C. R. Math. Rep. Acad. Sci. Canada Vol. **28** (2) 2006, pp. 39–62

# THE NOETHER NUMBER IN INVARIANT THEORY

DAVID L. WEHLAU

Presented by Vlastimil Dlab and Ram Murty, FRSC

Abstract. Let $\mathbb{F}$ be any field. Let $G$ be any reductive linear algebraic group and consider a finite dimensional rational representation $V$ of $G$. Then the $\mathbb{F}$-algebra $\mathbb{F}[V]^G$ of polynomial invariants for $G$ acting on $V$ is finitely generated. The Noether Number $\beta(G,V)$ is the highest degree of an element of a minimal homogeneous generating set for $\mathbb{F}[V]^G$. We survey what is known about Noether Numbers, in particular describing various upper and lower bounds for them. Both finite and infinite groups and both characteristic 0 and positive characteristic are considered.

Résumé. Soit $\mathbb{F}$ un corps commutatif. Soit $G$ un groupe algébrique linéaire réductif, et $V$ une représentation rationelle de dimension finie sur $\mathbb{F}$. Alors $\mathbb{F}[V]^G$, l'anneau des polynômes invariants pour l'action de $G$ sur $V$, admet un nombre fini de générateurs. Le nombre de Noether $\beta(G,V)$ est le degré maximal d'un membre d'un ensemble minimal de générateurs homogènes de $\mathbb{F}[V]^G$. Nous faisons une revue des résultats connus sur les nombres de Noether. En particulier, nous décrivons certaines bornes supérieures et inférieures pour les nombres de Noether. Nous considérons à la fois les groupes finis et infinis, sur des corps de charactéristique 0 ou $p > 0$.

## 1. Introduction.

The central problem in invariant theory is to find generators for the ring of invariants of some group representation. Given a particular action, it is often possible to construct many invariants. However, the question of when enough invariants have been obtained to generate the full ring of invariants is much more difficult. One solution to this difficulty is to find some upper bound on the degree of the invariants needed. The highest degree of an invariant required in a generating set is called the *Noether Number* of the representation.

Lately there have been many new results bounding the Noether Number for various representations. Here we will summarize many of these. There are a number of general references which discuss bounds on the Noether Number. The excellent book [7] by H. Derksen and G. Kemper covers all aspects of constructive invariant theory. The two articles [5], [6] by Derksen and the articles [7] by Derksen and H. Kraft and [51] by the author discuss the characteristic zero situation for infinite groups. F. Knop [35] has a recent article which examines finite modular groups over general rings.

Received by the editors on February 6, 2006; revised June 8, 2006.

The research of the author is partially supported by grants from ARP and NSERC.

AMS subject classification: Primary: 13A50; secondary: 20G15.

Keywords: invariant rings, degree bounds, Noether number.

**2. Preliminaries.** We begin with some definitions. We refer the reader to [7], [24], [48] for proofs and further details concerning these definitions. A *linear algebraic group* defined over a field $\mathbb{F}$ is any group $G$ which is isomorphic to a closed (in the Zariski topology) subgroup of $\mathrm{GL}_t(\mathbb{F})$ for some $t$. Important examples include $\mathbb{F}$ under addition, $\mathbb{F}^\times$ under multiplication, $\mathrm{GL}_n(\mathbb{F})$, $\mathrm{SL}_n(\mathbb{F})$, any finite group, and all the classical Lie groups.

Suppose now that $\mathbb{F}$ is algebraically closed. A linear algebraic group is *connected* if it is connected in the topological sense. We write $G^0$ to denote the connected component of $G$ which contains the multiplicative identity $e$ of $G$. It is easy to see that $G^0$ is a normal subgroup of $G$ of finite index.

A *Borel* subgroup $B$ of $G$ is any maximal solvable connected subgroup of $G$. A linear algebraic group is a *torus* if it is isomorphic to $(\mathbb{F}^\times)^r$ for some non-negative integer $r$. Two of the central theorems of algebraic group theory are that all Borel subgroups of $G$ are conjugate and that all maximal tori contained in $G$ are conjugate.

The *radical* of $G$ is the connected normal subgroup

$$\mathrm{Rad}(G) = \Big( \bigcap_{\substack{B \text{ is a Borel} \\ \text{subgroup of } G}} B \Big)^0 .$$

A linear algebraic group $G$ is *reductive* if $\mathrm{Rad}(G)$ is a torus and is *semi-simple* if $\mathrm{Rad}(G) = \{e\}$. For example all finite groups are both reductive and semi-simple. The dimension of $G$ is its dimension as an affine subvariety of $\mathrm{GL}_t(\mathbb{F})$. Its *rank* is the dimension of any maximal torus in $G$.

We consider a linear algebraic group $G$ over an arbitrary field $\mathbb{F}$ and a finite dimensional rational representation $\rho\colon G \to \mathrm{GL}(V)$ defined over $\mathbb{F}$. The term *rational* means that $\rho$ is given by polynomial functions on $G$. A more precise formulation of this is given in Section 8. Here and below we denote the $G$-action by writing $h \cdot v$ for $(\rho(h))(v)$ where $h \in G$, and $v \in V$.

Throughout we will always assume that representations are rational and finite dimensional. We will use $\mathbb{F}$ to denote the underlying field over which $G$ and $V$ are defined unless specified otherwise. We say the representation is *faithful* if $\rho$ is injective and *almost faithful* if $\rho$ has a finite kernel. We write $\mathbb{F}[V]$ for the symmetric algebra on $V^*$. If $\{x_1, x_2, \ldots, x_n\}$ is a basis for $V^*$ then $\mathbb{F}[V]$ is the polynomial ring in the $n$ indeterminants $x_1, x_2, \ldots, x_n$. This ring is graded by polynomial degree: $\mathbb{F}[V] = \bigoplus_{d=0}^{\infty} \mathbb{F}[V]_d$.

The action of $G$ on $V$ induces a natural action of $G$ on $V^*$ given by

$$(g \cdot f)(v) = f(g^{-1} \cdot v) \quad \text{for all } f \in V^*,\ v \in V \text{ and } g \in G.$$

The action on $V^*$ extends multiplicatively to a degree preserving action of $G$ on $\mathbb{F}[V]$. The *ring of invariants* $\mathbb{F}[V]^G$ is the graded subring of $\mathbb{F}[V]$ consisting of those polynomials which are fixed by every element of $G$:

$$\mathbb{F}[V]^G := \big\{ f \in \mathbb{F}[V] \mid g \cdot f = f \text{ for all } g \in G \big\}.$$

In his famous address to the International Congress in 1900, the 14th problem posed by David Hilbert was to determine whether every ring of invariants is finitely generated. Hilbert had already shown this to be true for $\mathrm{SL}_n(\mathbb{C})$ and $\mathrm{GL}_n(\mathbb{C})$. In 1959, M. Nagata [36] answered Hilbert's question in the negative by giving an example of a 32-dimensional representation of a 28-dimensional group defined over the field of complex numbers $\mathbb{C}$ whose ring of invariants is not finitely generated. For a discussion of Hilbert's 14th problem and its counterexamples see the article by Gene Freudenberg [17].

Due to results of Hilbert, H. Weyl, D. Mumford, Nagata and W. Haboush among others, it has been shown that $\mathbb{F}[V]^G$ is always finitely generated if $G$ is a reductive group. Accordingly we will assume from now on that $G$ is reductive.

We define the *Noether Number of* $V$,

$$\beta(G,V) := \min\bigl\{d \bigm| \mathbb{F}[V]^G \text{ is generated as a ring by } \bigoplus_{i=0}^{d} \mathbb{F}[V]^G_i\bigr\}$$

and the *Noether Number of* $G$,

$$\beta(G) := \sup\{\beta(G,V) \mid V \text{ is a finite dimensional } G\text{-representation over } \mathbb{F}\}.$$

Note that the number $\beta(G)$ depends upon the underlying field $\mathbb{F}$ which will be understood from the context.

Consider the maximal homogeneous ideal $\mathbb{F}[V]^G_+ := \bigoplus_{d=1}^{\infty} \mathbb{F}[V]^G_d \subset \mathbb{F}[V]^G$ and the natural surjection $\nu\colon \mathbb{F}[V]^G_+ \to \mathbb{F}[V]^G_+/(\mathbb{F}[V]^G_+)^2$. The graded Nakayama Lemma [7, Lemma 3.5.1] implies that a set of homogeneous positive degree invariants $\{f_1, f_2, \ldots, f_s\}$ generates $\mathbb{F}[V]^G$ if and only if its image $\{\nu(f_1), \nu(f_2), \ldots, \nu(f_s)\}$ spans the graded vector space $\mathbb{F}[V]^G_+/(\mathbb{F}[V]^G_+)^2$. Moreover this set of invariants minimally generates $\mathbb{F}[V]^G$ if and only if its image under $\nu$ is a vector space basis for $\mathbb{F}[V]^G_+/(\mathbb{F}[V]^G_+)^2$. Thus we can characterize $\beta(G,V)$ as the maximum integer $d$ such that $\bigl(\mathbb{F}[V]^G_+/(\mathbb{F}[V]^G_+)^2\bigr)_d \neq \{0\}$.

Suppose now that $\overline{\mathbb{F}}$ is any field extension of $\mathbb{F}$ and that $G$ and $V$ are defined over $\mathbb{F}$. Extending $\mathbb{F}$ to $\overline{\mathbb{F}}$, we may replace $V$ by $\overline{V} := V \otimes_{\mathbb{F}} \overline{\mathbb{F}}$ and $G \subset \mathrm{GL}_t(\mathbb{F}) \subset \mathrm{GL}_t(\overline{\mathbb{F}})$ by its toplogical closure $\overline{G}$ in $\mathrm{GL}_t(\overline{\mathbb{F}})$. Clearly, a set of invariants in $\mathbb{F}[V]^G_+$ maps to a basis for $\mathbb{F}[V]^G_+/(\mathbb{F}[V]^G_+)^2$ if and only if this same set maps to a basis for $\overline{\mathbb{F}}[\overline{V}]^{\overline{G}}_+/(\overline{\mathbb{F}}[\overline{V}]^{\overline{G}}_+)^2$. This shows that $\beta(V,G) = \beta(\overline{V},\overline{G})$. For this reason, unless stated otherwise, we will not assume that the field $\mathbb{F}$ is algebraically closed. Below, when working over non-algebraically closed fields, we will be considering a finite group $G$ which topologically may be viewed as a set of discrete points, and so we will have $\overline{G} = G$.

The behaviour of rings of invariants depends greatly upon whether the characteristic of the field $\mathbb{F}$ is zero or not. For example, many classical results which hold in characteristic zero fail over fields of positive characteristic. For finite groups the key question is whether $|G|$ is a unit. If $G$ is finite we distinguish two cases: if $|G| \in \mathbb{F}^\times$ the group and its (faithful) representations are called *non-modular*; otherwise they are called *modular*.

One very important tool, if it exists, is a so-called Reynolds operator. A *Reynolds operator* is a $G$-equivariant projection $\phi\colon \mathbb{F}[V] \to \mathbb{F}[V]^G$, *i.e.*, an $\mathbb{F}$-linear map satisfying the two conditions that $\phi(g \cdot f) = \phi(f)$ for all $g \in G$, $f \in \mathbb{F}[V]$ and that $\phi(f) = f$ for all $f \in \mathbb{F}[V]^G$. If a Reynolds operator for $V$ exists, it is unique.

In characteristic zero, every representation $V$ of a reductive group $G$ has a Reynolds operator. For finite non-modular groups, averaging over the group is the Reynolds operator:

$$\phi(f) := \frac{1}{|G|}\sum_{g\in G} g \cdot f.$$

G. Kempf [33] showed how bounds on the Noether Numbers for finite groups, semi-simple groups, and tori may be combined to obtain a bound on the Noether Number for any reductive group in characteristic 0, as follows. Let $V$ be a representation of a reductive group $G$ defined over a field $\mathbb{F}$ of characteristic 0. Suppose that $H$ is a normal subgroup of $G$ and suppose that $H$ is itself reductive. The action of $G$ on $V$ induces an action of $G/H$ on $\mathbb{F}[V]^H$. Define $W$ by $W^* := \bigoplus_{d=0}^{\beta(H,V)} \mathbb{F}[V]^H_d$. Then $W$ is a finite dimensional rational representation of the reductive group $G/H$. Consider the natural surjection $\phi\colon \mathbb{F}[W] \to \mathbb{F}[V]^H$ induced by the inclusion of $W^*$ into $\mathbb{F}[V]^H$. (Recall that $\mathbb{F}[W]$ is the symmetric algebra on $W^*$.) This map commutes with the action of $G/H$. Applying the Reynolds operators for $G/H$ for these representations gives a surjection $\phi^{G/H}\colon \mathbb{F}[W]^{G/H} \to (\mathbb{F}[V]^H)^{G/H} = \mathbb{F}[V]^G$. From this we see that $\beta(G,V) \le \beta(G/H,W)\cdot\beta(H,V)$. Thus we obtain a bound for the Noether Number of $G$ acting on $V$ using the two smaller groups $H$ and $G/H$.

For the general reductive group $G$ acting on the representation $V$ we first consider the connected normal reductive subgroup $G^0$ and the finite quotient group $G/G^0$. Then the radical of $G^0$ is a torus $T$. Furthermore $T$ is normal in $G^0$ and the quotient $G^0/T$ is a connected semi-simple group. Thus we find

$$\begin{aligned}\beta(G,V) &\le \beta(G/G^0,W)\cdot\beta(G^0,V)\\ &\le \beta(G/G^0,W)\cdot\beta(G^0/T,U)\cdot\beta(T,V)\end{aligned}$$

for certain representations $W$ of $G/G^0$ and $U$ of $G^0/T$.

## 3. Bounds for non-modular representations of finite groups.

In 1915, Emmy Noether [37] proved, for a finite group $G$ over the field of complex numbers $\mathbb{C}$, that $\beta(G) \le |G|$. An examination of her proof shows that it is valid for any field of characteristic 0 and also for fields of characteristic $p$ if $|G| < p$. In 1926 [38], she proved that the ring of invariants of a modular representation of a finite group is finitely generated but did not give a bound for $\beta(G,V)$.

Here we will prove that $\beta(G) \le |G|$ under the weaker hypothesis that $|G|$ is invertible in $\mathbb{F}$. This was proved independently by P. Fleischmann [12] and J. Fogarty [16] in 2000. D. Benson (see [7, p. 109]) simplified Fogarty's proof and here we present this simplified version.

Theorem 3.1. *Let $V$ be a vector space and let $G$ be a finite subgroup of* $\mathrm{GL}(V)$*. If $|G|$ is invertible in $\mathbb{F}$ then $\beta(G,V) \leq |G|$.*

Proof. Put $m := |G|$ and $[m] = \{1, 2, \ldots, m\}$. We begin by considering $\mathbb{F}[V]_+ := \sum_{d=1}^{\infty} \mathbb{F}[V]_d$, the unique homogeneous maximal ideal of $\mathbb{F}[V]$. We first show that its $m$-th power $(\mathbb{F}[V]_+)^m$ is a subset of the Hilbert ideal $J := (\mathbb{F}[V]_+^G)\mathbb{F}[V]$, the ideal generated by the homogeneous invariants of positive degree.

To see this take any $f_1, f_2, \ldots, f_m \in \mathbb{F}[V]_+$. Write $G = \{g_1, g_2, \ldots, g_m\}$, let $g \in G$ and consider the product $\prod_{i=1}^{m}\bigl(f_i - (gg_i)(f_i)\bigr) = 0$. Expanding this expression and summing over all $g \in G$ gives

$$\sum_{A \subseteq [m]} (-1)^{m-|A|} h_A \prod_{i \in A} f_i = 0,$$

where $h_A := \sum_{g \in G} \prod_{i \in [m] \setminus A} g(g_i f_i) \in \mathbb{F}[V]^G$.

The summand corresponding to $A = [m]$ in the above is $|G| f_1 f_2 \cdots f_m$. For all other subsets $A$, we have $h_A \in \mathbb{F}[V]_+^G$, and thus the summand corresponding to $A$ lies in the Hilbert ideal $J$. Therefore $f_1 f_2 \cdots f_m \in J$ and thus $(\mathbb{F}[V]_+)^m \subseteq J$.

By the Hilbert Basis Theorem (Theorem 5.2 below), there exist finitely many homogeneous invariants $h_1, h_2, \ldots, h_r \in \mathbb{F}[V]^G$ which generate the Hilbert ideal $J$. Without loss of generality we may assume that $\{h_1, h_2, \ldots, h_r\}$ is a minimal such set of invariants. Note that if $\deg h_i > m$ then $h_i = \sum_{j=1}^{n} h_{ij} x_j$, where each $h_{ij}$ is a homogeneous element of $\mathbb{F}[V] = \mathbb{F}[x_1, x_2, \ldots, x_n]$ with $\deg(h_{ij}) \geq m$, *i.e.*, where $h_{ij} \in (\mathbb{F}[V]_+)^m \subset J$. Since $m \leq \deg h_{ij} < \deg h_i$, we see that $h_{ij}$ lies in the ideal of $\mathbb{F}[V]$ generated by $h_1, h_2, \ldots, \widehat{h_i}, \ldots, h_r$. Thus if $\deg h_i > m$ then $h_i$ is not required as a generator of $J$. Thus our assumption that $h_1, h_2, \ldots, h_r$ minimally generate $J$ implies that $\deg h_i \leq m$ for all $i = 1, 2, \ldots, r$.

Consider any invariant $f \in \mathbb{F}[V]^G$ with $\deg(f) > m$. Since $\deg(f) > m$ we see that $f \in (\mathbb{F}[V]_+)^m \subseteq J$ and we may write $f = \sum_{i=1}^{r} k_i h_i$ where each $k_i$ is a homogeneous element of $\mathbb{F}[V]_+$. Applying the Reynolds operator $\phi$ we obtain $f = \phi(f) = \sum_{i=1}^{r} \phi(k_i h_i) = \sum_{i=1}^{r} \phi(k_i) h_i$. Since $\phi(k_i) \in \mathbb{F}[V]^G$, this expresses $f$ as a polynomial in homogeneous invariants of degree strictly less than $\deg(f)$. Hence $f$ cannot be part of a homogeneous minimal algebra generating set for $\mathbb{F}[V]^G$. ■

The above proof shows that in the non-modular case the Hilbert ideal is generated by homogeneous elements of degree at most $|G|$. G. Kemper [7, Conjecture 3.8.6 (b)] has made the following conjecture.

Conjecture 3.2. *Let $V$ be a representation of a finite group $G$. The Hilbert ideal $(\mathbb{F}[V]_+^G)\mathbb{F}[V]$ is generated by homogeneous elements of degree at most $|G|$.*

Consider a finite cyclic group $G$ of order $n$ and let $\mathbb{F}$ be a field of characteristic 0 containing a primitive $n$-th root of unity, $\xi$. Let $\sigma$ denote a generator of $G$. There are exactly $n$ inequivalent irreducible representations $W_0, W_1, \ldots, W_{n-1}$ of $G$, each of which is one-dimensional. The action of $G$ on $W_i$ is given by $\sigma \cdot v = \xi^i v$ for all $v \in W_i$.

It is easy to see that $\mathbb{F}[W_i]^{C_n} = \mathbb{F}[x^{n/\gcd(i,n)}]$, and thus if $i$ is relatively prime to $n$ then $\beta(C_n, W_i) = n$. Therefore we see that Noether's bound is sharp for cyclic groups.

Barbara Schmid [44] proved the following two inequalities for finite groups.

Proposition 3.3. *Let $G$ be a finite group defined over a field of characteristic zero. Let $H \leq G$ be a subgroup of $G$.*

(1) $\beta(G) \leq \beta(H)[G : H]$.
(2) *If $H$ is normal in $G$ then $\beta(G) \leq \beta(H)\beta(G/H)$.*

Remark 3.4. Although Schmid proved $\beta(G) \leq \beta(H)[G{:}H]$ under the assumption that $G$ is finite, her proof only requires that $H$ be of finite index in $G$.

Remark 3.5. Fleischmann [12] proved part (2) of Proposition 3.3 holds under the weaker assumption that $G$ is non-modular.

Remark 3.6. It is not known whether part (1) of Proposition 3.3 always holds over a field of positive characteristic when $G$ is non-modular. This question is known as the "Baby Noether gap".

Using the above inequalities Schmid proved:

Theorem 3.7. *Let $G$ be a finite group defined over a field of characteristic zero. If $G$ is not cyclic then $\beta(G) < |G|$.*

*Sketch of Proof* The proof is by induction on $|G|$. By Proposition 3.3 we see that if $G$ has either a proper subgroup $H < G$ or a proper quotient $G/H$ which is not cyclic, then by induction $\beta(G) < |G|$. Thus it is only necessary to consider groups $G$ all of whose proper subquotients are cyclic.

We consider two possibilities: $G$ is abelian or is not abelian. The abelian case is easily handled and we omit discussing it here.

If $G$ is not abelian and all proper subquotients of $G$ are cyclic then $G$ must be a semi-direct product of two groups of prime order: $G = C_p \rtimes C_q$ where $p$ and $q$ are two primes with $q$ dividing $p - 1$. By a careful study of the representations of such groups, $G$, Schmid was able to prove that $\beta(G) \leq pq - q + 1 < |G|$. ■

The above proof shows the importance of the groups $C_p \rtimes C_q$ for two primes $q < p$. The simplest case of such groups are the dihedral groups $C_p \rtimes C_2$. Schmid studied this case in detail and obtained the following more general exact result over $\mathbb{C}$.

Proposition 3.8. *$\beta(D_n) = n{+}1$ where $D_n$ is the dihedral group of order $2n$.*

Schmid also proved $\beta(A_4) = 6$.

In his Ph.D. thesis [39], Vivek Pawale studied $\beta(C_p \rtimes C_q)$ over $\mathbb{C}$, and he made the following conjecture.

Conjecture 3.9. *Let $p$ and $q$ be two primes such that $q$ divides $p-1$. Then $\beta(C_p \rtimes C_q) = p + q - 1$ (where the semi-direct product is not direct) over $\mathbb{C}$.*

Pawale proved $\beta(C_p \rtimes C_3) \leq p + 6$ and $\beta(C_7 \rtimes C_3) = 9$.

N. Wallach (see [9]) used the action of cyclic subgroups of $\Sigma_n$ to prove the following lower bound which shows that there can be no polynomial upper bound on $\beta(\Sigma_n)$.

Theorem 3.10. *For all $n$ sufficiently large,*

$$\beta(\Sigma_n) \geq e^{C\sqrt{n \ln n}},$$

*where $C$ is a positive constant less than 1.*

The work of Schmid has been extended by a number of people.

M. Domokos and P. Hegedūs [10] examined Schmid's proof by induction and were able to modify it to show:

Proposition 3.11. *Let $G$ be a finite non-cyclic group in characteristic 0.*

1. *If $|G|$ is even then $\beta(G) \leq \frac{3}{4}|G|$.*
2. *If $|G|$ is odd then $\beta(G) \leq \frac{5}{8}|G|$.*

M. Sezer [45] extended Proposition 3.11 to the non-modular case, *i.e.*, where $G$ is a finite group, $\mathbb{F}$ is a field of positive characteristic $p$ and $p$ does not divide $|G|$.

R. Shank [46] has observed that Schmid's induction proof works on any class of finite groups which is closed under taking subquotients and will yield a bound coming from the value of $\beta(G)$ for the minimal groups in such a class. Thus the fractions in the statement of Proposition 3.11 bounds arise from the fact that the Klein four group and the semi-direct products $C_p \rtimes C_q$ are the two base cases for the induction proofs. It is easy to see that $\beta(C_2 \times C_2) = 3$ and Domokos and Hegedūs prove that $\beta(C_p \rtimes C_q) \leq \frac{5}{8}pq$ (for $p$ and $q$ odd primes with $C_p \rtimes C_q$ non-abelian).

*3.12. Vector invariants.* Let $V$ be an $n$ dimensional representation of $G$. Let $m \in \mathbb{N}$. We denote by $m\,V$ the $nm$ dimensional representation

$$m\,V := \underbrace{V \oplus V \oplus \cdots \oplus V}_{m \text{ copies}}$$

on which $G$ acts diagonally via $g \cdot (v_1, v_2, \ldots, v_m) = (g \cdot v_1, g \cdot v_2, \ldots, g \cdot v_m)$. Invariants lying in $\mathbb{F}[m\,V]^G$ are called *vector invariants* of $V$. The classical procedure, known as *polarization*, constructs invariants of $m\,V$ from invariants of $V$ as follows. Given $f \in \mathbb{F}[V]^G$ consider the formal expansion

$$f(t_1 v_1 + t_2 v_2 + \cdots + t_m v_m) = \sum_{e_i \in \mathbb{N} 1 \leq i \leq m} t_1^{e_1} t_2^{e_2} \cdots t_m^{e_m} f_{e_1, e_2, \ldots, e_m}(v_1, v_2, \ldots, v_m)$$

where $(v_1, v_2, \ldots, v_m)$ is the general point in $m\,V$ and $t_1, t_2, \ldots, t_m$ are formal variables. The elements $f_{e_1, e_2, \ldots, e_m}$ are homogeneous invariants in $\mathbb{F}[m\,V]^G$ called polarizations of $f$. Notice that the polarizations of $f$ have the same degree as $f$. For more details on polarization see [53].

An important question is to consider the behaviour of $\beta(G, m\,V)$ as a function of $m$. The following theorem of H. Weyl [53] does not assume that $G$ is finite.

Theorem 3.13. *Let $V_1, V_2, \ldots, V_s$ be representations of the reductive group $G$ defined over a field $\mathbb{F}$ of characteristic zero. Put $n_i := \dim V_i$ and take integers $m_i \geq n_i$ for $i = 1, 2, \ldots, s$. Then $\mathbb{F}[m_1\, V_1 \oplus m_2\, V_2 \oplus \cdots \oplus m_s\, V_s]^G$ is generated by the polarizations of a set of generators of $\mathbb{F}[n_1\, V_1 \oplus n_2\, V_2 \oplus \cdots \oplus n_s\, V_s]^G$. In particular*

$$\beta(G, m_1\, V_1 \oplus m_2\, V_2 \oplus \cdots \oplus m_s\, V_s) = \beta(G, n_1\, V_1 \oplus n_2\, V_2 \oplus \cdots \oplus n_s\, V_s).$$

A consequence is the following.

Corollary 3.14. *Let $G$ be a finite group and let $\mathbb{F}$ be a field of characteristic zero. Let $V_{\text{reg}}$ denote the regular representation of $V$. Then*

$$\beta(G) = \beta(G, V_{\text{reg}}).$$

Proof. Let $V_1, V_2, \ldots, V_s$ be a complete set of inequivalent indecomposable representations of $G$. (Note that indecomposability and irreduciblility are equivalent here.) Put $n_i = \dim(V_i)$ for $i = 1, 2, \ldots, s$. Then $V_{\text{reg}} \cong n_1\, V_1 \oplus n_2\, V_2 \oplus \cdots \oplus n_s\, V_s$. Since every representation $V$ of $G$ may be written in the form $V \cong m_1\, V_1 \oplus m_2\, V_2 \oplus \cdots \oplus m_s\, V_s$ for some non-negative integers $m_1, m_2, \ldots, m_s$, the result follows. ■

4. **Bounds for modular representations of finite groups.** The behaviour of $\beta(G,V)$ in the modular setting is in sharp contrast to the characteristic zero situation. In a article published in 1990, David Richman [41] proved the following.

THEOREM 4.1. *Let $\mathbb{F}_q$ denote the finite field of order $q$ and let $G = \mathrm{SL}(V)$ where $V$ is an $n$ dimensional vector space over $\mathbb{F}_q$. Suppose that $m > n > 1$. Then*

$$\beta\big(\mathrm{SL}(V), m\,V\big) \geq (m-n+2)(q-1).$$

In 1990 (published posthumously in 1996), Richman [42] proved the following more general result.

PROPOSITION 4.2. *Let $\mathbb{F}$ be a field of positive characteristic $p$, let $G$ be a finite group whose order is divisible by $p$ and let $V$ be any faithful representation of $G$. Then*

$$\beta(G, m\,V) \geq \frac{m(p-1)}{p^{|G|-1}-1}.$$

Here we will give a proof of a related but simpler result of Richman's which applies over the prime field, *i.e.*, for the case $\mathbb{F} = \mathbb{F}_p$. In particular we will show that for that case

$$\beta(G, m\,V) \geq \frac{m}{\dim V - 1}.$$

Consider an element $\sigma \in G$ of order $p$. We choose a basis $\{x_1, x_2, \ldots, x_n\}$ for $V^*$ such that the element $\sigma \in \mathrm{GL}(V^*)$ takes Jordan normal form. Since $\sigma$ has order $p$ and the only $p$-th root of unity in characteristic $p$ is 1, we see that $(\sigma-1)x_j$ is either 0 or $x_{j-1}$ for all $j = 1, 2, \ldots, n$. Furthermore, we may assume that $(\sigma-1)x_n = x_{n-1}$. We construct the analogous basis $\{x_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ for $(m\,V)^*$. Thus $(\sigma-1)x_{i,j}$ is either 0 or $x_{i,j-1}$ and $(\sigma-1)x_{i,n} = x_{i,n-1}$, for all $i = 1, 2, \ldots, m$ and for all $j = 1, 2 \ldots, n$.

LEMMA 4.3. *Let $f \in \mathbb{F}_p[m\,V]^G$. If the coefficient in $f$ of the monomial $x_{1,n}^{a_1} x_{2,n}^{a_2} \cdots x_{m,n}^{a_m}$ is not zero then $p$ divides $a_i$ for all $i = 1, 2, \ldots, m$.*

PROOF. We may assume that $a_1 \geq 1$. Let $u$ and $v$ be the monomials $u := x_{1,n}^{a_1} x_{2,n}^{a_2} \cdots x_{m,n}^{a_m}$ and $v := u x_{1,n-1}/x_{1,n}$. Suppose $f = \cdots + cu + \cdots$ where $c \in \mathbb{F}_p$ is non-zero. Then $0 = \sigma(f) - f = \cdots + ca_1 v + \cdots$. Now it is not hard to see that $u$ is the unique monomial $w \in \mathbb{F}_p[m\,V]$ such that the coefficient of $v$ in $\sigma(w) - w$ is non-zero. Thus the coefficient of $v$ in $\sigma(f) - f$ is exactly $ca_1$. Since $\sigma(f) - f = 0$ and $c \neq 0$, we must have that $p$ divides $a_1$. Similarly we see that $p$ divides $a_i$ for all $i = 2, 3, \ldots, m$. ∎

We now prove $\beta(G, m\,V) \geq \frac{m}{\dim V - 1}$.

Proof. Define

$$f := \sum_{c_1\in\mathbb{F}_p}\sum_{c_2\in\mathbb{F}_p}\cdots\sum_{c_n\in\mathbb{F}_p}\prod_{i=1}^{m}(c_1x_{i,1}+c_2x_{i,2}+\cdots+c_nx_{i,n})^{p-1}.$$

By construction, $f$ is $\mathrm{GL}(V)$-invariant, hence also $G$-invariant.

Consider the monomial $\mu := (\prod_{i=1}^{n-1} x_{i,i}^{p-1})(\prod_{i=n}^{m} x_{i,n}^{p-1})$ where we assume $m >\ n$. The coefficient of $\mu$ in $f$ is given by

$$\sum_{c_1\in\mathbb{F}_p}\sum_{c_2\in\mathbb{F}_p}\cdots\sum_{c_n\in\mathbb{F}_p}\prod_{i=1}^{m} c_i^{p-1}c_n^{(m-n+1)(p-1)} = \sum_{c_1\in\mathbb{F}_p}\sum_{c_2\in\mathbb{F}_p}\cdots\sum_{c_n\in\mathbb{F}_p} 1 = (p-1)^n$$

which is not zero.

Let $f_1, f_2, \ldots, f_r$ be a homogeneous minimal generating set for $\mathbb{F}[m\,V]^G$ and express $f$ as a polynomial in these generating invariants. Then $\mu = \mu_1\mu_2\cdots\mu_s$ where each $\mu_k$ is a monomial occurring in some $f_i$.

Our goal is to show that there exists a $j$ with $1 \leq j \leq s$ such that $\deg(\mu_k) \geq m/(n-1)$. First suppose that some $\mu_k \in \mathbb{F}[x_{1,n}, x_{2,n}, \ldots, x_{m,n}]$. By the preceding lemma, this implies that every exponent of $\mu_k$ is divisible by $p$. But this cannot happen since $\mu_k$ divides $\mu$.

Define

$$\deg'\Big(\prod_{j=1}^{m}\prod_{i=1}^{n} x_{i,j}^{e_{j,i}}\Big) = \sum_{j=1}^{m}\sum_{i=1}^{n-1} e_{j,i}.$$

With this notation we know that $\deg'(\mu_k) \geq 1$ for all $k = 1, 2, \ldots, s$. Put $d_k := \deg(\mu_k)$ and $d'_k := \deg'(\mu_k)$ for $k = 1, 2, \ldots, s$.

We claim that there exists an index $\ell$ with $1 \leq \ell \leq s$ such that

$$\frac{d_\ell}{d'_\ell} \geq \frac{\sum_{k=1}^{s} d_k}{\sum_{k=1}^{s} d'_k}.$$

If not, then $d_\ell \sum_{k=1}^{s} d'_k < d'_\ell \sum_{k=1}^{s} d_k$ for all $k$. Summing these inequalities would give the contradiction $\sum_{\ell=1}^{s} d_\ell \sum_{k=1}^{s} d'_k < \sum_{\ell=1}^{s} d'_\ell \sum_{k=1}^{s} d_k$.

Now $\sum_{k=1}^{s} d_k = \deg(\mu) = m(p-1)$ and $\sum_{k=1}^{s} d'_k = \deg'(\mu) = (n-1)(p-1)$. From the definition of $\ell$ we see

$$\deg(\mu_\ell) = d_\ell \geq d'_\ell \frac{m(p-1)}{(n-1)(p-1)} \geq \frac{m}{n-1}. \qquad \blacksquare$$

Remark 4.4. The above results of Richman show that $\beta(G)$ may be infinite when $G$ is a finite modular group. Indeed the next theorem shows this is always the case. However, if we content ourselves with finding a so-called *separating subalgebra* of invariants rather than the entire ring of invariants, then we know [7, Corollary 3.9.14] that invariants of degree at most $|G|$ will always suffice.

H. Derksen and G. Kemper [8] proved that for a group $G$ defined over a field $\mathbb{F}$ of characteristic zero, that $\beta(G)$ is finite only when $G$ is finite. They conjectured that this result was true in any characteristic. R. Bryant and G. Kemper [2] were able to show this is indeed the case, giving the following theorem.

THEOREM 4.5. *Let $G$ be any linear algebraic group. If $\beta(G)$ is finite, then $G$ is a finite group with $|G| \in \mathbb{F}^{\times}$.*

We denote by $\theta_1$ the one-dimensional trivial representation of a group $G$. This is just the field $\mathbb{F}$ equipped with the trivial $G$-action. Since $\mathbb{F}[V \oplus \theta_1]^G = \mathbb{F}[x_1, x_2, \dots, x_n, z]^G \cong \mathbb{F}[x_1, x_2, \dots, x_n]^G \otimes \mathbb{F}[z]$ we see that $\beta(G, V \oplus \theta_1) = \beta(G, V)$. Thus when computing $\beta(G, V)$ it suffices to consider representations of $G$ which do not have $\theta_1$ as a summand. Such representations are called *reduced*.

Now we consider the case where $G = \mathbb{Z}/p$ the cyclic group of order $p$ where $p$ is the characteristic of $\mathbb{F}$. For this group there are precisely $p$ inequivalent indecomposable representations, one of each dimension $1, 2, \dots, p$. In a recent preprint [15], P. Fleischmann, M. Sezer, R. J. Shank and C. F. Woodcock prove the following exact result.

THEOREM 4.6. *Let $V$ be a reduced representation, defined over a field $\mathbb{F}$ of characteristic $p$, of the cyclic group $\mathbb{Z}/p$ of order $p$. Let $s$ be the maximum dimension of an indecomposable summand of $V$. (Thus $2 \le s \le p$.) Then*

$$\beta(\mathbb{Z}/p, V) = \begin{cases} p, & \text{if } V \cong V_2 \text{ or } V \cong 2\,V_2; \\ (p-1)\dim(V^{\mathbb{Z}/p}), & \text{if } V \cong m\,V_2 \text{ for } m \ge 3; \\ (p-1)\dim(V^{\mathbb{Z}/p}) + 1, & \text{if } s = 3; \\ (p-1)\dim(V^{\mathbb{Z}/p}) + p - 2, & \text{if } s \ge 4. \end{cases}$$

Derksen and Kemper showed [7, Theorem 3.9.11] how an old result of G. Hermann [19] can be used to obtain a bound for any modular representation of a finite group.

THEOREM 4.7. *Let $V$ be an $n$-dimensional modular representation of a finite group $G$. Then*

$$\beta(G, V) \le n(|G| - 1) + (|G|^{(2^{n-1})n+1})(n^{2^{n-1}+1}).$$

Recently D. B. Karaguezian and P. Symonds [27], [28] proved that if $\mathbb{F}$ is a finite field and $G$ is finite group then the infinite dimensional $G$ representation $\mathbb{F}[V]$ contains only finitely many inequivalent indecomposable $G$ subrepresentations. As a consequence of this they obtained the following improvement for finite fields.

THEOREM 4.8. *Let $V$ be an $n$ dimensional representation of a finite group $G$ defined over the finite field of order $q$ and characteristic $p$. Then $\beta(G, V) \le \frac{q^n - 1}{q - 1}(nq - n - 1)$. Furthermore, if $G$ is a $p$-group then $\beta(G, V) \le \frac{q^n - 1}{q - 1} - n$.*

E. Dade (see [49, p. 483]) gave a simple useful algorithm for constructing a set of so-called primary invariants for a finite group. We now describe his algorithm. Let $V$ be an $n$-dimensional representation of the finite group $G$ defined over any infinite field, $\mathbb{F}$. Since $\mathbb{F}$ is infinite, the vector space $V^*$ cannot be a finite union of proper subspaces.

Let $y_1$ be any non-zero element of $V^*$. For $i = 1, \ldots, n-1$ choose $y_{i+1} \in V^*$ such that $y_{i+1}$ does not lie in any of the $\mathbb{F}$ vector spaces spanned by $\{g_1 \cdot y_1, g_2 \cdot y_2, \ldots, g_i \cdot y_i\}$ for all $g_1, g_2, \ldots, g_i \in G$. Then define $f_i = \prod_{g \in G} g \cdot y_i$. Note that $\deg(f_i) = |G|$ for all $i = 1, 2, \ldots, n$. Then the set $\{f_1, f_2, \ldots, f_n\}$ is a homogeneous system of parameters as defined below (see Section 5). For non-modular finite groups, applying Theorem 6.6 gives the bound

$$\beta(G, V) \leq \max\{|G|, (n-1)|G|\}.$$

Remark 4.9. Note that if we begin working over a finite field $\mathbb{F}$ we may extend $\mathbb{F}$ to an infinite field $\widetilde{\mathbb{F}}$ and then use Dade's algorithm to construct $f_1, f_2, \ldots, f_n$. Then these $f_i$ will all lie in $\mathbb{F}'[V]^G$ for some finite field $\mathbb{F}'$ with $\mathbb{F} \subseteq \mathbb{F}' \subset \widetilde{\mathbb{F}}$. Also recall that $\beta(G, V)$ has the same value considered with respect to all three of these fields.

H. E. A. Campbell, A. V. Geramita, I. P. Hughes, R. J. Shank and the author [3] showed that the above bound is valid for modular finite groups if the ring of invariants satisfies the Gorenstein property.

In 1997, A. Broer [1] generalized these two results by weakening the hypothesis that $V$ is non-modular to the condition that $\mathbb{F}[V]^G$ is Cohen–Macaulay. The definition of Cohen–Macaulay is given in Section 5 below. Broer's bound is the following.

Theorem 4.10. *Let $V$ be a representation of a finite group $G$. If $\mathbb{F}[V]^G$ is Cohen–Macaulay then*

$$\beta(G, V) \leq \max\{|G|, (\dim V - 1)|G|\}.$$

In fact, it has been conjectured by many people that the hypothesis of Cohen–Macaulayness is not required:

Conjecture 4.11. *Let $V$ be a representation of a finite group $G$. Then*

$$\beta(G, V) \leq \max\{|G|, (\dim V - 1)|G|\}.$$

Kemper has conjectured [7, Conjecture 3.8.6 (a)] the following improvement of Broer's result.

Conjecture 4.12. *Let $V$ be a representation of a finite group $G$. If $\mathbb{F}[V]^G$ is Cohen–Macaulay then*

$$\beta(G, V) \leq |G|.$$

*4.13. Permutation groups.* A representation $V$ of $G$ is called a *permutation representation* if there is a basis $\{v_1, v_2, \dots, v_n\}$ of $V$ which is mapped to itself by all elements $g \in G$. In this case $\{v_1, v_2, \dots, v_n\}$ is called a *permutation basis.*

Suppose $V$ is a permutation representation of $G$ with permutation basis $\{v_1, v_2, \dots, v_n\}$ and let $\{x_1, x_2, \dots, x_n\}$ be the dual basis of $V^*$. Then $G$ will permute the $x_i$ and also the set of all monomials

$$\{x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \mid a_1, a_2, \dots, a_n \in \mathbb{N}\}.$$

Given a monomial $m := x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, let $G \cdot m = \{g \cdot m \mid g \in G\} = \{m = m_1, m_2, \dots, m_r\}$ be its orbit. We define the *orbit sum* of $m$, denoted $\mathcal{O}_G(m) = \mathcal{O}(m)$, by

$$\mathcal{O}(m) = \sum_{\alpha \in G\cdot m} \alpha = m_1 + m_2 + \cdots + m_r.$$

Note that if $V$ is a permutation representation of $G$, then the matrices representing elements of $G$ with respect to a permutation basis are permutation matrices. In particular these matrices contain only zeros and ones and thus such a representation is defined over any field. It is not hard to see that the set of orbit sums of all the monomials is a vector space basis for the ring of invariants.

The following result of M. Göbel [18] gives an upper bound on $\beta(G, V)$ for any permutation representation $V$.

Theorem 4.14. *Let $V$ be a permutation representation of a finite group $G$. Then $\beta(G, V) \leq \max\{\binom{\dim V}{2}, \dim V\}$.*

Proof. Let $\{v_1, v_2, \dots, v_n\}$ be a permutation basis of $V$ with dual basis $\{x_1, x_2, \dots, x_n\}$. The permutation group $\Sigma_n$ acts on $V$ and $V^*$ by permuting these bases. Then $\mathbb{F}[V]^G \supseteq \mathbb{F}[V]^{\Sigma_n} = \mathbb{F}[\sigma_1, \sigma_2, \dots, \sigma_n]$ where $\sigma_i$ is the $i$-th elementary symmetric function in $x_1, x_2, \dots, x_n$. We introduce a relation on the set of $G$-orbit sums of monomials as follows. Given two distinct orbit sums $\mathcal{O}_G(m_1)$ and $\mathcal{O}_G(m_2)$ we first write $\Sigma_n \cdot m_1 = \Sigma_n \cdot (x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n})$ and $\Sigma_n \cdot m_2 = \Sigma_n \cdot (x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n})$ where $a_1 \geq a_2 \geq \cdots \geq a_n$ and $b_1 \geq b_2 \geq \cdots \geq b_n$. Then we declare $\mathcal{O}_G(m_1) < \mathcal{O}_G(m_2)$ if and only if there is an index $j \geq 0$ with $a_1 = b_1$, $a_2 = b_2, \dots, a_j = b_j$ and $a_{j+1} < b_{j+1}$. If $\mathcal{O}_G(m_1) < \mathcal{O}_G(m_2)$ fails to hold we write $\mathcal{O}_G(m_1) \geq \mathcal{O}_G(m_2)$.

Note that in general $\mathcal{O}_G(m) \leq \mathcal{O}_G(m')$ and $\mathcal{O}_G(m') \leq \mathcal{O}_G(m)$ does not imply that $\mathcal{O}_G(m) = \mathcal{O}_G(m')$ (unless $G = \Sigma_n$). However this relation is transitive and does have has the property that for any monomial $m$, there are only finitely many $G$-orbit sums, $\mathcal{O}_G(m')$ with $\mathcal{O}_G(m') < \mathcal{O}_G(m)$. Furthermore if $m$, $m'$ and $m''$ are any three monomials with $\mathcal{O}_G(m') < \mathcal{O}_G(m)$ then $\mathcal{O}_G(m'm'') < \mathcal{O}_G(mm'')$.

A $G$-orbit sum $\mathcal{O}_G(x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n})$ is called *special* if $\{a_1, a_2, \dots, a_n\} = \{0, 1, 2, \dots, r\}$ for some positive integer $r$. Here we must have $1 \leq r \leq n-1$. We will show that the set of special $G$-orbit sums, together with the set of elementary symmetric functions $\sigma_1, \sigma_2, \dots, \sigma_n$, generate $\mathbb{F}[V]^G$. This clearly implies the theorem.

We will show that every orbit sum can be written as a polynomial in the elementary symmetric functions and the special $G$-orbit sums. Assume, by way of contradiction, that $\mathcal{O}_G(m)$ is some minimal $G$-orbit sum which does not lie in the ring generated by the special $G$-orbit sums together with the elementary symmetric functions. Write $m = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$.

If $m'$ is any monomial which is divisible by $\sigma_n = x_1 x_2 \cdots x_n$ then $\mathcal{O}_G(m') = \sigma_n \mathcal{O}_G(m'/\sigma_n)$ and thus $\mathcal{O}_G(m')$ can only lie in a minimal generating set for $\mathbb{F}[V]^G$ if $m' = \sigma_n$. Since $\mathcal{O}_G(m) \neq \sigma_n$ we must have some $b_i = 0$.

Since $\mathcal{O}_G(m)$ is a non-special orbit sum there must exist positive integers $t$ and $r = \max\{b_j \mid 1 \leq j \leq n\}$ such that $\{t+1, t+2, \ldots, r\} \subset \{b_1, b_2, \ldots, b_n\}$ and $t \notin \{b_1, b_2, \ldots, b_n\}$. Let

$$c_j := \begin{cases} b_j, & \text{if } b_j \leq t; \\ b_j - 1, & \text{if } b_j > t. \end{cases}$$

Define $m' := x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n}$ and $s := |\{j \mid b_j > t\}| = \deg(m) - \deg(m')$. Expanding $\sigma_s \mathcal{O}_G(m')$ as an integer linear combination of $G$-orbit sums, we have

$$\sigma_s \mathcal{O}_G(m') = \mathcal{O}_G(m) + \sum_{i=1}^{\ell} k_i \mathcal{O}_G(m_i)$$

for some some monomials $m_i$ and positive integers $k_i$. By the definition of $t$, we see that $\mathcal{O}_G(m_i) < \mathcal{O}_G(m)$ for all $1 \leq i \leq \ell$. Also it is clear that $\mathcal{O}_G(m') < \mathcal{O}_G(m)$. By the minimality of $\mathcal{O}_G(m)$, each of the orbit sums $\mathcal{O}_G(m_i)$ and $\mathcal{O}_G(m')$ lies in the ring generated by the special $G$-orbit sums together with the elementary symmetric functions. This contradiction completes the proof of the theorem. ∎

In contrast to Göbel's theorem, Kemper [29] found the following lower bound for a permutation representation.

Theorem 4.15. *Let $\mathbb{F}$ be a field of characteristic $p$ and let $V$ be a faithful modular permutation representation of the finite group $G$. Suppose $G$ contains an element of order $p^k$ for some $k \in \mathbb{N}$. Then*

$$\beta(G, m\,V) \geq m(p^k - 1).$$

About the same time, Fleischmann [11] obtained the following exact result.

Theorem 4.16. *Let $G = \Sigma_n$ be the symmetric group on $n = p^k$ letters acting naturally by permuting a basis of the $n$-dimensional representation $V$ over the field $\mathbb{F}_q$ of order $q = p^r$. Then*

$$\beta(\Sigma_n, m\,V) = \max\{n, m(n-1)\}.$$

## 5. **Infinite groups in characteristic zero.**

In the 1870's Camille Jordan [25], [26] obtained the following bound for $G = \mathrm{SL}_2(\mathbb{C})$. For a modern discussion of this result see the article [54] by J. Weyman.

Theorem 5.1. *Let $V$ be a representation of $\mathrm{SL}_2(\mathbb{C})$. Suppose that when $V$ is decomposed into a direct sum of irreducible sub-representations that all irreducible components of $V$ have dimension $\leq t+1$. Then $\beta\big(\mathrm{SL}_2(\mathbb{C}), V\big) \leq 2t^6$.*

In 1890 [20] and 1893 [21], David Hilbert published two of the most important and influential papers in modern algebra. In the 1890 paper, Hilbert proved the *Hilbert Basis Theorem* which we now state.

Theorem 5.2. (Hilbert Basis Theorem) *Every generating set for an ideal in the polynomial ring $\mathbb{F}[x_1, x_2, \ldots, x_n]$ contains a finite generating set.*

Using this theorem Hilbert showed that $\mathbb{F}[V]^G$ is finitely generated for $G = \mathrm{SL}_n(\mathbb{C})$ and $G = \mathrm{GL}_n(\mathbb{C})$. Here we give Hilbert's proof of this fact for more general $G$.

Theorem 5.3. *Suppose $V$ is representation of the group $G$ which has a Reynolds operator $\rho$. Then $\mathbb{F}[V]^G$ is a finitely generated $\mathbb{F}$-algebra.*

Proof. Let $J$ denote the Hilbert ideal $J := (\mathbb{F}[V]^G_+)\mathbb{F}[V]$. By the Hilbert Basis Theorem, there exist homogeneous invariants $h_1, h_2, \ldots, h_r \in \mathbb{F}[V]^G_+$ which generate $J$. Suppose that $f \in \mathbb{F}[V]^G$ is homogeneous of degree $d$. We will show by induction on $d$ that $f \in \mathbb{F}[h_1, \ldots, h_r]$. This is clear for $d = 0$. For general $d$, since $f \in J$, we may write $f = \sum_{i=1}^r k_i h_i$ where $k_i \in \mathbb{F}[V]$ is homogeneous with $\deg(k_i) < d$ for $i = 1, 2, \ldots, r$. Applying the Reynolds operator gives

$$f = \rho(f) = \sum_{i=1}^{r} \rho(k_i) h_i.$$

By induction, $\rho(k_i) \in \mathbb{F}[h_1, h_2, \ldots, h_r]$ for $i = 1, 2, \ldots, r$ and therefore $f \in \mathbb{F}[h_1, h_2, \ldots, h_r]$. ■

Although this proof does show that $\mathbb{F}[V]^G$ is finitely generated, it is not a constructive proof and for this reason Hilbert's 1890 paper occasioned much criticism. Most famously, Paul Gordon said "Das ist nicht Mathematik, das ist Theologie!" [This is not mathematics; this is theology].[1]

In light of these criticisms Hilbert attempted to give a more constructive proof of the finite generation. The result was his 1893 paper. For the second proof Hilbert introduced and proved the *Nullstellensatz*, the so-called *Noether Normalization Lemma* and the *Hilbert Syzygy Theorem.* Together with the Basis Theorem these are four of the most important theorems in modern algebra.

[1] Later, after Gordan simplified Hilbert's 1890 proof and exploited it for his own purposes, Gordan added "I have become persuaded that even theology has its uses."

Let $R = \sum_{d=0}^{\infty} R_d$ be a graded Noetherian $\mathbb{F}$-algebra. A sequence $f_1, f_2, \ldots, f_r$ of homogeneous elements of $R$ is called a *homogeneous system of parameters* if $f_1, f_2, \ldots, f_r$ are algebraically independent and $R$ is finitely generated as a module over the subring $A = \mathbb{F}[f_1, f_2, \ldots, f_r]$, *i.e.*, if there exist $g_1, g_2, \ldots, g_m \in R$ such that $R = Ag_1 + Ag_2 + \cdots + Ag_m$. The Noether Normalization Lemma, proved by Hilbert in his 1893 paper, asserts that $R$ always has a homogeneous system of parameters. The number $r$ is called the *Krull dimension* of $R$. It can also be characterized as maximum number of algebraically independent elements in $R$.

The ring $R$ is *Cohen–Macaulay* if $R$ is a free $\mathbb{F}[h_1, h_2, \ldots, h_r]$-module for some homogeneous system of parameters, $h_1, h_2, \ldots, h_r$. It can be shown that if $R$ is Cohen–Macaulay then $R$ is a free $\mathbb{F}[h_1, h_2, \ldots, h_r]$-module for every homogeneous system of parameters, $h_1, h_2, \ldots, h_r$.

A very important result in invariant theory is the Theorem of Hochster and Roberts [23], [31] which asserts that if $\mathbb{F}$ is characteristic zero and $G$ is a reductive group, then $\mathbb{F}[V]^G$ is Cohen–Macaulay.

Let $h_1, h_2, \ldots, h_r$ be a homogeneous system of parameters and define $A := \mathbb{F}[h_1, h_2, \ldots, h_r]$. If $R$ is Cohen–Macaulay we may write $R = Ag_1 \oplus Ag_2 \oplus \cdots \oplus Ag_t$ where $g_1, g_2, \ldots, g_t$ are homogenous elements of $R$. This decomposition of $R$ as a direct sum of cyclic $A$-modules is called a *Hironaka decomposition*. Notice that $R$ is generated (usually non-minimally) as an algebra by the elements $h_1, h_2, \ldots, h_r, g_1, g_2, \ldots, g_t$. In particular, the highest degree needed for a generator of $R$ is at most $\max\{\deg(h_1), \deg(h_2), \ldots, \deg(h_r), \deg(g_1), \deg(g_2), \ldots, \deg(g_t)\}$.

If $R = \mathbb{F}[V]^G$, then the elements of a homogeneous system of parameters, $f_1, f_2, \ldots, f_r$, are called *primary invariants*, and the module generators

$$g_1, g_2, \ldots, g_m \in R$$

are called *secondary invariants*. Of course there are many choices for primary invariants and secondary invariants.

## 6. Semi-simple groups.

*6.1. Hilbert's 1893 proof.* In his 1893 proof, Hilbert attempted to bound $\beta(G, V)$ in order to obtain a constructive proof of the finite generation of $\mathbb{C}[V]^G$. However, as he remarks in the paper, he was unable to get an upper bound and so "[left] the question of an explicit calculation of $[\beta(G, V)]$ somewhat vague."

Here is an outline of some of the programme of Hilbert's 1893 proof.

The nullcone $\mathcal{N}$ of $V$ is the subset of $V$ defined by

$$\mathcal{N} := \{v \in V \mid f(v) = 0 \text{ for all } f \in \mathbb{F}[V]^G_+\}.$$

We say that a set of homogenous invariants $\Omega$ *cuts out the nullcone* if $f(v) = 0$ for all $f \in \Omega$ implies that $v \in \mathcal{N}$. Hilbert showed that a set of invariants $\Omega$ cuts out the null cone if and only if the algebra $B$ generated by $\Omega$ is such that $\mathbb{F}[V]^G$ is a finite $B$-module.

The number $\sigma(G,V)$ is defined to be the least integer $b$ such that the set $\bigcup_{d=1}^{b} \mathbb{F}[V]_d^G$ cuts out the null cone.

By the Hilbert Basis theorem there exists a finite set $k_1, k_2, \ldots, k_s \in \mathbb{F}[V]^G$ of homogeneous invariants which cut out the nullcone and with $c_i := \deg(k_i) \leq \sigma(G,V)$ for all $i$. Let $N$ be the least common multiple of $c_1, c_2, \ldots, c_s$. Then the invariants $k_i' := k_i^{N/c_i}$ all have the same degree, namely $N$. Furthermore it is easy to see that $k_1', k_2', \ldots, k_s'$ also cut out the nullcone. Since the $k_i'$ share the same degree, by Hilbert's proof of the Noether Normalization Lemma, there exists a homogeneous system of parameters $f_1, f_2, \ldots, f_r$ with each $f_i$ a linear combination of the $k_i'$. In particular, $\deg(f_i) = N$ for all $i$. Hilbert was able to bound $\sigma(G,V)$ (for $G = \mathrm{SL}_n(\mathbb{C})$) and thus to bound the degrees of the primary invariants $f_1, f_2, \ldots, f_r$. However he was unable to extend this to a bound for $\beta(G,V)$.

*6.2. Popov's bound.* In 1981, V. L. Popov using modern results extended the above ideas of Hilbert as follows.

The power series $\mathcal{H}(R,\lambda) := \sum_{d=0}^{\infty} \dim_{\mathbb{F}}(R_d)\lambda^d$ is called the *Hilbert Series* of the graded algebra $R$. One consequence of the Hilbert Syzygy Theorem is that the Hilbert series of a Noetherian graded algebra can always be expressed as a rational function.

Let $h_1, h_2, \ldots, h_r$ be a homogeneous system of parameters for $\mathbb{F}[V]^G$ and define $A := \mathbb{F}[h_1, h_2, \ldots, h_r]$. Since $A \cong \mathbb{F}[h_1] \otimes \mathbb{F}[h_2] \otimes \cdots \otimes \mathbb{F}[h_r]$, it is easy to see that $\mathcal{H}(A,\lambda) = \prod_{i=1}^{r}(1-\lambda^{a_i})$ where $a_i = \deg(h_i)$. Then the Hironaka decomposition shows that

$$\mathcal{H}(R,\lambda) = \frac{\sum_{j=1}^{t} \lambda^{b_j}}{\prod_{i=1}^{r}(1-\lambda^{a_i})} \tag{6.2.1}$$

where $g_1, g_2, \ldots, g_t$ are secondary invariants and $b_j = \deg(g_j)$.

The degree of a rational function $f(\lambda)/h(\lambda)$ is defined to be $\deg\bigl(f(\lambda)\bigr) - \deg\bigl(h(\lambda)\bigr)$. In 1979, G. Kempf [31] showed that in characteristic 0 the degree of $\mathcal{H}(\mathbb{F}[V]^G,\lambda)$ is always negative. Therefore $b_j \leq a_1 + a_2 + \cdots + a_r$ for all $j = 1, 2, \ldots, t$ and thus $\beta(G,V) \leq a_1 + a_2 + \cdots + a_r$.

Combining this with Hilbert's method, Popov obtained the following.

THEOREM 6.3. *Suppose that $G$ is a connected semi-simple group defined over a field $\mathbb{F}$ of characteristic zero and that $V$ is an almost faithful $G$-representation. Then*

$$\beta(G,V) \leq \dim(V)\,\mathrm{lcm}\{1, 2, \ldots, \sigma(G,V)\}.$$

Following Hilbert's proof, Popov bounded $\sigma(G,V)$ and proved the following bound.

Theorem 6.4. *Suppose that $G$ is a connected semi-simple group defined over a field $\mathbb{F}$ of characteristic zero and that $V$ is an almost faithful $G$-representation. Then*

$$\beta(G,V) \leq r\, C\Bigg(\frac{2^{d+q} n^{q+1}(n-1)^{q-d} w^r (q+1)!}{3^q \Big(\big(\frac{q-d}{2}\big)!\Big)^2}\Bigg)$$

*where $q = \dim G$, $r = \text{Krull} \dim \mathbb{F}[V]^G \leq n = \dim V$, $d = \operatorname{rank} G \leq r$, $C(x)$ is the least common multiple of $\{1, 2, \ldots, \lfloor x \rfloor\}$ and $w = w(T) \in \mathbb{N}$ is defined, in Section 7, using the action on $V$ of a maximal torus $T$ of $G$.*

In 1993, Karin Hiss [22] gave new bounds for $\sigma(G,V)$ which have the advantage of being independent of $\dim V$. One of her bounds is expressed in terms of the *nilpotency degree* $N_V$ of $V$ which is defined as follows. The Borel subgroup $B$ of $G$ can be written as a product $B = TU$ where $U$ is a maximal unipotent subgroup of $G$ and $T$ is a maximal torus in $G$. Then $N_V := \min\{s \mid X^s(v) = 0 \text{ for all } v \in V,\ X \in \text{Lie Algebra } (U)\}$. Hiss proved the following bound.

Theorem 6.5. *Let $V$ be a representation of a connected semi-simple group defined over an algebraically closed field. Then*

$$\sigma(G,V) \leq \frac{2^r (m+1)!\, r!}{((m-r)/2)!^2} N_V^{m-r} \operatorname{Vol}(\mathcal{W}_V)$$

*where $m = \dim G$, $r = \operatorname{rank} G$, and $\mathcal{W}_V$ is the convex hull of the weights of $V$ as described in Section 7 below.*

Hiss also proved another upper bound on $\sigma(G,V)$ involving the degree (as varieties) of the $G$ orbits in $V$. Derksen [5], using a result of Kazarnovskii gave an improvement on Hiss's bounds.

In 1989, F. Knop [34] showed that if $G$ is connected and semi-simple and the characteristic of $\mathbb{F}$ is zero then $\deg\big(\mathcal{H}(\mathbb{F}[V]^G, \lambda)\big) \leq -\dim\big(\mathbb{F}[V]^G\big)$. This gives the following improvement of Theorem 6.3.

Theorem 6.6. *Let $V$ be a representation of a connected connected semi-simple group $G$ defined over a field $\mathbb{F}$ of characteristic zero. Suppose $a_1, a_2, \ldots, a_r$ is a homogeneous system of parameters for $\mathbb{F}[V]^G$. Then*

$$\beta(G,V) \leq \max\{a_1 + a_2 + \cdots + a_r - r, a_1, a_2, \ldots, a_r\}.$$

## 7. Tori.

Suppose that $\mathbb{F}$ is algebraically closed and $G = T$ is a torus, *i.e.*, $G \cong (\mathbb{F}^\times)^r$ for some $r \in \mathbb{N}$. In 1987, Kempf [31] adapted the 1981 proof by Popov of Theorem 6.4 to representations of tori.

Let $G = T$, be a torus. We may choose a basis $\{x_1, x_2, \ldots, x_n\}$ of the dual space of $V$, $V^*$ such that $t \cdot x_i = \omega_i(t) x_i$ for some $\omega_i \in X^*(T) \cong \mathbb{Z}^r$, the character group of $T$. In this case we say $T$ acts diagonally on $V$. The elements $\omega_1, \omega_2, \ldots, \omega_n$ are called the weights of $V$. We denote their convex hull in $X^*(T) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^r$ by $\mathcal{W}_V$.

Let $S$ be the monoid $S := \{E = (e_1, \ldots, e_n) \in \mathbb{Z}^n \mid \sum_{i=1}^n e_i\omega_i = 0 \in X^*(T)\}$. Then $E \in S$ if and only if $X^E = x_1^{e_1} \cdots x_n^{e_n} \in \mathbb{F}[V]^T$. Fix an explicit isomorphism $\psi\colon X^*(T) \to \mathbb{Z}^r$ and write $\omega_i = (\omega_{i,1}, \ldots, \omega_{i,r})$ with $\omega_{i,j} \in \mathbb{Z}$. Then the value $w$, used in Popov's bound given above, is defined by $w = w(T) := \max\{|\omega_{i,j}| : 1 \leq i \leq n, 1 \leq j \leq r\}$. Notice that the value of $w$ depends on the choice of $\psi$, which is determined only up to $\mathrm{GL}_r(\mathbb{Z})$.

Studying $S$, Kempf [33] was able to find $k_1, \ldots, k_s$ with $\mathbb{F}[V]^T$ finitely generated over $\mathbb{F}[k_1, \ldots, k_s]$ and $\deg k_j \leq n\, r!\, w^r$ for all $1 \leq j \leq s$ and so prove the following.

Theorem 7.1. *Let $V$ be an $n$-dimensional faithful representation for an $r$-dimensional torus, $T \cong (\mathbb{F}^\times)^r$. Then $\beta(T, V) \leq n\, C(n\, r!\, w^r)$ where $C(x) =$ least common multiple of $\{1, 2, \ldots, \lfloor x \rfloor\}$.*

The author [50] used geometric properties of the monoid $S$ and of the cone it generates $C = S \otimes_{\mathbb{Z}} \mathbb{Q}_{\geq 0} \subset X^*(T) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^r$ to obtain a much better (sometimes sharp) bound for $\beta(T, V)$.

Theorem 7.2. *Let $V$ be an $n$-dimensional diagonal faithful representation of torus $T \cong (\mathbb{F}^\times)^r$. Then $\beta(T, V) \leq (n - r)\, r!\, \mathrm{Vol}(\mathcal{W}_V)$. In terms of the number $w$, we have $\beta(T, V) \leq (n - r)\lfloor w^r (r + 1)^{(r+1)/2} \rfloor$.*

Proof. Since any invariant is a linear combination of invariant monomials it suffices to consider invariant monomials and thus we may concentrate our attention on $S$.

We define the degree of an element $E$ of $S$ by $\deg(E) := \deg X^E$. The cone $C$ has a finite number of extremal rays: $L_1, L_2, \ldots, L_s$. These rays are characterized by the condition $L_i \cap C = \mathbb{Q}_{\geq 0} \cdot R_i$ for some $R_i \in S$. The element $R_i$ is uniquely determined if we add the condition that $L_i \cap S = \mathbb{N} R_i$. Let $E \in S$. Since the dimension of $S$ is $n - r$, $E$ lies in some simplicial cone spanned by $R_{i_1}, R_{i_2}, \ldots, R_{i_{n-r}}$ for some $1 \leq i_1 < i_2 < \cdots < i_{n-r}$.

By Carathéodory's theorem we may write $E = \alpha_1 R_{i_1} + \alpha_2 R_{i_2} + \cdots + \alpha_{n-r} R_{i_{n-r}}$ where $\alpha_1, \alpha_2, \ldots, \alpha_{n-r} \in \mathbb{Q}_{\geq 0}$.

If $\alpha_{j_i} > 1$ then we may decompose $E$ within $S$ as $E = (E - R_{j_i}) + R_{j_i}$. Multiplicatively this corresponds to decomposing the monomial $X^E = X^{E - R_{j_i}} X^{R_{j_i}}$. Hence if $X^E$ is a generator of $\mathbb{F}[V]^T$ then each $\alpha_i \leq 1$. But then

$$\begin{aligned}\deg X^E = \alpha_1 \deg R_{j_1} + \cdots + \alpha_{n-r} \deg R_{j_{n-r}} &\leq \deg R_{j_1} + \cdots + \deg R_{j_{n-r}} \\ &\leq (n - r) \max\{\deg R_i \mid 1 \leq i \leq s\}.\end{aligned}$$

Hence we have reduced to bounding the degrees of the $R_i$. Reordering the variables if necessary, we may assume that $R_i = (\gamma_1, \gamma_2, \ldots, \gamma_d, 0, 0, \ldots, 0)$ where each $\gamma_j$ is a positive integer. The fact that $R_i$ lies in the extremal ray $L_i$ of $S$ implies that the $d$ weights $\omega_1, \omega_2, \ldots, \omega_d$ span a $(d-1)$-dimensional subspace of $\mathbb{Q}^{n-r}$.

The system of $r$ linear equations in the $n$ unknowns $y_1, y_2, \ldots, y_n$:

$$y_1\omega_1 + \cdots + y_d\omega_d = 0 = y_{d+1} = y_{d+2} = \cdots = y_n$$

has a one-dimensional solution space.

Using Cramer's rule to solve this system we get an integer solution $E = (e_1, e_2, \ldots, e_d, 0, 0, \ldots, 0)$, where

$$\begin{aligned} e_i &= (-1)^i \det(\omega_1, \omega_2, \ldots, \omega_{i-1}, \omega_{i+1}, \omega_{i+2}, \ldots, \omega_d) \\ &= \pm r! \text{ Volume of Convex Hull } (\omega_1, \omega_2, \ldots, \omega_{i-1}, \mathbf{0}, \omega_{i+1}, \omega_{i+2}, \ldots, \omega_d) \end{aligned}$$

for $i = 1, 2, \ldots, d$.

Now $R_i$ is a integer multiple of the solution $E$ and thus all the non-zero entries $e_j$ of $E$ share the same signum which (after multiplying $E$ by $-1$ if necessary) we may assume is positive. Therefore

$$\begin{aligned} \deg(R_i) &= e_1 + e_2 + \cdots + e_d \\ &= r! \sum_{i=1}^{d} \text{Volume of Convex Hull } (\omega_1, \omega_2, \ldots, \omega_{i-1}, \mathbf{0}, \omega_{i+1}, \omega_{i+2}, \ldots, \omega_d) \\ &= r! \text{ Volume of Convex Hull } (\omega_1, \omega_2, \ldots, \omega_d) \\ &\leq r! \text{ Volume of Convex Hull } (\omega_1, \omega_2, \ldots, \omega_n). \end{aligned}$$

The final assertion of the theorem may be proved by bounding the volume of the convex hull of the $\omega_i$ in terms of their coordinates $\omega_{ij}$. ■

Remark 7.3. If $\dim V \geq \operatorname{rank} T + 2$ then the above bound may be improved to $\beta(T, V) \leq (n - r - 1)r! \operatorname{Vol}(\mathcal{W})$ [50].

The author has conjectured [52] that:

Conjecture 7.4. $\beta(T, V) \leq r! \operatorname{Vol}(\mathcal{W})$.

The author also proved [50] the following bound which is independent of $\dim V$.

Theorem 7.5. *Let $T$ be an $r$-dimensional torus acting diagonally on $V$. Then $\beta(T, V) \leq (2w)^{2^{r-1}}$.*

This is proved by induction on $r$ using $T \cong (\mathbb{F}^\times)^{r-1} \times \mathbb{F}^\times$.

## 8. **Derksen's bounds.**

In 2001, Derksen [6] gave new dramatically better upper bounds on $\beta(G,V)$ in terms of the number $\sigma(G,V)$ (which we remind the reader was defined in Section 6.1). By working with a larger set of invariants which cut out the nullcone, rather than a homogeneous system of parameters, Derksen proved the following.

Theorem 8.1. *Let $G$ be a reductive group defined over an algebraically closed field $\mathbb{F}$ of characteristic zero. Then*

$$\beta(G,V) \leq \max\Big\{2, \frac{3}{8} s\sigma^2(G,V)\Big\}$$

*where $s = \dim \mathbb{F}[V]^G \leq \dim V$.*

In the same paper Derksen also gave a good new upper bound on $\sigma(G,V)$ as follows. Since $G$ is a linear algebraic group it is given as the set of common zeroes of some finite collection of polynomials $h_1, h_2, \ldots, h_\ell \in \mathbb{F}[y_1, y_2, \ldots, y_c]$ for some $c \in \mathbb{N}$. The fact that the $n$-dimensional representation $\rho\colon G \to \mathrm{GL}(V)$ is rational means that there exist polynomials $a_{i,j} \in \mathbb{F}[y_1, y_2, \ldots, y_c]$ for $1 \leq i, j \leq n$ such that $\rho(g)$ is given by

$$\rho(g) = \begin{pmatrix} a_{1,1}(g) & a_{1,2}(g) & \ldots & a_{1,n}(g) \\ a_{2,1}(g) & a_{2,2}(g) & \ldots & a_{2,n}(g) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1}(g) & a_{n,2}(g) & \ldots & a_{n,n}(g) \end{pmatrix}.$$

Derksen showed the following.

Theorem 8.2. *Let $G$ be a reductive group defined over an algebraically closed field $\mathbb{F}$ of characteristic zero. Then*

$$\sigma(G,V) \leq H^{c-m} A^m$$

*where $H = \max\{\deg(h_1), \deg(h_2), \ldots, \deg(h_\ell)\}$, $A = \max\{\deg(a_{i,j}) \mid 1 \leq i, j \leq n\}$, $m = \dim G$ and $c$ is the number of variables needed to define the $h_i$ as in the preceding paragraph.*

Remark 8.3. It is important to note that by combining the above two results Derksen gave a bound on $\beta(G,V)$ which grows *polynomially* with respect to the various parameters.

*Acknowledgements.* I thank Gregor Kemper and the anonymous referee and especially John Harris for reading earlier drafts of this article and making many useful suggestions, corrections and remarks.

## References

**1**. Abraham Broer, *Remarks on invariant theory of finite groups.* Preprint, Université de Montréal, Montréal, 1997.

**2**. Roger M. Bryant and Gregor Kemper, *Global degree bounds and the transfer principle for invariants.* J. Algebra **284** (2005), 80–90.

**3**. H. E. A. Campbell, A. V. Geramita, I. P. Hughes, R. J. Shank and D. L. Wehlau, *Non-Cohen–Macaulay vector invariants and a Noether bound for a Gorenstein ring of invariants.* Canad. Math. Bull. **42** (1999), 155–161.

**4**. Jianjun Chuai, *A new degree bound for invariant rings.* Proc. Amer. Math. Soc. **133** (2005), 1325–1333 (electronic).

**5**. Harm Derksen, *Computation of invariants for reductive groups.* Adv. Math. **141** (1999), 366–384.

**6**. ———, *Polynomial bounds for rings of invariants.* Proc. Amer. Math. Soc. **129** (2001), 955–963 (electronic).

**7**. Harm Derksen and Gregor Kemper, *Computational invariant theory.* In: Invariant Theory and Algebraic Transformation Groups, I. Encyclopaedia of Mathematical Sciences **130**, Springer-Verlag, Berlin, 2002.

**8**. ———, *On global degree bounds for invariants.* In: Invariant theory in all characteristics, CRM Proc. Lecture Notes **35**, Amer. Math. Soc., Providence, RI, 2004, 37–41.

**9**. Harm Derksen and Hanspeter Kraft, *Constructive invariant theory.* In: Algèbre non commutative, groupes quantiques et invariants (Reims, 1995), Sémin. Congr. **2**, Soc. Math. France, Paris, 1997, 221–244.

**10**. M. Domokos and P. Hegedüs, *Noether's bound for polynomial invariants of finite groups.* Arch. Math. (Basel) **74** (2000), 161–167.

**11**. P. Fleischmann, *A new degree bound for vector invariants of symmetric groups.* Trans. Amer. Math. Soc. **350** (1998), 1703–1712.

**12**. ———, *The Noether bound in invariant theory of finite groups.* Adv. Math. **156** (2000), 23–32.

**13**. ———, *On invariant theory of finite groups.* In: Invariant theory in all characteristics, CRM Proc. Lecture Notes **35**, Amer. Math. Soc., Providence, RI, 2004, 43–69.

**14**. Peter Fleischmann and Wolfgang Lempken, *On degree bounds for invariant rings of finite groups over finite fields.* In: Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997), Contemp.Math. **225**, Amer. Math. Soc., Providence, RI, 1999, 33–41.

**15**. P. Fleischmann, M. Sezer, R. J. Shank and C. F. Woodcock, *The Noether numbers for cyclic groups of prime order.* arXiv:math.AC/0508075, IMS Technical Report UKC/IMS/05/10, August 2005, 6 pages.

**16**. John Fogarty, *On Noether's bound for polynomial invariants of a finite group.* Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 5–7 (electronic).

**17**. G. Freudenburg, *A survey of counterexamples to Hilbert's fourteenth problem.* Serdica Math. J. **27** (2001), 171–192.

**18**. Manfred Göbel, *Computing bases for rings of permutation-invariant polynomials.* J. Symbolic Comput. **19** (1995), 285–291.

**19**. Grete Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.* (German) Math. Ann. **95** (1926), 736–788.

**20**. David Hilbert, *Ueber die Theorie der algebraischen Formen.* (German) Math. Ann. **36** (1890), 473–534.

**21**. ———, *Ueber die vollen Invariantensysteme.* (German) Math. Ann. **42** (1893), 313–373.

**22**. Karin Hiss, *I. Constructive Invariant Theory for Reductive Algebraic Groups II. Degree of Orbits and Linear Slices.* Ph.D. thesis, Brandeis University, Feb. 1997.

**23**. Melvin Hochster and Joel L. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen–Macaulay.* Advances in Math. **13** (1974), 115–175.

**24**. James E. Humphreys, *Linear algebraic groups.* Graduate Texts in Math. **21**, Springer-Verlag, New York–Heidelberg, 1975.

**25**. Camille Jordan, *Mémoire sur les covariants des formes binaires.* J. Math. **2** (1876), 177–232.

**26**. ______, *Sur les covariants des formes binaires.* J. Math. **5** (1879), 345–378.

**27**. D. B. Karagueuzian and P. Symonds, *The module structure of a group action on a polynomial ring: examples, generalizations, and applications.* In: Invariant theory in all characteristics, CRM Proc. Lecture Notes **35**, Amer. Math. Soc., Providence, RI, 2004, 139–158.

**28**. ______, *The module structure of a group action on a polynomial ring: a finiteness theorem.* Preprint, www.ma.umist.ac.uk/pas/preprints/.

**29**. G. Kemper, *Lower degree bounds for modular invariants and a question of I. Hughes.* Transform. Groups **3** (1998), 135–144.

**30**. ______, *Hilbert series and degree bounds in invariant theory.* In: Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, 249–263.

**31**. George Kempf, *The Hochster–Roberts theorem of invariant theory.* Michigan Math. J. **26** (1979), 19–32.

**32**. ______, *Algebraic representations of reductive groups.* In: Proceedings of the International Congress of Mathematicians (Helsinki, 1978), Acad. Sci. Fennica, Helsinki, 1980, 575–577.

**33**. ______, *Computing invariants.* In: Invariant theory, Lecture Notes in Math. **1278**, Springer, Berlin, 1987, 81–94.

**34**. Friedrich Knop, *Der kanonische Modul eines Invariantenrings.* (German) [The canonical module of a ring of invariants] J. Algebra **127** (1989), 40–54.

**35**. ______, *On Noether's and Weyl's bound in positive characteristic.* In: Invariant theory in all characteristics, CRM Proc. Lecture Notes **35**, Amer. Math. Soc., Providence, RI, 2004, 175–188.

**36**. Masayoshi Nagata, *On the 14th problem of Hilbert.* Amer. J. Math. **81** (1959), 766–772.

**37**. E. Noether, *Der Endlichkeitssatz der invarianten endlicher Gruppen.* Math. Ann. **77** (1915), 89–92; reprinted in: Collected Papers, Springer-Verlag, Berlin, 1983, 181–184.

**38**. E. Noether, *Der endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p.* Nachr. v. d. Ges. Wiss. zu Göttingen, 1926, 485–491.

**39**. Vivek Pawale, *Invariants of semi-direct products of cyclic groups.* Ph.D. thesis, Brandeis University, 1999.

**40**. V. L. Popov, *Constructive invariant theory.* In: Young tableaux and Schur functors in algebra and geometry (Toruń, 1980), Astérisque **87–88**, Soc. Math. France, Paris, 1981, 303–334.

**41**. David R. Richman, *On vector invariants over finite fields.* Adv. Math. **81** (1990), 30–65.

**42**. ______, *Invariants of finite groups over fields of characteristic p.* Adv. Math. **124** (1996), 25–48.

**43**. ______, *Explicit generators of the invariants of finite groups.* Adv. Math. **124** (1996), 49–76.

**44**. Barbara J. Schmid, *Finite groups and invariant theory.* In: Topics in invariant theory (Paris, 1989/1990), Lecture Notes in Math. **1478**, Springer, Berlin, 1991, 35–66.

**45**. Müfit Sezer, *Sharpening the generalized Noether bound in the invariant theory of finite groups.* J. Algebra **254** (2002), 252–263.

**46**. R. James Shank, private communication, June 2001.

**47**. R. James Shank and David L. Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order.* Bull. London Math. Soc. **34** (2002), 438–450.

**48**. T. A. Springer, *Linear algebraic groups.* (2nd edition) Progress in Mathematics **9**, Birkhäuser Boston, Inc., Boston, MA, 1998.

**49**. Richard P. Stanley, *Invariants of finite groups and their applications to combinatorics.* Bull. Amer. Math. Soc. (N.S.) **1** (1979), 475–511.

**50**. David L. Wehlau, *Constructive invariant theory for tori.* Ann. Inst. Fourier (Grenoble) **43** (1993), 1055–1066.

**51**. ______, *Constructive invariant theory.* In: Algebraic groups and their generalizations: classical methods (University Park, PA, 1991), Proc. Sympos. Pure Math. **56**, Part 1, Amer. Math. Soc., Providence, RI, 1994, 377–383.

**52**. ———, *Degree bounds in invariant theory.* Queen's Invariant Theory Seminar (unpublished), February 1995.

**53**. Hermann Weyl, *The classical groups. Their invariants and representations.* (Fifteenth printing) Princeton Landmarks in Mathematics, Princeton Paperbacks, Princeton University Press, Princeton, NJ, 1997.

**54**. Jerzy Weyman, *Gordan ideals in the theory of binary forms.* J. Algebra **161** (1993), 370–391.

*Department of Mathematics & Computer Science*
*Royal Military College*
*Kingston, Ontario*
*K7K 7B4*
*email: wehlau@rmc.ca*