hom}_{\mathbb{F}[V]\odot\mathcal{P}^*}(M, \sum^k \mathbb{F}). \tag{6.2}$$

The functor $\mathbf{\Upsilon}^k$ being exact, these modules $\mathbf{J}_{\mathbb{F}[V]\odot\mathcal{P}^*}(k)$ are injective objects in $\mathcal{U}_{\mathbb{F}[V]}$. For any unstable $\mathbf{D}^*(n) \odot \mathcal{P}^*$-module M the natural map

$$M \to \prod_{\varphi \in \mathbf{\Upsilon}^k(M)} \mathbf{J}_{\mathbb{F}[V]\odot\mathcal{P}^*}(k) \cdot \varphi$$

given by the adjointness relation (6.2) embeds M in an injective object of the category $\mathcal{U}_{\mathbb{F}[V]}$, so the category $\mathcal{U}_{\mathbb{F}[V]}$ has enough injectives, and each object M in $\mathcal{U}_{\mathbb{F}[V]}$ has an **injective hull** in $\mathcal{U}_{\mathbb{F}[V]}$ which we denote by $\mathbf{E}_{\mathbb{F}[V]\odot\mathcal{P}^*}(M)$.

For a Noetherian unstable $\mathbb{F}[V] \odot \mathcal{P}^*$-module the injective hull is a finite direct sum of certain basic injectives that we describe next. If $i_W : W \leq V$ is a vector subspace, then the inclusion induces a map $i_W^* : \mathbb{F}[V] \to \mathbb{F}[W]$ whose kernel is denoted by $\mathfrak{p}_W$. The quotient map $V \to V/W$ induces an inclusion $\mathbb{F}[V/W] \subseteq \mathbb{F}[V]$, and $\mathfrak{p}_W$ is the ideal in $\mathbb{F}[V]$ generated by the linear forms in the image of this map. Via i_W^* we may regard $\Sigma^k(\mathbb{F}[W]) = \Sigma^k(\mathbb{F}[V]/\mathfrak{p}_W)$ as an object in $\mathcal{U}_{\mathbb{F}[V]}$, and there it has an injective hull, which we denote by $\mathbf{E}(V, W, k)$. The natural map

$$\Sigma^k(\mathbb{F}[W]) = \mathbb{F}[V] \otimes_{\mathbb{F}[V/W]} \Sigma^k(\mathbb{F}) \to \mathbb{F}[V] \otimes_{\mathbb{F}[V/W]} \mathbf{J}_{\mathbb{F}[V/W]}(k)$$

induces an isomorphism [64]

$$\mathbb{F}[V] \otimes_{\mathbb{F}[V/W]} \mathbf{J}_{\mathbb{F}[V/W]}(k) \to \mathbf{E}(V, W, k).$$

The basic structure theorem that we need is:

Theorem 6.1 (J. Lannes and S. Zarati [64])**.** *Let M be a Noetherian unstable $\mathbb{F}[V] \odot \mathcal{P}^*$-module. Then*

$$\mathbf{E}_{\mathbb{F}[V]\odot\mathcal{P}^*}(M) = \bigoplus \mathbf{E}(V,W,k)^{a_M(W,k)}$$

where

(i) *W ranges over the subspaces $W \leq V$ (a finite set),*
(ii) *$k, a_M(W,k) \in \mathbb{N}_0$, and*
(iii) *for a given $W \leq V$ only finitely many $a_M(W,k)$ are nonzero.* □

It is via this theorem that the Steenrod algebra enters into the proof of the depth conjecture in a central way. The key step in the proof is:

Theorem 6.2 (D. Bourguiba and S. Zarati)**.** *If M is a Noetherian unstable $\mathbb{F}[V] \odot \mathcal{P}^*$-module, then* $\text{hom-codim}_{\mathbb{F}[V]}(M) \leq \text{hom-codim}_{\mathbb{F}[V]}(\mathbf{E}_{\mathbb{F}[V]\odot\mathcal{P}^*}(M))$.

The proof of this theorem will occupy most of the rest of this section. It is different from the one in [13] in that we do not make use of the functors $\text{Fix}(V,W)$ nor do we make any direct use of T-technology[37]. Instead we solve [31] appendix 3 exercises A3.4 and A3.3 in this new context.

Proof. By the structure theorem for injective hulls, 6.1,

$$\mathbf{E}_{\mathbb{F}[V]\odot\mathcal{P}^*}(M) = \bigoplus \mathbf{E}(V,W,k)^{a_M(W,k)},$$

and therefore

$$\begin{aligned}&\text{hom-codim}_{\mathbb{F}[V]}(\mathbf{E}_{\mathbb{F}[V]\odot\mathcal{P}^*}(M))\\ &\quad = \min\{\text{hom-codim}_{\mathbb{F}[V]\odot\mathcal{P}^*}(\mathbf{E}(V,W,k)) \mid a_M(W,k) \neq 0\}.\end{aligned}$$

Fix once and for all a $W \leq V$ such that $a_M(W,k) \neq 0$ and

$$\text{hom-codim}_{\mathbb{F}[V]}(\mathbf{E}_{\mathbb{F}[V]\odot\mathcal{P}^*}(M)) = \text{hom-codim}_{\mathbb{F}[V]}(\mathbf{E}(V,W,k).$$

Lemma 6.3. *Every element of $\mathbf{E}(V,W,k)$ is annihilated by some power of $\mathfrak{p}_W$.*

Proof. By the Artin-Rees lemma ([31] chapter 5 lemma 5.1) there exists an integer $n \in \mathbb{N}$ such that $\forall l \in \mathbb{N}$

$$\begin{aligned}&(\mathfrak{p}_W^{n+l} \cdot \mathbf{E}(V,W,k)) \bigcap (\Sigma^k(\mathbb{F}[W]))\\ &\quad = \mathfrak{p}_W^l \cdot \Big((\mathfrak{p}_W^n \cdot \mathbf{E}(V,W,k)) \bigcap (\Sigma^k(\mathbb{F}[W]))\Big)\\ &\quad = \mathfrak{p}_W^{n+l}\mathbf{E}(V,W,k) \bigcap \mathfrak{p}_W^l \Sigma^k(\mathbb{F}[W]) \subseteq \mathbf{E}(V,W,k) \bigcap \{0\} = \{0\}.\end{aligned}$$

The subset $\mathfrak{p}_W^{n+l} \cdot \mathbf{E}(V,W,k) \subseteq \mathbf{E}(V,W,k)$ is an $\mathbb{F}[V] \odot \mathcal{P}^*$-submodule since $\mathfrak{p}_W$ is a $\mathcal{P}^*$-invariant ideal. The inclusion into the injective hull $\Sigma^k(\mathbb{F}[W]) \hookrightarrow \mathbf{E}(V,W,k)$ is an essential monomorphism in the category $\mathcal{U}_{\mathbb{F}[V]}$, so it follows that $\mathfrak{p}_W^{n+l} \cdot \mathbf{E}(V,W,k) = \{0\}$. In particular, $\mathfrak{p}_W^{n+1} \cdot \mathbf{E}(V,W,k) = \{0\}$ as required. □

[37] This is not meant to imply that these functors and technology are uninteresting. Quite the contrary; T-technology has proven a very useful tool in algebraic topology (see e.g. [97] and the many references there), and the functors $\text{Fix}(—,—)$ are very natural. We just wish to emphasize that given the one structure theorem 6.1 for injective hulls, the proof can be developed almost entirely in the context of traditional commutative algebra, with the key additional fact that the Steenrod algebra acts unstably on everything.

The inclusion $M \hookrightarrow \mathbf{E}_{\mathbb{F}[V]\odot\mathcal{P}^*}(M)$ is also an essential monomorphism and $\mathbf{E}(V,W,k) \subseteq \mathbf{E}_{\mathbb{F}[V]\odot\mathcal{P}^*}(M)$ since $a_M(W,k) \neq 0$. Therefore $M \cap \mathbf{E}(V,W,k) \neq \{0\}$, and hence there is an element $0 \neq x \in M$ also annihilated by some power of $\mathfrak{p}_W$. Let l be the smallest integer so that $\mathfrak{p}_W^l \subseteq \mathrm{Ann}_{\mathbb{F}[V]}(x)$. If $l = 0$, set $y = x$; otherwise choose a nonzero element y in $\mathfrak{p}_W^{l-1} \cdot x$. Then $0 \neq y \in M$ is annihilated by $\mathfrak{p}_W$. An easy Koszul complex argument then yields:

Lemma 6.4. $\text{hom-dim}_{\mathbb{F}[V]}(M) \geq \mathrm{ht}(\mathfrak{p}_W)$.

Proof. Let[38] $r = \dim_{\mathbb{F}}(W)$ and $s = n - r = \dim_{\mathbb{F}}(V/W) = \mathrm{ht}(\mathfrak{p}_W)$. Choose a basis $x_1, \ldots, x_s$ for the linear forms in $\mathfrak{p}_W$ and adjoin $z_1, \ldots, z_r$ to them to obtain a basis for V^*, the linear forms in $\mathbb{F}[V]$. Then

$$\mathrm{Tor}^*_{\mathbb{F}[V]}(\mathbb{F}[W], M) = \mathrm{Tor}^*_{\mathbb{F}[x_1,\ldots,x_s,z_1,\ldots,z_r]}(\mathbb{F}[z_1,\ldots,z_r], M) \cong \mathrm{Tor}^*_{\mathbb{F}[x_1,\ldots,x_s]}(\mathbb{F}, M).$$

If we use the Koszul complex[39]

$$\mathcal{K} = \mathbb{F}[x_1,\ldots,x_s] \otimes E(u_1,\ldots,u_s)$$
$$\partial(f \otimes 1) = 0, \qquad \forall f \in \mathbb{F}[x_1,\ldots,x_s], \qquad \partial(1 \otimes u_i) = x_i \otimes 1 \quad \text{for } i = 1,\ldots,s$$

to compute this torsion product, we find

$$u_1 \cdots u_s \otimes y \neq 0 \in \mathcal{K} \otimes_{\mathbb{F}[x_1,\ldots,x_s]} M$$

is a nonzero cycle (since $x_i \cdot y = 0$ for $i = 1,\ldots,s$) and cannot be a boundary since there are no chains of homological degree $s+1$. Hence we conclude

$$\mathrm{Tor}^s_{\mathbb{F}[V]}(\mathbb{F}[W], M) = \mathrm{Tor}^s_{\mathbb{F}[V]}(\mathbb{F}[z_1,\ldots,z_r], M) \neq 0$$

and therefore $\text{hom-dim}_{\mathbb{F}[V]}(M) \geq s = \mathrm{ht}(\mathfrak{p}_W)$ as claimed. □

Lemma 6.5. $\text{hom-dim}_{\mathbb{F}[V]}(\mathbf{E}(V,W,k)) = \mathrm{ht}(\mathfrak{p}_W)$.

Proof. Recall that

$$\mathbf{E}(V,W,k) = \mathbb{F}[V] \otimes_{\mathbb{F}[V/W]} \mathbf{J}_{\mathbb{F}[V/W]}(k)$$

and $\mathbf{J}_{\mathbb{F}[V/W]}(k)$ itself is a totally finite graded vector space. If we employ the Koszul complex

$$\mathcal{L} = E(u_1,\ldots,u_s,w_1,\ldots,w_r) \otimes \mathbb{F}[V]$$
$$\partial(1 \otimes f) = 0 \qquad \forall f \in \mathbb{F}[V], \qquad \partial(u_i \otimes 1) = 1 \otimes x_i \quad \text{for } i = 1,\ldots,s,$$
$$\partial(w_j \otimes 1) = 1 \otimes z_j \quad \text{for } j = 1,\ldots,r$$

to resolve $\mathbb{F}$ as an $\mathbb{F}[V]$-module, we find

$$\begin{aligned}
\mathrm{Tor}^*_{\mathbb{F}[V]}(\mathbb{F}, \mathbf{E}(V,W,k)) &= H(\mathcal{L} \otimes_{\mathbb{F}[V]} \mathbf{E}(V,W,k)) \\
&= H(E(u_1,\ldots,u_s,w_1,\ldots,w_r) \otimes \mathbb{F}[V] \otimes_{\mathbb{F}[V]} \mathbb{F}[V] \otimes_{\mathbb{F}[V/W]} \mathbf{J}_{\mathbb{F}[V/W]}(k)) \\
&= H(E(u_1,\ldots,u_s,w_1,\ldots,w_r) \otimes \mathbb{F}[V] \otimes_{\cancel{\mathbb{F}[V]}} \cancel{\mathbb{F}[V]} \otimes_{\mathbb{F}[V/W]} \mathbf{J}_{\mathbb{F}[V/W]}(k)) \\
&= H(E(u_1,\ldots,u_s) \otimes (E(w_1,\ldots,w_r) \otimes \mathbb{F}[W]) \otimes \mathbf{J}_{\mathbb{F}[V/W]}(k)) \\
&= E(u_1,\ldots,u_s) \otimes \mathbf{J}_{\mathbb{F}[V/W]}(k)
\end{aligned}$$

[38] $\mathrm{ht}(\mathfrak{p}_W)$ denotes the **height** of the ideal $\mathfrak{p}_W$.
[39] See [106] §6.2 for the notation we are using.

since the Koszul complex

$$E(w_1,\dots,w_r)\otimes\mathbb{F}[W]$$
$$\partial(1\otimes f)=0 \qquad \forall f\in\mathbb{F}[W], \qquad \partial(w_j\otimes 1)=z_j \quad \text{for } j=1,\dots,r$$

is acyclic, and the differential in the complex

$$E(u_1,\dots,u_s)\otimes\mathbf{J}_{\mathbb{F}[V/W]}(k)$$

is trivial, because $x_1,\dots,x_s\in\mathfrak{p}_W$ and $\mathfrak{p}_W$ annihilates $\mathbf{J}_{\mathbb{F}[V/W]}(k)$. Therefore

$$\operatorname{Tor}^s_{\mathbb{F}[V]}(\mathbb{F},\mathbf{E}(V,W,k))\neq 0$$
$$\operatorname{Tor}^{s+1}_{\mathbb{F}[V]}(\mathbb{F},\mathbf{E}(V,W,k))=0$$

and hence $\text{hom-dim}_{\mathbb{F}[V]}(\mathbf{E}(V,W,k))=s$ as claimed. □

Combining lemmas 6.4 and 6.5, we obtain

$$\text{hom-dim}_{\mathbb{F}[V]}(M)\geq \operatorname{ht}(\mathfrak{p}_W)=\text{hom-dim}_{\mathbb{F}[V]}(\mathbf{E}(V,W,k)),$$

and therefore the theorem follows from the Auslander-Buchsbaum equality. □

We next investigate when the Dickson polynomials $\mathbf{d}_{n,n-1},\dots,\mathbf{d}_{n,n-r}\mathbb{F}[V]$ are a regular sequence on one of the modules $\mathbf{E}(V,W,k)$. The following lovely lemma and its proof are due to Dorra Bourguiba and Said Zarati.

Lemma 6.6 (D. Bourguiba and S. Zarati)**.** *Let $V=\mathbb{F}^n$ and $W\leq V$ be an r-dimensional vector subspace. If N is a totally finite $\mathbb{F}[V/W]\odot\mathcal{P}^*$-module, then $\mathbf{d}_{n,n-1},\dots,\mathbf{d}_{n,n-r}\in\mathbb{F}[V]$ is a regular sequence on $\mathbb{F}[V]\otimes_{\mathbb{F}[V/W]}N$.*

Proof. Suppose first that N is a trivial $\mathbb{F}[V/W]$-module. Then

$$\mathbb{F}[V]\otimes_{\mathbb{F}[V/W]}N\cong\mathbb{F}[W]\otimes_{\mathbb{F}}N$$

as $\mathbb{F}[V]$-modules. Under the natural map $\mathbb{F}[V]\to\mathbb{F}[W]$ the Dickson polynomials $\mathbf{d}_{n,n-1},\dots,\mathbf{d}_{n,n-r}\in\mathbb{F}[V]$ map to $\mathbf{d}_{r,r-1}^{q^{n-r}},\dots,\mathbf{d}_{r,0}^{q^{n-r}}\in\mathbb{F}[W]$. These form a regular sequence on $\mathbb{F}[W]$ and hence also on $\mathbb{F}[W]\otimes N$, since this is just a direct sum of degree-shifted copies of $\mathbb{F}[W]$.

If N is totally finite but not trivial, then there exists $d\in\mathbb{N}_0$ such that $N_d\neq 0$ but $N_m=0$ for $m>d$. Let N' be the graded submodule of N defined by

$$N'_m=\begin{cases}N_d & \text{for } m=d\\ 0 & \text{otherwise.}\end{cases}$$

Then $N'\subseteq N$ is an $\mathbb{F}[V]\odot\mathcal{P}^*$-submodule, and there is an exact sequence

$$0\to N'\to N\to N''\to 0$$

of $\mathbb{F}[V]\odot\mathcal{P}^*$-modules. The module N'' is also totally finite with $\dim_{\mathbb{F}}(N'')<\dim_{\mathbb{F}}(N)$, and N' is a trivial $\mathbb{F}[V]\odot\mathcal{P}^*$-module. Hence by induction on the dimension of the totally finite module we obtain that $\mathbf{d}_{n,n-1},\dots,\mathbf{d}_{n,n-r}\in\mathbb{F}[V]$ is a regular sequence on both $\mathbb{F}[V]\otimes_{\mathbb{F}[V/W]}N'$ and $\mathbb{F}[V]\otimes_{\mathbb{F}[V/W]}N''$. The functor $\mathbb{F}[V]\otimes_{\mathbb{F}[V/W]}$ — is exact since $\mathbb{F}[V]$ is a free $\mathbb{F}[V/W]$-module. Applying this functor to the preceding exact sequence, we see that the end terms are free $\mathbb{F}[\mathbf{d}_{n,n-1},\dots,\mathbf{d}_{n,n-r}]$-modules; therefore by exactness so is the middle term. □

Since $\mathbf{E}(V,W,k)=\mathbb{F}[V]\otimes_{\mathbb{F}[V/W]}\mathbf{J}_{\mathbb{F}[V/W]}(k)$ and $\mathbf{J}_{\mathbb{F}[V/W]}(k)$ is totally finite, we obtain from this lemma:

Proposition 6.7 (D. Bourguiba and S. Zarati)**.** *If V is an n-dimensional $\mathbb{F}$-vector space and $W \leq V$ an r-dimensional subspace, then $\mathbf{d}_{n,n-1}, \ldots, \mathbf{d}_{n,n-r} \in \mathbb{F}[V]$ is a regular sequence on $\mathbf{E}(V, W, k)$.* □

Corollary 6.8 (D. Bourguiba and S. Zarati)**.** *If M is a Noetherian unstable $\mathbb{F}[V] \odot \mathcal{P}^*$-module, then* $\text{hom-codim}_{\mathbb{F}[V]} = \min\{\text{codim}_{\mathbb{F}}(W \subseteq V) | a_M(W, k) \neq 0\}$. □

We can now prove the main result of D. Bourguiba and S. Zarati.

Theorem 6.9 (D. Bourguiba and S. Zarati)**.** *Let M be a Noetherian unstable $\mathbb{F}[V] \odot \mathcal{P}^*$-module with* $\text{hom-codim}_{\mathbb{F}[V]} \geq r$. *Then $\mathbf{d}_{n,n-1}, \ldots, \mathbf{d}_{n,n-r} \in \mathbb{F}[V]$ is a regular sequence on M.*

Proof. Consider the exact sequence arising from the inclusion into the injective hull

$$0 \to M \xrightarrow{e} \mathbf{E}_{\mathbb{F}[V] \odot \mathcal{P}^*}(M) \xrightarrow{f} N \to 0.$$

By theorem 6.2 $\text{hom-codim}_{\mathbb{F}[V]}(\mathbf{E}_{\mathbb{F}[V] \odot \mathcal{P}^*}(M)) \geq r$. Therefore one sees (e.g. using the characterization of codimension in terms of the functors $\text{Ext}_{\mathbb{F}[V]}(—, \mathbb{F})$ [14] §1.2 or [106] §6.6) that $\text{hom-codim}_{\mathbb{F}[V]}(N) \geq r - 1$.

By induction we may suppose that $\mathbf{d}_{n,n-1}, \ldots, \mathbf{d}_{n,n-(r-1)}$ is a regular sequence on M and on N, whereas corollary 6.8 and the Lannes-Zarati structure theorem 6.1 imply that $\mathbf{d}_{n,n-1}, \ldots, \mathbf{d}_{n,n-r}$ is a regular sequence on $\mathbf{E}_{\mathbb{F}[V] \odot \mathcal{P}^*}(M)$. It is an easy matter from this to prove that $\mathbf{d}_{n,n-1}, \ldots, \mathbf{d}_{n,n-r}$ is a regular sequence on M. □

The functor $\mathbb{F}[V] \otimes_{\mathbf{D}^*(n)} —$ is exact and $\mathbf{D}^*(n) \leq \mathbb{F}[V]$ is a finite extension, hence

$$\begin{aligned} \text{hom-codim}_{\mathbf{D}^*(n)}(M) &= \text{hom-codim}_{\mathbf{D}^*(n)}(\mathbb{F}[V] \otimes_{\mathbf{D}^*(n)} M) \\ &= \text{hom-codim}_{\mathbb{F}[V]}(\mathbb{F}[V] \otimes_{\mathbf{D}^*(n)} M), \end{aligned}$$

and the sequence $\mathbf{d}_{n,n-1}, \ldots, \mathbf{d}_{n,n-r}$ is a regular sequence on $\mathbb{F}[V] \otimes_{\mathbf{D}^*(n)} M$ if and only if it is a regular sequence on M. Therefore we obtain

Corollary 6.10 (D. Bourguiba and S. Zarati)**.** *Let M be a Noetherian unstable $\mathbf{D}^*(n) \odot \mathcal{P}^*$-module with* $\text{hom-codim}_{\mathbf{D}^*(n)}(M) \geq r$. *Then $\mathbf{d}_{n,n-1}, \ldots, \mathbf{d}_{n,n-r} \in D^*(n)$ is a regular sequence on M.* □

This corollary includes the depth conjecture as the special case where $M = \mathbb{F}[V]^G$ is a ring of invariants. The proof of the depth conjecture makes clear the significance of developing a commutative algebra for algebras and modules over the Steenrod algebra and the desirability of a convergence in the view emanating from the germinal article [91] and the emerging one coming out of algebraic topology [87].

References

[1] J. F. Adams and H. R. Margolis, *Modules over the Steenrod Algebra*, Topology **10** (1971), 271–282. MR **45:**3520

[2] J. F. Adams and C. W. Wilkerson, *Finite H-spaces and algebras over the Steenrod algebra*, Ann. of Math. **111** (1980), 95–143; *Finite H-spaces and algebras over the Steenrod algebra: A correction* **113** (1981), 621–622. MR **81h:**55006; MR **82i:**55010

[3] A. Adem and R. J. Milgram, *Cohomology of finite groups*, Springer-Verlag, Heidelberg, Berlin, New York, 1994. MR **96f:**20082
[4] G. Almkvist, *Some formulas in invariant theory*, J. Algebra **77** (1982), 338–359. MR **84i:**14030
[5] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Menlo Park, CA, 1969. MR **39:**4129
[6] S. Bałcerzyk and T. Józefiak, *Commutative Noetherian and Krull rings*, ARS-Polona, 1989. MR **92f:**13001
[7] ———, *Commutative rings*: *Dimension, multiplicity and homological methods*, ARS-Polona, 1989. MR **92b:**13001
[8] G. Barbançon and M. Raïs, *Sur le théorème de Hilbert différentiable pour les groupes linéaires finis*, Ann. Sci. École Norm. Sup. (4) **16** (1983), 355–373. MR **86b:**58010
[9] D. Benson, *Polynomial invariants of finite groups*, Cambridge Univ. Press, London, 1993. MR **94j:**13003
[10] M.-J. Bertin, *Anneau des invariants du groupe alterné, en caractéristique* 2, Bull. Sci. Math. France **94** (1970), 65–72. MR **42:**1819
[11] ———, *Anneaux d'invariants d'anneaux de polynômes en caractéristique p*, C. R. Acad. Sci. Paris Série A **264** (1967), 653–656. MR **35:**6661
[12] N. Bourbaki, *Eléments de mathématiques*: *Groupes et algèbres de Lie*, Masson, Paris, 1981. MR **39:**1590
[13] D. Bourguiba and S. Zarati, *Depth and Steenrod operations*, Preprint, Univ. of Tunis II, 1995.
[14] W. Bruns and J. Herzog, *Cohen-Macaulay rings*, Cambridge Stud. Adv. Math., vol. 39, Cambridge Univ. Press, Cambridge, 1993. MR **95h:**13020
[15] S. R. Bullett and I. G. Macdonald, *On the Adem relations*, Topology **21** (1982), 329–332. MR **83h:**55035
[16] H. E. A. Campbell, J. C. Harris, and D. L. Wehlau, *On rings of invariants of non-modular Abelian groups*, Preprint, Queens Univ., 1996.
[17] H. E. A. Campbell and I. P. Hughes, 2*-Dimensional invariants of* $\mathrm{GL}(2,\mathbb{F}_p)$ *and some of its subgroups over the field* $\mathbb{F}_p$, Preprint, Queens Univ., 1993.
[18] H. E. A. Campbell, I. P. Hughes, and R. D. Pollack, *Rings of invariants and p-Sylow subgroups*, Canad. Math. Bull. **34** (1991), 42–47. MR **92h:**13008
[19] H. E. A. Campbell, I. P. Hughes, R. J. Shank, and D. L. Wehlau, *Bases for rings of coinvariants*, Transform. Groups **1** (1996), 307–336. MR **1:**424 447
[20] H. Cartan, *Quotient d'un éspace analytique par un groupe d'automorphismes*, Algebraic Geometry and Topology, A Symposium in Honor of S. Lefschetz (eds: R. H. Fox, D. C. Spencer and A. W. Tucker), Princeton Univ. Press, Princeton, 1957. MR **18:**823b
[21] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Univ. Press, Princeton, 1956. MR **17:**1040e
[22] A. Clark and J. Ewing, *The realization of polynomial algebras as cohomology rings*, Pacific J. Math. **50** (1974), 425–434. MR **51:**4221
[23] P. M. Cohen, *Algebra*, second ed., J. Wiley, New York, 1989.
[24] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Springer-Verlag, Heidelberg, Berlin, 1992. MR **93j:**13031; MR **1:**355 998
[25] L. E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. Amer. Math. Soc. **12** (1911), 75–98.
[26] ———, *Binary modular groups and their invariants*, Amer. J. Math. **33** (1911), 175–192.
[27] ———, *On finite algebras*, Nachr. Akad. Wiss. Göttingen (1905), 358–393.
[28] ———, *Linear groups*, Dover, New York, 1958. MR **21:**3488
[29] ———, *The collected mathematical papers of Leonard Eugene Dickson*, 6 volumes, Chelsea, New York, 1975. MR **56:**68a/b/c/d/e; MR **85e:**01059
[30] W. G. Dwyer and C. W. Wilkerson, *Kähler differentials, the T-functor, and a theorem of Steinberg*, Preprint, the Hopf archives (hopf@math.purdue.edu), 1996.
[31] D. Eisenbud, *Commutative algebra*, Springer-Verlag, Heidelberg, Berlin, 1995. MR **97a:**13001
[32] D. Engelmann, *Optimal, pseudooptimal and perfect homogeneous systems of parameters for rings of invariants*, Preprint, Humboldt Univ., 1996.

[33] G. Ellingsrud and T. Skjelbred, *Profondeur d'anneaux d'invariants en caractéristique p*, Comp. Math. **41** (1980), 233–244. MR **82c:**13015
[34] P. Erdős, J. Dixmier, and J.-L. Nicolas, *Sur le nombre d'invariants fondamentaux des formes binaires*, C. R. Acad. Sci. Paris Série I **305** (1987), 319–322. MR **89a:**11040
[35] W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029. MR **29:**3538
[36] M. Feshbach, *The image of the trace in the ring of invariants*, Preprint, Univ. Minnesota, 1981.
[37] ———, *p-Subgroups of compact Lie groups and torsion of infinite height in* $H^*(BG;\mathbb{F}_p)$, Mich. Math. J. **29** (1982), 299–306. MR **83m:**55026
[38] P. Fleischmann, *On the ring of vector invariants for the symmetric group*, Preprint, Institute for Experimental Mathematics, Essen, 1996.
[39] P. Fleischmann and W. Lempken, *On generators of modular invariant rings of finite groups*, Preprint, Institute for Experimental Mathematics, Essen, 1996.
[40] R. M. Fossum and P. A. Griffith, *Complete local factorial rings which are not Cohen-Macaulay in characteristic p*, Ann. Sci. École Norm. Sup. (4) **8** (1975), 189–199. MR **52:**3142
[41] A. K. Garsia and D. Stanton, *Group actions of Stanley-Reisner rings and invariants of permutation groups*, Adv. in Math. **51** (1984), 107–201. MR **86f:**20003
[42] O. E. Glenn, *Modular invariant processes*, Bull. Amer. Math. Soc. **21** (1914–15), 167–173.
[43] M. Göbel, *Computing bases for permutation invariant polynomials*, J. Symbolic Comput. **19** (1995), 285–291. MR **96f:**13006
[44] N. L. Gordeev, *Coranks of elements of linear groups and the complexity of algebras of invariants*, Leningrad Math. J. **2** (1991), 245–267. MR **91h:**20063
[45] D. Hilbert, *Über die Theorie der Algebraischen Formen*, Math. Ann. **36** (1890), 473–534.
[46] ———, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–373.
[47] ———, *Hilbert's invariant theory papers*, Lie Groups: History, Frontiers and Applications, Volume VIII (translated by M. Ackerman, commented by R. Hermann), Math. Sci. Press, Brookline, MA, 1978. MR **80e:**01035
[48] ———, *Theory of algebraic invariants* (translated by Reinhard C. Laudenbacher), Cambridge Univ. Press, Cambridge, 1993. MR **1:**266 168
[49] H. Hiller, *Geometry of Coxeter groups*, Pitman, London, 1982. MR **83h:**14045
[50] H. Hiller and L. Smith, *On the realization and classification of cyclic extensions of polynomial algebras over the Steenrod algebra*, Proc. Amer. Math. Soc. **100** (1987), 731–738. MR **89c:**55017
[51] M. Hochster and J. A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. **93** (1971), 1020–1058. MR **46:**1787
[52] Shou-Jen Hu and Ming-chang Kang, *Efficient generation of rings of invariants*, J. Algebra **180** (1996), 341–363. MR **97b:**13006
[53] V. G. Kac, *Root systems, representations of quivers, and invariant theory*, Lecture Notes in Math., vol. 996, Springer-Verlag, Heidelberg, Berlin, 1983, pp. 74–108. MR **85j:**14088
[54] V. G. Kac and D. H. Peterson, *Generalized invariants of groups generated by reflections*, Geometry Today (Roma, 1984), Progress in Mathematics, vol. 60, Birkhäuser-Verlag, Boston, 1985. MR **88k:**14027
[55] G. Kemper, *Calculating invariant rings of finite groups over arbitrary fields*, J. Symbolic Comput. **21** (1996), 351–366. MR **1:**400 337
[56] G. Kemper and G. Malle, *The finite irreducible linear groups with polynomial ring of invariants*, Preprint, Univ. Heidelberg, 1996.
[57] N. Killius, *Some modular invariant theory of finite groups with particular emphasis on the cyclic group*, Diplomarbeit, Univ. Göttingen, 1996.
[58] H. Kraft, *Geometrische Methoden in der Invariantentheorie*, Aspects of Math., Vieweg-Verlag, Braunschweig, 1984. MR **86j:**14006
[59] H. Kraft, P. Slodowy, and T. A. Springer (editors), *Algebraische Transformationsgruppen und Invariantentheorie*, DMV Seminar 13, Birkhäuser-Verlag, Basel, 1989. MR **91m:**14074
[60] N. J. Kuhn, *Generic representations of the finite general linear groups and the Steenrod algebra I*, Amer. J. Math. **116** (1994), 327–360. MR **95c:**55022
[61] K. Kuhnigk, *Transfer in Invariantenringen*, Diplomarbeit, Univ. Göttingen (to appear).

[62] P. S. Landweber and R. E. Stong, *The depth of rings of invariants over finite fields*, Proc. New York Number Theory Seminar (1984), Lecture Notes in Math., vol. 1240, Springer-Verlag, New York, 1987. MR **88k:**13004

[63] J. Lannes, *Sur les éspaces fonctionnels dont la source est le classifiant d'un p-groupe abélien élémentaire*, Inst. Hautes Études Sci. Publ. Math. **75** (1992), 135–224. MR **93j:**55019

[64] J. Lannes and S. Zarati, *Théorie de Smith algébrique et classification des $H^*V--\mathcal{U}$-injectifs*, Bull. Soc. Math. France **123** (1995), 189–223. MR **96c:**55003

[65] J. Martino and S. Priddy, *Stable homotopy classification of $BG_{\hat{p}}$*, Topology **34** (1995), 633–649. MR **96m:**55028

[66] W. S. Massey and F. P. Peterson, *The cohomology structure of certain fibre spaces I*, Topology **4** (1965), 47–65. MR **32:**6459

[67] V. L. Popov, *Syzygies in the theory of invariants*, Math. USSR-Izv. **47** (1983), 544–622. MR **85g:**14013

[68] I. G. Macdonald, *Symmetric functions and Hall polynomials*, Clarendon Press, Oxford, 1995. MR **96h:**05207

[69] H. Matsumura, *Commutative ring theory* (translated by M. Reid), Cambridge Univ. Press, Cambridge, 1986. MR **88h:**13001

[70] H. Miller and C. W. Wilkerson, *Vanishing lines for modules over the Steenrod algebra*, J. Pure Appl. Algebra **22** (1981), 293–307. MR **82m:**55024

[71] T. Molien, *Über die Invarianten der linearen Substitutionsgruppen*, Sitzungsber. König. Preuss. Akad. Wiss. (1897), 1152–1156.

[72] H. Nakajima, *Invariants of reflection groups in positive characteristics*, Proc. Japan Acad. Ser. A Math. Sci. **55** (1979), 219–221. MR **80i:**14019

[73] ———, *Invariants of finite groups generated by pseudoreflections in positive characteristic*, Tsukuba J. Math. **3** (1979), 109–122. MR **82i:**20058

[74] ———, *Invariants of finite abelian groups generated by transvections*, Tokyo J. Math. **3** (1980), 201–214. MR **82e:**14058

[75] ———, *On some invariant subrings of polynomial rings in positive characteristics*, Proc. 13th Sympos. on Ring Theory (Okayama, 1980), Okayama Univ, Okayama, 1981, pp. 91–107. MR **82h:**13012

[76] ———, *Modular representations of p-groups with regular rings of invariants*, Proc. Japan Acad. Ser. A Math. Sci. **56** (1980), 469–473. MR **82a:**20016

[77] ———, *Modular representations of Abelian groups with regular rings of invariants*, Nagoya Math. J. **86** (1982), 229–248. MR **83i:**14038

[78] ———, *Relative invariants of finite groups*, J. Algebra **79** (1982), 218–234. MR **84c:**13006

[79] ———, *Rings of invariants of finite groups which are hypersurfaces*, J. Algebra **80** (1983), 279–294. MR **85e:**20036

[80] ———, *Regular rings of invariants of unipotent groups*, J. Algebra **85** (1983), 253–286. MR **85f:**20038

[81] ———, *Rings of invariants of finite groups which are hypersurfaces II*, Adv. in Math. **65** (1987), 39–64. MR **89h:**14035

[82] A. Neeman, *The connection between a conjecture of Carlisle and Kropholler, now a theorem of Benson and Crawley-Bovey, and Grothendieck's Riemann-Roch and duality theorems*, Comment. Math. Helv. **70** (1995), 339–349. MR **96f:**14060

[83] F. Neumann, M. D. Neusel, and L. Smith, *Rings of generalized and stable invariants of pseudoreflections and pseudoreflection groups*, J. Algebra **182** (1996), 85–122. MR **1:**388 859

[84] ———, *Rings of generalized invariants and classifying spaces of compact Lie groups*, Preprint Nr. 14, Otto-von-Guericke-Universität Magdeburg, 1996.

[85] M. D. Neusel, *Invariants of some abelian p-groups in characteristic p*, Proc. Amer. Math. Soc. (to appear). MR **1:**377 000

[86] ———, *Integral extensions of unstable algebras over the Steenrod algebra*, Preprint, Royal Institute of Technology, Stockholm, 1996.

[87] ———, *$\mathcal{P}^*$-Commutative algebra* (to appear).

[88] M. D. Neusel and L. Smith, *The Lasker-Noether theorem for $\mathcal{P}^*$-invariant ideals*, Preprint Nr. 26, Otto-von-Guericke-Universität Magdeburg, 1995.

[89] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1916), 89–92.
[90] ———, *Der Endlichkeitssatz der Invarianten endlicher linear Gruppen der Characteristik p*, Nachr. Akad. Wiss. Göttingen (1926), 28–35.
[91] C. Peskine and L. Szpiro, *Dimension projective finie et cohomologie locale*, Inst. Hautes Études Sci. Publ. Math. **42** (1972), 47–119. MR **51:**10330
[92] V. Reiner, *On Göbel's bound for invariants of permutation groups*, Arch. Math. **65** (1995), 475–480. MR **96h:**13013
[93] V. Reiner and L. Smith, *Systems of parameters for rings of invariants*, Preprint, Göttingen, 1996.
[94] D. R. Richman, *On vector invariants over finite fields*, Adv. in Math. **81** (1990), 30–65. MR **91g:**15020
[95] ———, *On vector invariants over finite fields*, Adv. in Math. (to appear).
[96] B. J. Schmid, *Finite groups and invariant theory*, Séminaire d'Algèbre (P. Dubriel et M.-P. Malliavin, 1989–1990), Lecture Notes in Math., vol. 1478, Springer-Verlag, Heidelberg, Berlin, 1991. MR **94c:**13002
[97] L. Schwartz, *Lectures on Lannes technology*, Univ. of Chicago Press, Chicago, 1994.
[98] J.-P. Serre, *Algèbre locale multiplicités*, 3rd ed., Lecture Notes in Math., Springer-Verlag, Heidelberg, Berlin, 1975. MR **34:**1352
[99] ———, *Sur la dimension cohomologique des groupes profinis*, Topology **3** (1965), 413–420. MR **31:**4853
[100] ———, *Représentations linéaires des groupes finis*, Hermann, Paris, 1978. MR **80f:**20001
[101] W. M. Singer, *Iterated loop functors and the homology of the Steenrod algebra*, J. Pure Appl. Algebra **11** (1977), 83–101. MR **57:**17644
[102] ———, *The transfer in homological algebra*, Math. Zeit. **202** (1989), 493–523. MR **90i:**55035
[103] N. J. A. Sloane, *Error correcting codes and invariant theory*, Amer. Math. Monthly **84** (1977), 82–107. MR **54:**12361
[104] L. Smith, *Realizing certain polynomial algebras as cohomology rings of spaces of finite type fibered over* $\times B\mathbf{U}(d)$, Pacific J. Math. **126** (1987), 361–377. MR **88d:**55020
[105] ———, *e-Invariants and finite covers, II*, Trans. Amer. Math. Soc. **347** (1995), 5009–5021. MR **1:**316 862
[106] ———, *Polynomial invariants of finite groups*, A. K. Peters, Wellesley, MA, 1995. MR **96f:**13008
[107] ———, *Noether's bound in the invariant theory of finite groups*, Arch. Math. **66** (1966), 89–92. MR **96k:**13004
[108] ———, $\mathcal{P}^*$*-Invariant ideals in rings of invariants*, Forum Math. **8** (1996), 319–342. MR **97c:**13003
[109] L. Smith and R. E. Stong, *On the invariant theory of finite groups*: *Orbit polynomials and splitting principles*, J. Algebra **110** (1987), 134–157. MR **88k:**20077
[110] L. Smith and R. M. Switzer, *Realizability and nonrealizability of Dickson algebras as cohomology rings*, Proc. Amer. Math. Soc. **89** (1983), 303–313. MR **85e:**55036
[111] R. P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), 475–511. MR **81a:**20015
[112] R. Steinberg, *Differential equations invariant under finite reflection groups*, Trans. Amer. Math. Soc. **112** (1964), 392–400. MR **29:**4807
[113] ———, *On Dickson's theorem on invariants*, J. Fac. Sci. Univ. Tokyo Sect. 1A Math. **34** (1987), 699–707. MR **89c:**11177
[114] B. Sturmfels, *Algorithms in invariant theory*, Springer-Verlag, Heidelberg, Berlin, Vienna, 1993. MR **94m:**13004
[115] B. L. van der Waerden, *Modern algebra I, II* (translated by F. Blum), Ungar, New York, 1949. MR **10:**587b
[116] H. Weyl, *The classical groups*, second ed., Princeton Univ. Press, Princeton, 1946. MR **1:**42c
[117] C. W. Wilkerson, *A primer on the Dickson invariants*, Proc. Northwestern Homotopy Theory Conference, Contemp. Math., vol. 19, Amer. Math. Soc., Providence, RI, 1983, pp. 421–434. MR **85c:**55017

[118] R. M. W. Wood, *An introduction to the Steenrod algebra through differential operators*, Preprint, Manchester Univ., 1995.
[119] Wu Wen-Tsün, *Sur les puissances de Steenrod*, Colloque de Topologie de Strasbourg, 1951. MR **14:**491b

AG-Invariantentheorie, Mittelweg 3, D 37133 Friedland, Germany
E-mail address: larry@sunrise.uni-math.gwdg.de
E-mail address: agi@sunrise.uni-math.gwdg.de