Invariants of Finite Groups over Finite Fields: Recent Progress and New Conjectures

Peter Fleischmann

Institute of Mathematics and Statistics,
University of Kent at Canterbury,
Canterbury, CT2 7NF, England
E-mail: pf10@ukc.ac.uk

Let G be a finite group acting on a polynomial ring $A := \mathbb{F}[x_1, \dots, x_n]$ by graded algebra automorphisms. If $\mathbb{F}$ is a field of characteristic zero, then due to classical results of Emmy Noether one knows that the invariant ring A^G can be generated in degrees less or equal to $|G|$. If $\mathbb{F}$ is a field of positive characteristic p dividing the group order $|G|$, this is no longer true. The situation in characteristic p not dividing $|G|$ has been clarified recently after being open for several decades. This paper presents an account on these developments, including some related questions and conjectures dealing with constructive and structural properties of modular invariant rings.

1. INTRODUCTION

Let $\mathbb{F}$ be a field and let $\mathbb{F}[x_1, x_2, \cdots, x_n]$ be a polynomial algebra on which the group G acts by graded algebra automorphisms. The *ring of invariants* consists of all polynomials unchanged by elements of G and is the major object of study in classical invariant theory. One major motivation comes from algebraic geometry, where more general 'affine' algebras and group actions occur. Assume for the moment that $\mathbb{F}$ is algebraically closed and let X be an affine algebraic variety with $A := \mathcal{O}(X)$ the corresponding algebra of regular functions, such that X can be identified with the set of maximal ideals in A. For a group G of automorphisms of X let $X//G$ denote the *categorical quotient*. Then a natural question is, whether $X//G$ is again an affine algebraic variety. A necessary condition for this is, that the invariant ring

$$A^G := \{a \in A \mid g(a) = a \; \forall \; g \in G\}$$

is a finitely generated $\mathbb{F}$ - algebra. In this case the maximal ideal spectrum $\max - \operatorname{spec} A^G$ of the invariant ring is a natural candidate for $X//G$ and one might hope that $X//G$ coincides with the set - theoretic quotient, namely the orbit space X/G. In general neither does A^G have to be finitely generated, nor does the categorical quotient $X//G$ have to coincide with the 'geometric quotient' X/G, but if G is a finite group, then due to a fundamental theorem of Emmy Noether, the situation is much better (see e.g. [1] 1.4.4).

THEOREM 1.1. *(Emmy Noether (1926)[13]) If $|G| < \infty$, then A^G is finitely generated and $X//G \cong \max - \mathrm{spec}\ A^G$ is in bijection with the orbit - space X/G.*

Therefore the natural questions arise

- how can A^G be constructed ?
- what are the geometrical properties of A^G?

When invariant theory was created in the middle of the 19'th century, the main interest was focused on the situation where $\mathbb{F}$ is the field of complex numbers and G is a classical (infinite) group. Therefore invariant theory 'in characteristic zero' is highly developed. Recent applications in geometry, algebraic topology and cohomology theory ask for results in the situation where $\mathbb{F}$ is of positive characteristic, in particular a finite field, and G is a finite group (see [19]). As I pointed out in my talk at the Fq4 - conference in Waterloo ([4]), much less is known in this situation, because many of the methods developed for characteristic zero do not carry over, and some results on 'classical invariant rings' are known to be false in positive characteristic. Since 1997 considerable progress has been achieved, in particular with respect to constructive methods. For example the problem of Emmy Noether's degree bound which was addressed in [4], has in the meantime been resolved to full satisfaction ([6], [8]). The experience gained in this process has led to various new questions and conjectures which also deal with geometrical and structural properties of invariant rings. In this paper I want to give an account on these developments and will present an admittedly subjective outlook into the nearer future.

Notation: Throughout the paper $\mathbb{N}_0$ denotes the set of nonnegative integers; for $n \in \mathbb{N}$, $\underline{n}$ denotes the set $\{1, 2, \cdots, n\}$ and $\mathbb{N}_0^{\underline{n}}$ denotes the set of functions from $\underline{n}$ to $\mathbb{N}_0$.

2. CONSTRUCTIVE ASPECTS

Noether's proof of Theorem 1.1 was one of the first major applications of her newly developed theory of rings and modules with ascending chain condition. The price one has to pay for the generality of Theorem 1.1 is, that its proof is not constructive.

DEFINITION 2.1. Let R be a commutative ring, $A := R[a_1, a_2, \cdots, a_k]$ a finitely generated R - algebra with generators $a_1, \cdots, a_k$ and G a finite group acting on A as R - algebra automorphisms, stabilizing the R - module $\sum_{i=1}^k Ra_i$. For $\alpha \in \mathbb{N}_0^{\underline{k}}$ we denote with $\underline{a}^\alpha$ the power product $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_k^{\alpha_k} \in A$ and with

$\mathcal{M}_\ell(\underline{(a_i)})$ we denote the R - module spanned by $\{\underline{a}^\alpha \mid |\alpha| := \sum_{i=1}^k \alpha_i \leq \ell\} \subseteq A$. For a subalgebra or ideal B of A we define the **Noether number**

$$\beta(B, (a_1, \ldots, a_k)) \in \mathbb{N} \cup \{\infty\}$$

to be the infimum of the set of all $\ell \in \mathbb{N}$ such that $\{b_1, \ldots, b_m\} \subseteq \mathcal{M}_\ell(\underline{(a_i)})$, satisfying $B = R[b_1, \ldots, b_m]$ if B is a subalgebra, or satisfying $B = (b_1, \ldots, b_m)A$ if B is an ideal. If there is an obvious set of chosen generators (a_i) or the choice does not matter, we will simply write $\beta(B)$. For example, if $A = R[x_1, \cdots, x_k]$ is a polynomial ring generated by variables x_i of degree 1 and B is a finitely generated graded subring or a homogeneous ideal, then $\beta(B) := \beta(B, \underline{(x_i)})$ will be the minimal number k such that B is generated by homogeneous elements in A of degree less or equal to k.

Remark 2. 1. By Theorem 1.1, $\beta := \beta(A^G, (a_1, \ldots, a_k)) < \infty$, if G is finite and R is Noetherian, but the proof does not give any bound for β.

Obviously the Noether number $\beta(B)$ is a measure for the *algorithmic complexity* of a subring or ideal. In particular if R is a field and $B := A^G$, then invariants in $\mathcal{M}_\ell(\underline{(a_i)})$ can be computed by solving linear equations of size increasing with ℓ. Since $\beta(A^G)$ is an upper bound for the ℓ needed to generate A^G, it also bounds the overall size of linear systems to solve.

In 1916 Emmy Noether gave two different proofs for the fact that

$$\beta(\mathbb{F}[x_1, \cdots, x_k]^G) \leq |G|,$$

if G is a finite group and $R = \mathbb{F}$ is a field of characteristic zero. This is usually referred to as the 'Noether bound' in invariant theory. Both of these proofs fail in positive characteristics. On the other hand it is known from [15], that $\beta(A^G)$ can be arbitrarily large, if the characteristic of $\mathbb{F}$ divides $|G|$. After Emmy Noether's general result (Theorem 1.1), the question of degree bounds somewhat fell into oblivion, until it resurrected again with the upcoming of constructive invariant theory in conjunction with new powerful methods in computer algebra. In particular the so called 'Noether gap', i.e. the conjecture that the Noether bound $\beta(\mathbb{F}[x_1, \cdots, x_k]^G) \leq |G|$ holds if $\mathrm{char}\, \mathbb{F}$ does not divide $|G|$, has de facto been open since 1916, but was considered more seriously during the past decade (see e.g. [17], [14], where the it was shown to hold for solvable groups). This question has recently been answered to the affirmative by the author and J Fogarty independently and with slightly different approaches (see [6], [8]). In the following I will present a 'combined version' of these proofs, incorporating an essential observation by D Benson which makes the combinatorics in [6] more transparent.

The fact that Noether's degree bound does not hold in general can be seen already in the simple example $A := \mathbb{F}_2[x_1, \cdots, x_k, y_1, \cdots, y_k]$ with $G = \Sigma_2 = \langle g \rangle$ acting by swapping the 'variable types' $x_i \leftrightarrow y_i$. It is an easy exercise to show that the invariant $\mathfrak{r} := (x_1 \cdots x_k)^+ := x_1 \cdots x_k + y_1 \cdots y_k$ is indecomposable, i.e. cannot be written as a sum of products of invariants of smaller degree. Therefore

$$\beta(A^G, (x_1, \cdots, y_k)) \geq k \to \infty \text{ if } k \to \infty.$$

It is interesting, though, to observe that

$$\mathfrak{r} = (x_2 \cdots x_k)^+ x_1 + (x_1 x_3 \cdots x_k)^+ y_2 - (x_3 \cdots x_k)^+ x_1 y_2,$$

i.e. $\mathfrak{r}$ decomposes in the *Hilbert - ideal* $A^{G,+}A$, generated *in* A by all invariants of positive degree. Hence one can easily see that $\beta(A^{G,+}A) = 2$ for all $k \geq 2$. In fact a generalization of this observation led to the proof of Noether's bound in [6].

Let $H \leq G$ be a subgroup of index n with coset - decomposition $G := \uplus_{i:=1}^n g_i H$. The homomorphism of A^G - modules given by

$$t_H^G : A^H \to A^G, \ a \mapsto \sum_{g \in G:H} g(a)$$

is called the *relative transfer map* with respect to H; its image is an ideal in A^G, called the *relative transfer ideal* (w.r.t. H). The following lemma gives a useful decomposition in A of high degree relative transfer elements:

LEMMA 2.1. *For* $b, b_1, b_2, \cdots, b_n \in A^H$ *we have*

$$t_H^G(bb_1 \cdots b_n) = \sum_{I \subset \underline{n},\ I \neq \underline{n}} (-1)^{n-|I|+1} \ t_H^G(b \prod_{j \in I} b_j) \prod_{j \notin I} g_j(b_j).$$

Proof. By Benson's trick we have the obvious equality:

$$\prod_{j=1}^n (\ g_i(b_j) - g_j(b_j)\ ) = 0.$$

Expansion and multiplication with $g_i(b)$ for fixed i gives:

$$0 = \sum_{I \subseteq \underline{n}} (-1)^{|I|} \prod_{j \notin I} g_j(b_j) \cdot (\prod_{j \in I} g_i(b_j)) \cdot g_i(b).$$

Now summation over $i \in \underline{n}$ yields the claimed identity. ∎

THEOREM 2.1. *Let A be as in Definition 2.1 and H a subgroup of G such that either $|G|$ invertible in R or $H \triangleleft G$ a normal subgroup with index $[G : H]$ invertible in R. Then*

$$\beta(A^G) \leq \beta(A^H) \cdot [G : H].$$

In particular, if $|G| \in \mathbb{F}^*$, then Noether's degree bound holds, i.e.

$$\beta(\mathbb{F}[x_1, \cdots, x_k]^G) \leq |G|.$$

Proof. Under both assumptions on H, the relative transfer map t_H^G is surjective. Also note that the elements $g_j(b_j)$ appearing in the previous lemma are in A^H, if H is normal in G. Now suppose that $\beta := \beta(A^H) = \beta(A^H, (a_\ell))$ with $A := R[a_1, \cdots, a_\ell]$ and $A^H = R[b_1, \cdots, b_k]$ with $b_i \in A^H \cap \mathcal{M}_\beta(\underline{(a_\ell)})$. If $H \leq G$ and $|G|$ invertible, we have $t_H^G(bb_1 \cdots b_n) = \frac{1}{|G|} t_1^G(t_H^G(bb_1 \cdots b_n)) =$

$$\sum_{I \subset \underline{n},\ I \neq \underline{n}} (-1)^{n-|I|+1}\, t_H^G(b \prod_{j \in I} b_j) \frac{1}{|G|}\, t_1^G(\prod_{j \notin I} g_j(b_j)) \in A^G \cap \mathcal{M}_{n\beta}(\underline{(a_\ell)}).$$

If $H \triangleleft G$ and $|G/H|$ invertible, we replace $|G|$ by $|G/H|$ and t_1^G by t_H^G to conclude in a similar way that $t_H^G(bb_1 \cdots b_n) \in A^G \cap \mathcal{M}_{n \cdot \beta}(\underline{(a_\ell)})$. Now an iterative application of this result finishes the proof. ∎

One might hope to remove the requirement $H \triangleleft G$ for subgroups of invertible index:

Conjecture 2.1. : If $H \leq G$ with index $[G : H]$ invertible in R, then

$$\beta(A^G) \leq \beta(A^H) \cdot [G : H].$$

If $A = \mathbb{F}[x_1, \cdots, x_k]$, the formula in Lemma 2.1 describes a decomposition of relative transfer elements in the Hilbert - ideal $A^{G,+}A$. Extensive sample calculations done by Harm Derksen and Gregor Kemper led them to the following far reaching conjecture:

Conjecture 2.2. [Noether bound for Hilbert ideals] (H. Derksen / G. Kemper): Let G be a finite group, $\mathbb{F}$ a field and $A := \mathbb{F}[x_1, \cdots, x_k]$ a polynomial ring, such that G acts by graded algebra automorphisms. Then

$$\beta(A^{G,+}A) \leq |G|.$$

In the next section we will show that in special cases this conjecture can be verified using the techniques of the proof of Theorem 2.1, which we are now going to refine.

From now on for the rest of the paper let $R := \mathbb{F}$ be a field of characteristic $p \mid |G|$ and V a finitely generated $\mathbb{F}G$ - module. We consider the symmetric algebra $A := \mathrm{Sym}(V^*)$ of the dual module V^* as a polynomial ring with the induced graded G -action, and let P be a fixed Sylow p - group of G with normalizer $N_G(P)$ and $N := N_G(P)/P$. For subgroups $U \le H \le G$ we define the (homogeneous) *relative transfer ideal*

$$\mathcal{I}^H_{<U} := \sum_{Y<U} t^H_Y(A^Y) \triangleleft A^H.$$

LEMMA 2.2.

$$\beta(A^{G,+} \cdot A) \le \max\{\beta(A^Q/\mathcal{I}^Q_{<Q}) \cdot [G:Q] \mid Q \le P\}.$$

Proof. Let $f \in A^{G,+}$ be indecomposable in $A^{G,+}A$. Since $n := [G:P]$ is invertible, f is of the form $t^G_P(h)$ for some $h \in A^{P,+}$, which itself can be written as

$$h = \sum_{Q \le P} t^P_Q(b_{Q,1}b_{Q,2}\cdots b_{Q,\ell_Q})$$

with $b_{Q,j} + \mathcal{I}^Q_{<Q} \in A^Q/\mathcal{I}^Q_{<Q}$ and $b_{Q,j}$ homogeneous of positive degree $\le \beta_Q := \beta(A^Q/\mathcal{I}^Q_{<Q})$. Moreover we can assume that every nonzero transfer element

$$t^G_P(t^P_Q(b_{Q,1}b_{Q,2}\cdots b_{Q,\ell_Q})) = t^G_Q(b_{Q,1}b_{Q,2}\cdots b_{Q,\ell_Q})$$

is indecomposable in $A^{G,+}A$ as well. But from lemma 2.1 we see that this requires $\ell_Q \le [G:Q]$, hence

$$f \in \sum_Q A^{G,+}_{\le \beta_Q[G:Q]} \cdot A.$$

∎

Hence Noether's bound in case of relative transfer quotients for p - groups implies Conjecture 2.2:

COROLLARY 2.1. *If $\beta(A^Q/\mathcal{I}^Q_{<Q}) \le |Q|$ for all $Q \le P \in \mathrm{Syl}_p(G)$, then conjecture 2.2 holds, i.e. $\beta(A^{G,+}A) \le |G|$.*

To obtain degree bounds for A^G rather than $A^{G,+}A$ one can make use of the *Brauer homomorphism* from representation theory, i.e. is the canonical homomorphism $A^G \to \overline{A^G} := A^G/\mathcal{I}^G_{<P}$. Using Mackey's formula for the relative transfer, we get

$$t^G_P(b) = \sum_{g \in P\backslash G/P} t^P_{P\cap\, {}^gP}({}^gb) \equiv \sum_{g\in N/P} {}^gb \equiv t^N_1(b) \mod \mathcal{I}^P_{<P},$$

where $P\backslash G/P$ denotes a chosen system of double cosets of P in G. It is easy to see that $\mathcal{I}^P_{<P} \cap A^G = \mathcal{I}^G_{<P}$, hence we get

$$\overline{A^G} = (A^G + \mathcal{I}^P_{<P})/\mathcal{I}^P_{<P} = t^N_1(A^P/\mathcal{I}^P_{<P}) \cong (A^P/\mathcal{I}^P_{<P})^N.$$

Since p does not divide $|N|$, Theorem 2.1 gives

LEMMA 2.3.

$$\beta(\overline{A^G}) \leq \beta(\overline{A^P}) \cdot |N|.$$

$$\beta(A^G) \leq \max\{\beta(\mathcal{I}^G_{<P}),\ \beta(\overline{A^P}) \cdot |N|\}.$$

It has been conjectured by several experts that

$$\beta(\mathrm{Sym}(V^*)^G) \leq \max\{|G|, \dim V \cdot (|G|-1)\}$$

might be a 'natural degree bound' for modular invariant rings of type $\mathrm{Sym}(V^*)^G$. Using the above technique this certainly would follow from the next two slightly sharper conjectures:

Conjecture 2.3. Let P be a Sylow p - group of G. Then

1. $\beta(A^G/\mathcal{I}^G_{<P}) \leq |N_G(P)|$.
2. If $A = \mathrm{Sym}(V^*)$ with $\mathbb{F}G$ - module V, then

$$\beta(\mathcal{I}^G_{<P}) \leq \max\{|G|, \dim V \cdot (|G|-1)\}.$$

3.

3. p - PERMUTATION MODULES

In this section we present some evidence for the previous conjectures, based on the analysis of a special type of invariant rings. An $\mathbb{F}G$ - module V in characteristic

p is called a p - *permutation module* or *trivial source module*, if its restriction to any Sylow p - subgroup is an ordinary permutation module, or in other words, if a basis $\mathfrak{b}$ of V can be found, which is permuted by some Sylow p - group. Note that, since any two Sylow p - groups are conjugate, the property of being a p - permutation module does not depend on the choice of the Sylow group. Note also that V is a p - permutation module if and only if so is the dual V^*. The following lemma is a known fact in modular representation theory (e.g. see [16]):

LEMMA 3.1. *The $\mathbb{F}G$ - module V is a p - permutation module if and only if it is a direct summand of a permutation module for G.*

Now choose a Sylow p - group P and assume that $V_{|P}$ is a permutation module of dimension d. Then for any subgroup $Q \leq P$ the restricted module $V^*_{|Q}$ is also a permutation module. Moreover for every integer m, the homogeneous component $A_m = \mathrm{Sym}(V^*)_m$ of degree m is generated as a vector space by power products $\mathbf{x}^{\mathbf{a}} := x_1^{a_1} x_2^{a_2} \cdots x_d^{a_d}$ of exponent sum m, which themselves are permuted by Q. In particular an element

$$\mathfrak{x} := \sum_{\mathbf{a} \in \mathbb{N}_0^d} c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}$$

is Q - invariant, if and only if $c_{\mathbf{a}}$ is constant on the orbit $\mathbf{a}^Q := \{\mathbf{a} \circ g \mid g \in Q\}$, where Q is viewed as permuting the set $\underline{d}$ and therefore acting naturally on the set of functions $\mathbb{N}_0^{\underline{d}}$. In other words, each Q - invariant is a linear combination of *orbit - sums* of the form

$$(\mathbf{x}^{\mathbf{a}})^+ := \sum_{g \in Q/Q_{\mathbf{a}}} \mathbf{x}^{\mathbf{a} \circ g},$$

where $Q/Q_{\mathbf{a}}$ is a chosen cross section for the cosets of the stabilizer subgroup $Q_{\mathbf{a}}$ in Q. In particular $(\mathbf{x}^{\mathbf{a}})^+ \in \mathcal{I}^Q_{<Q}$ if and only if $Q_{\mathbf{a}} < Q$. On the other hand, the Q - stable power products are products of 'norm - like elements' of the form $\mathfrak{n}_i := \prod_{x_i \in \mathcal{O}_i} x_i$, where $\{\mathcal{O}_i \mid i = 1, \cdots, s\}$ is the set of all Q - orbits on a chosen permutation basis $\{x_1, \cdots, x_d\}$ of V. From this it is easy to see that

$$A^Q = \mathcal{I}^Q_{<Q} \oplus \mathbb{F}[\mathfrak{n}_1, \cdots, \mathfrak{n}_s].$$

In particular $A^Q/\mathcal{I}^Q_{<Q} \cong \mathbb{F}[\mathfrak{n}_1, \cdots, \mathfrak{n}_s]$ is a polynomial ring generated by elements of degree $\leq |Q|$. This together with Lemma 2.2 gives:

PROPOSITION 3.1. *If V is a p - permutation module and P is a Sylow p - group of G, then $\beta(A^Q/\mathcal{I}^Q_{<Q}) \leq |Q|$ for each subgroup $Q \leq P$. In particular conjecture 2.2 holds for $A = \mathrm{Sym}(V^*)$.*

To show that the second degree bound of conjecture 2.3 holds in this case, we can argue in a similar way as in the proof of Lemma 2.2: Let $f \in \mathcal{I}_{<}^{G,+}$ be indecomposable; by the transitivity of relative transfers ($t_{U\,|A^U}^H = (t_Y^H \circ t_U^Y)_{|A^U}$ for $U \le Y \le H$) we can in fact assume that f is of the form $t_Q^G(h)$ with h being a power product in the $\mathfrak{n}_i$'s. Each polynomial $\prod_{g\in G/Q}(T - g(\mathfrak{n}_i)) \in A^G[T]$ has $\mathfrak{n}_i$ as a zero, showing that $\mathfrak{n}_i^{|G:Q|} \in \sum_{0\le j<|G:Q|} A^G \mathfrak{n}_i^j$. This allows for reductions of exponents in h and since the operator t_Q^G is A^G - linear, we can assume that these exponents do not exceed $|G:Q|-1$. Hence the total degree of f can be assumed to be less or equal to $s\cdot(|G:Q|-1)$. Since $s \le d = \dim\, V$ and $\deg\, \mathfrak{n}_i \le |Q|$ we conclude that $\beta(\mathcal{I}_{<P}^G) \le \max\{|G|, d\cdot(|G|-1)\}$. Hence

Proposition 3.2. *If the $\mathbb{F}G$ - module V is a direct summand of a permutation module, then*

$$\beta(\mathrm{Sym}(V^*)^G) \le \max\{|G|, \dim\, V\cdot(|G|-1)\}.$$

4. STRUCTURAL ASPECTS

Let B be a positively graded $\mathbb{F}$ - algebra with $B_0 \cong \mathbb{F}$, M a finitely generated B - module and $I \triangleleft B$ an ideal. Recall that a sequence $a_1, a_2, \cdots, a_r$ of homogeneous elements in I is called a *regular M - sequence* if $B(a_1, a_2, \cdots, a_r)\cdot M < M$ and for every $1 \le i \le r$ the multiplication with a_i is an injective operator on the quotient $M/(a_1, a_2, \cdots, a_{i-1})M$. It is a known fact that all maximal regular M - sequences in I have the same length, which is called the *grade* of I on M. The grade of B on M is called the *depth* of M and the module M is called *Cohen - Macaulay*, if its depth coincides with its Krull - dimension Dim M = Dim $(B/\mathrm{Ann}_B(M))$. Here $\mathrm{Ann}_B(M) := \{a \in B \mid aM = 0\}$ is the annihilator of M in B. The ring B is called Cohen - Macaulay, if the regular module ${}_BB$ is Cohen - Macaulay. It can be shown that B is Cohen - Macaulay if and only if B is a finitely generated free module over some polynomial subring of B (see [1] 4.3).

It has been known for quite some time that rings of polynomial invariants of the form $\mathrm{Sym}(V^*)$ form $\mathbb{F}[x_1, \cdots, x_k]^G$ are Cohen - Macaulay, if G is a finite group whose order is coprime to the characteristic of $\mathbb{F}$. This is known to be false in general, once $p = \mathrm{char}\ \mathbb{F}$ divides $|G|$ (see [9] and the references there). The degree to which it fails is measured by the *defect* def $A^* := \mathrm{Dim}\ A^* - \mathrm{depth}\ A^*$. Clearly if $A = \mathrm{Sym}(V^*)$ and G is finite, then $\mathrm{Dim}\ A = \mathrm{Dim}\ A^G = \dim_{\mathbb{F}} V$, because A is a finite extension of A^G.

In 1980 G. Ellingsrud and T. Skjelbred proved the celebrated result that, if P is a Sylow p - group P of G with fixed point space V^P, one has

$$\mathrm{depth}\ \mathrm{Sym}(V^*)^G \ge 2 + \dim\, V^P \qquad (*)$$

if $\dim V \geq \dim V^P + 2$, with equality if G is a cyclic p - group (see [3]). For almost two decades this has been the only general result on the depth of modular invariant rings, which remains to be one of their most interesting, but difficult to determine parameters. In particular the classification of modular Cohen - Macaulay - invariant rings is an open problem. The result of Ellingsrud and Skjelbred was achieved using homological algebra, in particular a Grothendieck spectral sequence. During the last five years or so, these techniques have been revitalized (see e.g. [9], [20], [11]), most notably by Gregor Kemper who was able to classify all groups, whose modular regular representation has a Cohen - Macaulay ring of invariants.

With regard to the techniques laid out in the previous sections of this paper, some recent results show that the relative transfer ideal $\mathcal{I}^G_{<P}$ and its radical $\sqrt{\mathcal{I}^G_{<P}}$ can shed some new light on the problem of determining the depth of modular invariant rings. Let $P \leq G$ be a chosen Sylow p - group of G and assume for technical reasons, that $\mathbb{F}$ is algebraically closed of characteristic $p > 0$. This allows us to consider $A := \mathrm{Sym}(V^*)$ as the algebra of polynomial functions on V, and A^G as the algebra of polynomial functions on the orbit space V/G. Hence for an ideal $\mathcal{I} \lhd A^G$, the variety $\mathcal{V}(\mathcal{I})$ consists of all orbits v^G in V such that $f(x) = 0$ for every $f \in \mathcal{I}$ and $x \in v^G$. On the other hand for each subset $S \subseteq V$ there is the ideal $\mathcal{I}(S) := \{f \in A \mid f(s) = 0\ \forall s \in S\}$ and $\mathcal{I}^G(S) := \mathcal{I}(S) \cap A^G$. In [5] relative transfer ideals have been investigated geometrically which led to the following description of $\sqrt{\mathcal{I}^G_{<P}}$ in terms of its variety in the orbit space V/G:

THEOREM 4.1. *([5])*
1. $\mathcal{V}(\mathcal{I}^G_{<P}) = \{v^G \in V/G \mid p \not| \, |v^G|\}$,
2. $\sqrt{\mathcal{I}^G_{<P}} = \mathcal{I}^G(V^P)$*, where* V^P *denotes the space of* P *- fixed points in* V.
3.If the action of P *on* V *is defined over* $\mathbb{F}_p$*, then*

$$A^G/\sqrt{\mathcal{I}^G_{<P}} \text{ is Cohen} - \text{Macaulay of Krull dimension } \dim_{\mathbb{F}} V^P.$$

In particular the latter result indicated that the ideal $\sqrt{\mathcal{I}^G_{<P}}$ might 'measure the depth' of $\mathrm{Sym}(V^*)^G$: the formula (*) of Ellingsrud - Skjelbred shows, that $\dim V^P$ is a lower bound for the depth of A^G, so it was conceivable that the 'missing part' of the depth is provided by regular elements in the ideal $\mathcal{I}^G_{<P}$[1]. In the case of p - groups this follows from a result of G. Kemper (see [10], Theorem 1.5) and for general groups it is a consequence of the following

THEOREM 4.2. *(P. Fl, R.J. Shank, [7])*

$$\mathrm{depth}\ A^G = \mathrm{grade}(\mathcal{I}^G_{<P}, A^G) + \dim V^P.$$

[1] note that the grade of an ideal always coincides with the grade of its radical.

Moreover, if V is defined over $\mathbb{F}_q$, one can at least in principle use the 'Dickson invariants' $d_i \in \mathrm{Sym}(V^*)^{\mathrm{GL}_n(q)} \leq \mathrm{Sym}(V^*)^G$ to determine the grade of $\mathcal{I}^G_{<P}$ on A^G. Theorem 4.2, in connection with Lemma and Conjecture 2.3, shows that the relative transfer ideal $\mathcal{I}^G_{<P}$ contains the clues for some of the most important structural and constructive properties of modular invariant rings. Hence an efficient algorithm to find minimal generating sets for the ideal $\sqrt{\mathcal{I}^G_{<P}}$ is very much needed as an important step to determine its grade henceforth the depth of A^G.

REFERENCES

1. D. Benson, *Polynomial Invariants of Finite Groups*, Cambridge Univ. Press 1993.
2. W. Bruns, J. Herzog, *Cohen-Macaulay Rings*, Cambridge Univ. Press 1993.
3. G. Ellingsrud, Tor Skjelbred, *Profondeur d'anneaux d'invariants en caractéristique p*, Compos. Math. **41** (1980), 233-244
4. P. Fleischmann, W. Lempken *On Degree Bounds for Invariant Rings of Finite Groups Over Finite Fields*, Cont. Math. **225**, 33-41, (1997).
5. P. Fleischmann, Relative trace ideals and Cohen - Macaulay quotients of modular invariant rings in 'Computational Methods for Representations of Groups and Algebras', Dräxler, P. / Michler, G., Ringel, C.M. Ed., Birkhäuser, Basel (1999).
6. P. Fleischmann, *The Noether Bound in Invariant Theory of Finite Groups*, Adv. in Mathematics, **156**, 23-32, (2000).
7. P. Fleischmann, R.J. Shank, *Depth and the Relative Trace Ideal*, to appear in Arch. Math.
8. J. Fogarty, *On Noether's Bound for Polynomial Invariants of a Finite Group.*, Elec. Res. Ann. of the AMS (7), 5-7, (2001).
9. G.Kemper, *On the Cohen- Macaulay property of modular invariant rings*, J. of Algebra **215**, (1999). 330-351.
10. G. Kemper, *The depth of invariant rings and cohomology*, with an appendix by K. Magaard, preprint (1999), Universität Heidelberg, to appear in the J. of Algebra.
11. M. Lorenz, J. Pathak, *On Cohen-Macaulay Rings of Invariants*, preprint (2001), Temple University.
12. E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77**, 89-92, (1916).
13. E. Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachr. Ges. Wiss. Göttingen (1926), 28-35, in 'Collected Papers', pp.485-492, Springer Verlag, Berlin (1983).
14. D. Richman, *Explicit generators of the invariants of finite groups*, Adv. Math. **124** (1996), 49-76.
15. D. Richman, *Invariants of finite groups over fields of characteristic p*, Adv. Math. **124** (1996), 25-48.
16. P. Landrock, *Finite Group Algebras and their Modules*, LMS Lecture Note Series, Cambridge University Press (1984).
17. L. Smith, *E. Noether's bound in the invariant theory of finite groups*, Arch. Math. **66**, 89-92, (1995).
18. L. Smith, *Polynomial Invariants of Finite Groups*, A.K. Peters Ltd., (1995).
19. L. Smith, *Polynomial invariants of finite groups, a survey of recent developments*, Bull. Amer. Math. Soc. (1997), 211-250.
20. L. Smith, *Homological Codimension of Modular Rings of Invariants and the Koszul Complex*, preprint (1997).