

Degree Bounds **– An Invitation to Postmodern Invariant Theory–**

Mara D. Neusel

DEPARTMENT OF MATHEMATICS AND STATISTICS
MAILSTOP 4-1042
TEXAS TECH UNIVERSITY
LUBBOCK, TX 79409
USA

EMAIL: MARA.D.NEUSEL@TTU.EDU

IN MEMORY OF C. AND C.

AMS CODE: 13A50 Invariant Theory, 55XX Algebraic Topology, 20XX Group Theory and Generalizations

KEYWORDS: Invariant Theory of Finite Groups, Degree Bounds, Weyl Groups, Group Cohomology

TYPESET BY *L*^ST_EX

SUMMARY : *This is an invitation to invariant theory of finite groups; a field where methods and results from a wide range of mathematics merge to form a new exciting blend. We use the particular problem of finding degree bounds to illustrate this.*

Invariant theory is a relatively young field. Although we will give explicit definitions later, a brief discussion on its short but illustrious history can give insight into this area of mathematics:

In 1773, J. L. Lagrange observed that the determinant of a binary quadratic form is an invariant polynomial under any linear transformation.

Around 1800, Carl F. Gauss considered the general problem of the invariance of binary quadratic forms with integral coefficients under an action of the special linear group. However, it was George Boole who, in 1843, laid the foundations of invariant theory with his papers [6] and [7]. In the second half of the 19th century, invariant theory blossomed under the hands of people like Sir Arthur Cayley in England and James J. Sylvester in England and the US, Felix Klein in Germany, and many others. Indeed, the history of invariant theory in the 19th century is exciting and rich, and we recommend the survey articles by W. Franz Meyer [38] and [39], and of course the lovely lectures by Felix Klein ([34]).

A culmination point of this early phase was Paul Gordan's proof that the invariant binary forms (under an action of the special linear group $SL(2, \mathbb{C})$) are finitely generated (see [25]). However, the early history of invariant theory ended abruptly with David Hilbert's proof of the finite generatedness of the $SL(n, \mathbb{C})$ -invariants using, or better creating, completely new tools and paradigms (see [27]). Indeed, David Hilbert's viewpoint was earthshaking and rang in mathematical modernity.¹ However, the school around David Hilbert and later Emmy Noether was just too successful; they solved the current problems of invariant theory of finite groups, leaving behind a seemingly complete, and thus dead branch of mathematics (see [17] and the response [52]).

On the other hand, modular invariant theory over finite fields was a field presenting problems and questions of a completely different type. These were studied by Leonard E. Dickson and his school at Chicago. Impressive as these results are (Leonard E. Dickson's collected works, 6 huge volumes [14], are a treasure box for everybody who works in the area) the tools available back then were soon exhausted, and so no wonder that also his algorithmic approach faded.

However, modernity that had marginalized classical invariant theory at the same time brought new questions and problems to invariant theory. In particular, the entire field of modular invariant theory over finite fields was revitalized by algebraic topology.² Nowadays there are many other connections and overlaps with fields like group cohomology³, representation theory, algebraic combinatorics (see [55] for an idiosyncratic look back), commutative algebra, and number theory.

Also, the electronic revolution of the 20th century and in the course of that the development of powerful computer algebra programs allows to tackle problems that were out of reach for, e.g., Dickson's school. And, of course, vice versa: hard algorithmic problems in invariant theory serve as motivation for the development of such software.

But not only does invariant theory profit from the neighbouring areas; these areas also take advantage of its results. And indeed, invariant-theoretic problems have been discovered in almost every area of mathematics. Moreover, invariant theory is continuously challenged by daily life problems in physics (think of Emmy Noether's milestone paper [49]), coding theory

¹ And, in particular, modern algebra.

² We recover our rings of invariants as rings of invariants of Weyl groups acting on the cohomology ring of elementary abelian p -groups, if we ignore the exterior part in odd characteristic.

³ The ring of invariants is just the zeroth cohomology of the group in question with twisted coefficients in $\mathbb{F}[V]$, see, e.g., [2].

(see the survey article [62] for more information on this), numerical analysis (see, e.g., [69]), engineering (e.g., in the production of rubbermats for the car industry, [37]), and elsewhere (see Chapter 5 of [12] for an overview).

§1. Introduction

Consider a quadratic polynomial

$$p(x, y) = ax^2 + 2bxy + cy^2 \in \mathbb{C}[x, y]$$

in two variables x, y with complex coefficients, i.e., a **binary quadratic form**. If we replace the variables x, y by

$$x' = x + y, \quad \text{and} \quad y' = y,$$

we obtain the polynomial

$$p'(x, y) = p(x + y, y) = a'x^2 + 2b'xy + c'y^2,$$

where

$$a' = a, \quad b' = b + a, \quad \text{and} \quad c' = c + 2b + a.$$

We observe that the coefficients of both polynomials satisfy the following equation

$$ac - b^2 = a'c' - b'^2.$$

This is not an accident. Indeed, let $p(x, y)$ be an arbitrary binary quadratic form, and let \mathbf{T} be a linear transformation given by

$$\mathbf{T} \begin{cases} x \mapsto x + \lambda y, & \lambda \in \mathbb{C} \\ y \mapsto y. \end{cases}$$

Then the **determinant** of p , $\det(p) = ac - b^2$, remains unchanged under the \mathbf{T} -action:

$$\det(p) = \det(p'),$$

where $p'(x, y) = p(x + \lambda y, y)$. This observation was made by Joseph Louis Lagrange in 1773 (see Corollaire II in [36]).

Let us rephrase this result in order to put it into a broader context.

A polynomial $p(x, y) = ax^2 + 2bxy + cy^2$ is determined by the three coefficients a, b, c . We arrange them in a symmetric 2×2 matrix

$$\mathbf{M}(p) = \begin{bmatrix} a & b \\ b & c \end{bmatrix}.$$

Then the determinant of the polynomial p is nothing but the determinant of the associated matrix $\mathbf{M}(p)$. The linear transformation \mathbf{T} translates into the following matrix operation

$$\mathbf{M}(p') = \begin{bmatrix} a' & b' \\ b' & c' \end{bmatrix} = \begin{bmatrix} a & a\lambda + b \\ a\lambda + b & a\lambda^2 + 2\lambda b + c \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} a & b \\ b & c \end{bmatrix} \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix},$$

and J. L. Lagrange observed that

$$\det(\mathbf{M}(p)) = \det(\mathbf{M}(p')).$$

If we view the space of binary quadratic forms as a 3-dimensional vector space over \mathbb{C} by assigning to a polynomial $p(x, y) = ax^2 + 2bxy + cy^2$ the column vector

$$(a, b, c)^t \in \mathbb{C}^3,$$

then the change of variables becomes a linear map

$$\mathbf{T}(\lambda) : \mathbb{C}^3 \rightarrow \mathbb{C}^3, (a, b, c)^t \mapsto (a, \lambda a + b, \lambda^2 a + 2\lambda b + c)^t$$

given by the matrix

$$\mathbf{T}(\lambda) = \begin{bmatrix} 1 & \lambda & \lambda^2 \\ 0 & 1 & 2\lambda \\ 0 & 0 & 1 \end{bmatrix}.$$

It is not hard to check that the family of maps $\mathbf{T}(\lambda)$, where $\lambda \in \mathbb{C}$, forms a group G under matrix multiplication. Indeed, we have an isomorphism into the additive group of complex numbers given by

$$G \rightarrow \mathbb{C}, \mathbf{T}(\lambda) \mapsto \lambda.$$

Hence, we have a subgroup $G \subset \text{GL}(3, \mathbb{C})$ (abstractly isomorphic to \mathbb{C}) of the general linear group $\text{GL}(3, \mathbb{C})$ of invertible 3×3 -matrices acting via matrix multiplication on the 3-dimensional vector space of all binary quadratic forms. Next, we consider polynomials in these coefficients, and we end up with the result that the determinant (which is a polynomial of degree 2 in the coefficients) is *invariant* under the action of G .

Let us formalize this.

Let \mathbb{F} be any field, G a group and

$$\rho : G \rightarrow \text{GL}(n, \mathbb{F})$$

a linear representation of G of degree n over \mathbb{F} . The group G acts via ρ on the n -dimensional vector space $V = \mathbb{F}^n$ by

$$g \cdot v = \rho(g)v \quad \forall g \in G, v \in V.$$

Since only the image $\rho(G) \subset \text{GL}(n, \mathbb{F})$ of G in $\text{GL}(n, \mathbb{F})$ matters for our purposes, we might as well assume that ρ is faithful. This action induces an action of G on the ring

$$\mathbb{F}[V] = \mathbb{F}[x_1, \dots, x_n]$$

of polynomials in n variables, where $x_1, \dots, x_n \in V^*$ is the standard dual basis, by⁴

$$gf(v) = f(\rho(g)^{-1}v) \quad \forall g \in G, v \in V, f \in \mathbb{F}[V].$$

The subset

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

of polynomials invariant under this action forms a ring, the **ring of polynomial invariants of G** .⁵

In this survey we are concerned with *finite* groups G and their rings of invariants $\mathbb{F}[V]^G$. We refer to the monographs [3], [12], [47], [51], and [63], and to the survey articles [18], [64] and [68] for detailed expositions from various different view points and more references.

Let us look at an explicit example taken from page 273 in [18].

EXAMPLE 1.1 : Let k be a natural number. Consider the full symmetry group D_{2k} of a regular polygon with k vertices in the plane. It is generated by the two matrices⁶

$$\mathbf{D} = \begin{bmatrix} \cos(\frac{2\pi}{k}) & -\sin(\frac{2\pi}{k}) \\ \sin(\frac{2\pi}{k}) & \cos(\frac{2\pi}{k}) \end{bmatrix} \quad \text{and} \quad \mathbf{S} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

⁴The inverse $(\cdot)^{-1}$ is introduced in order to obtain a left action.

⁵More precisely we should write $\mathbb{F}[V]^{\rho(G)}$ for this ring, since it is the image in $\text{GL}(n, \mathbb{F})$ that matters. However, this notation is a bit clumsy, and usually we know which representation we are talking about. So, we stick to the first (imprecise) notation.

⁶The \mathbf{D} stands for *Drehung* (rotation) and the \mathbf{S} for *Spiegelung* (reflection).

In other words, the representation

$$\rho : D_{2k} \hookrightarrow \mathrm{GL}(2, \mathbb{R})$$

afforded by the matrices \mathbf{D} and \mathbf{S} defines the dihedral group D_{2k} of order $2k$.⁷ Its ring of invariants is a polynomial ring

$$\mathbb{R}[x, y]^{D_{2k}} = \mathbb{R} \left[x^2 + y^2, \prod_{j=0}^{k-1} \left(\cos\left(\frac{2\pi j}{k}\right)x + \sin\left(\frac{2\pi j}{k}\right)y \right) \right].$$

It is not hard to check that the given polynomials are indeed invariant under the D_{2k} -action. However, that these two form a complete set of generators needs an argument. We will address this a bit later. For now, let us have a look at another classical result.

If we choose our ground field \mathbb{F} to be finite of order q , then the full general linear group $\mathrm{GL}(n, \mathbb{F})$ is a finite group of order

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

The ring of invariants of $\mathrm{GL}(n, \mathbb{F})$ acting by its tautological representation was calculated by Leonard E. Dickson in [13].

EXAMPLE 1.2 (Leonard E. Dickson [13]): Consider the tautological representation of the general linear group $\mathrm{GL}(n, \mathbb{F}_q)$ over a finite field of size q and characteristic p . Its ring of invariants

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

called the **Dickson algebra**, is a polynomial ring in n generators $\mathbf{d}_{n,i}$, $i = 0, \dots, n-1$, of degree $q^n - q^i$. The generators are explicitly given by the following formula⁸

$$\mathbf{d}_{n,i} = \sum_{\substack{W^* < V^* \\ \dim(W^*)=i}} (-1)^{n-i} \prod_{v \notin W^*} v,$$

where the sum runs over all vector subspaces $W^* < V^*$ of V^* . Another way of describing them would be the following: The group $\mathrm{GL}(n, \mathbb{F}_q)$ acts transitively on the nonzero elements in V^* , i.e., this action consists of two orbits, namely $\{0\}$ and $V^* \setminus \{0\}$. Note that these are finite sets since the ground field \mathbb{F} is finite. So, we can form the elementary symmetric polynomials in the nonzero elements of the vector space V^* . They are by construction invariant under the group action, and are the only nonzero so-called **orbit Chern classes**, see, e.g., Section 4.1 of [47] for an introduction to orbit Chern classes. We will see later more of those.

From the purely ring-theoretic point of view, $\mathbb{F}[V]^G$ is an extremely well-behaved ring. By construction it is a commutative, nonnegatively graded, connected⁹ \mathbb{F} -algebra without zero

⁷ Let G be a finite group generated by g_1, \dots, g_d . We say that a representation

$$\rho : G \rightarrow \mathrm{GL}(n, \mathbb{F})$$

is **afforded** by the matrices $\mathbf{M}_1, \dots, \mathbf{M}_d$ if

$$\rho(g_i) = \mathbf{M}_i \quad \forall i = 1, \dots, d.$$

For an arbitrary element $g \in G$ we then have

$$\rho(g) = \rho(g_{i_1} \cdots g_{i_k}) = \rho(g_{i_1}) \cdots \rho(g_{i_k}) = \mathbf{M}_{i_1} \cdots \mathbf{M}_{i_k},$$

where $g = g_{i_1} \cdots g_{i_k}$ is a product in the group generators.

⁸ According to David J. Benson this formulae was obtained by Ian Macdonald sometime in the 70s but never published ([4] and Proposition 8.1.3 in [3]). According to Larry Smith the formula was independently obtained by Robert E. Stong in the 80s and by Tsuneo Tamagawa in 1991 (see the comments before Theorem 8.1.6 in [63]). These two never published the result either.

⁹ **Connected** means that the ring coincides with the ground field \mathbb{F} in degree zero.

divisors. Furthermore, we have a classical finiteness result due to Emmy Noether (see [48], [50]).

THEOREM 1.3 (Emmy Noether [48], [50]): *The ring of polynomial invariants $\mathbb{F}[V]^G$ is finitely generated as an algebra over \mathbb{F} , and $\mathbb{F}[V]$ is finitely generated as a module over $\mathbb{F}[V]^G$.*

PROOF: Let $f \in \mathbb{F}[V]$ be a polynomial. We define the monic polynomial

$$\Phi_f(t) = \prod_{g \in G} (t - gf) \in \mathbb{F}[V]^G[t]$$

in an additional variable t with coefficients¹⁰ in $\mathbb{F}[V]^G$. Since the polynomial $\Phi_f(t)$ has root f , the ring extension

$$\mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]$$

is integral. Let $H \subseteq \mathbb{F}[V]$ be the subalgebra generated by the coefficients of

$$\Phi_{x_i}(t) \quad \forall i = 1, \dots, n.$$

Then H is a finitely generated \mathbb{F} -algebra, and $\mathbb{F}[V]$ is a finitely generated module over H . Observe that

$$H \hookrightarrow \mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V].$$

Since H is Noetherian, the H -submodule $\mathbb{F}[V]^G$ of $\mathbb{F}[V]$ is also finitely generated. Therefore, $\mathbb{F}[V]^G$ is finitely generated as an \mathbb{F} -algebra by the algebra generators of H and the H -module generators of $\mathbb{F}[V]^G$. \bullet

Emmy Noether's result tells us that only finitely many invariants generate the entire ring. *How many are there? How do we find them?*

EXAMPLE 1.4 : Recall the defining representation of the dihedral group D_{2k} of order $2k$ from above. If we allow coefficients to be taken from the field \mathbb{C} of complex numbers, then we can diagonalize the rotation matrix, and we obtain the matrices

$$\mathbf{D}' = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} \quad \text{and} \quad \mathbf{S}' = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

where $\lambda = \exp(\frac{2\pi i}{k})$ is a k th root of unity. It is much easier to read off the invariants from this representation.¹¹ Indeed, we have

$$\mathbb{C}[x, y]^{D_{2k}} = \mathbb{C}[xy, x^k + y^k].$$

¹⁰ Note that the coefficients are the elementary symmetric functions in the orbit elements of the orbit $\{gf \mid g \in G\}$ of the polynomial $f \in \mathbb{F}[V]$.

¹¹ Yes, here is something to prove. We have

$$\mathbf{D}' = \begin{bmatrix} 1 & 1 \\ -\mathbf{i} & \mathbf{i} \end{bmatrix}^{-1} \mathbf{D} \begin{bmatrix} 1 & 1 \\ -\mathbf{i} & \mathbf{i} \end{bmatrix} \quad \text{and} \quad \mathbf{S}' = \begin{bmatrix} 1 & 1 \\ -\mathbf{i} & \mathbf{i} \end{bmatrix}^{-1} \mathbf{S} \begin{bmatrix} 1 & 1 \\ -\mathbf{i} & \mathbf{i} \end{bmatrix}.$$

Since these two matrices generate the group, we obtain the representation, say $\rho_{\mathbb{C}}$, over \mathbb{C} by conjugation from the representation $\rho_{\mathbb{R}}$ over \mathbb{R}

$$\rho_{\mathbb{C}}(D_{2k}) = \begin{bmatrix} 1 & 1 \\ -\mathbf{i} & \mathbf{i} \end{bmatrix}^{-1} \rho_{\mathbb{R}}(D_{2k}) \begin{bmatrix} 1 & 1 \\ -\mathbf{i} & \mathbf{i} \end{bmatrix}.$$

We rewrite this as

$$\begin{bmatrix} 1 & 1 \\ -\mathbf{i} & \mathbf{i} \end{bmatrix} \rho_{\mathbb{C}}(D_{2k}) = \rho_{\mathbb{R}}(D_{2k}) \begin{bmatrix} 1 & 1 \\ -\mathbf{i} & \mathbf{i} \end{bmatrix}$$

and observe that for any vector v invariant under $\rho_{\mathbb{C}}(D_{2k})$ we obtain the $\rho_{\mathbb{R}}(D_{2k})$ -invariant vector $\begin{bmatrix} 1 & 1 \\ -\mathbf{i} & \mathbf{i} \end{bmatrix} v$. This leads (after some calculations) to the fact that conjugate representations have isomorphic rings of invariants.

Note that the degrees of the generators have not changed, because the two representations are conjugate. We are, however, stuck with the same problem as above. *Why do the given two invariants form a complete set of generators?* Well, we could argue as follows: A polynomial $f(x, y) \in \mathbb{C}[x, y]$ is invariant under D_{2k} if and only if each of its homogeneous parts is invariant, because the group action does not change the degree of a polynomial. Furthermore,

$$f(x, y) = a_d x^d + a_{d-1} x^{d-1} y + \cdots + a_1 x y^{d-1} + a_0 y^d$$

is invariant if and only if it is invariant under \mathbf{D}' and \mathbf{S}' , because these two elements generate the group. Since the matrix \mathbf{S}' interchanges the variables x and y , an invariant polynomial f must be symmetric, i.e., $a_i = a_{d-i}$. Next we observe that

$$\mathbf{D}'(f(x, y)) = \lambda^{-d} a_d x^d + \lambda^{-d+2} a_{d-1} x^{d-1} y + \cdots + \lambda^{d-2} a_{d-1} x y^{d-1} + \lambda^d a_d y^d.$$

Since λ is a primitive k th root of unity, we have that

$$\lambda^m = 1 \quad \text{if and only if } k \mid m.$$

From this we can derive the above result with just a bit more calculations.

Over the last 150 years, invariant theorists have developed quite a number of tools for constructing invariants, some of which we will encounter in this article. However, the question raised above *Does a given set of invariants form a complete set of generators?* has no practical solution in general. In the above example of the defining representation of the dihedral group D_{2k} we were able to construct the ring of invariants by hand just because the representation is small, the group is small, and comes with a nice geometry. There exist methods to show completeness in special cases, one of them we could apply to this example: Our test ring $\mathbb{C}[xy, x^k + y^k]$ is a polynomial ring. Moreover, $\mathbb{C}[xy, x^k + y^k] \hookrightarrow \mathbb{C}[x, y]^{D_{2k}}$ is a finite ring extension and the product of the degrees is equal to the group order. This allows us to conclude that the two invariants form a complete set of generators (Proposition 4.5.5 in [47]). This chain of reasoning is always applicable when the ring of invariants turns out to be a polynomial ring. There are a few other argumentation schemes that allow us to check whether a given test ring is the desired ring of invariants. However, all of these methods apply either only to special cases like the case of a polynomial ring as above, or are just reformulations of the very same problem in a different language, or are tricky ad hoc methods.¹² To make things worse all of these methods require a test ring. How do we get this? And even if some angel hands us a test ring, what is if this ring fails to be the ring of invariants desired? How do we proceed then?

Note that we have graded rings. This means that we could check degreewise all polynomials on invariance. This is an algorithm that must lead to a complete set of generators by Emmy Noether's finiteness theorem above. So, we start with degree one and check all linear polynomials for invariance; then we proceed with degree two and find all invariant quadratic polynomials; then we look at degree three, then four, then ... But where to end? It seems that we have an algorithm but no stopping condition. Or?

¹² Polynomial rings are indeed rings of invariants of a very special type of representations. The famous Shephard–Todd classification shows that the ring of invariants is polynomial precisely when the group is generated by pseudoreflections (i.e., elements of finite order fixing a subspace $U < V$ of codimension 1), if we are in characteristic zero or prime to the group order! (See Section 7.1 in [47] for more information on this.) Moreover, there is a (slightly more complicated) general procedure to show completeness in the next worse case, when the ring of invariants turns out to be a factorial complete intersection. This is used in the proof of the structure of the invariant ring of the finite symplectic groups (see [10], [42], or Section 8.3 in [3]) and in [41].

§2. The Nonmodular Case I: Noether's Bound

Emmy Noether gave more than one proof for her finiteness result. Among those we find in [48] one that is *constructive*. In other words, she more or less explicitly writes down a generating set. From that we can read off an upper bound¹³ on the maximal degree of a generator in a minimal generating set. So, we obtain the desired stopping condition for our algorithm. Indeed, degree bounds provide us with one of the main tools that allow us to make statements about completeness of sets of generators.

We introduce the following notation.

NOTATION: Let H be a finitely generated graded commutative connected \mathbb{F} -algebra. A set of homogeneous elements $\{h_1, \dots, h_k\} \subset H$ is called a **minimal generating set** if the elements h_1, \dots, h_k generate H as an algebra over \mathbb{F} and if none of them can be omitted. Note that this is, of course, again a graded set. We write

$$\beta(H) = \max\{\deg(h_i) \mid i = 1, \dots, k\}$$

for the maximal degree of an algebra generator in a minimal generating set.¹⁴ For rings of invariants we sometimes write $\beta(\rho)$ instead of $\beta(\mathbb{F}[V]^G)$, if we want to emphasize the representation. We write

$$\beta_{\mathbb{F}}(G) = \max\{\beta(\rho) \mid \rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})\}$$

if there is an upper bound depending only on the group and the field.

Let the ground field be the complex numbers \mathbb{C} . Denote by $|G| = d$ the order of the group G and enumerate the group elements in any order, say g_1, \dots, g_d . Let

$$X = \{x_{ij} \mid i = 1, \dots, d, j = 1, \dots, n\}.$$

be a set of formal variables of degree one. Then form the polynomial \mathbb{C} -algebra $\mathbb{C}[X]$ on the set X . The group G acts on $\mathbb{C}[X]$ by permutation

$$g x_{ij} = x_{i'j},$$

where $g g_i = g_{i'}$. Then define a map

$$\eta_G : \mathbb{C}[X] \rightarrow \mathbb{C}[V], x_{ij} \mapsto g_i x_j.$$

By construction this map commutes with the G -action. Moreover, it is a surjective algebra homomorphism. Hence, it induces a map between the respective rings of invariants, the so-called **Noether map**

$$\eta_G^G : \mathbb{C}[X]^G \rightarrow \mathbb{C}[V]^G.$$

The Noether map η_G^G is surjective as we see next. This follows from the fact that the **averaging operator**

$$\pi^G : \mathbb{C}[V] \rightarrow \mathbb{C}[V]^G, f \mapsto \frac{1}{|G|} \sum_{g \in G} g f.$$

splits the canonical inclusion

$$i : \mathbb{C}[V]^G \hookrightarrow \mathbb{C}[V].$$

We obtain the commutative diagram with surjective horizontal maps

¹³ Since her generating set is not *minimal*, we obtain only upper bounds.

¹⁴ That $\beta(H)$ is independent of the choice of the minimal generating set, is something that you have to prove.

$$\begin{array}{ccc} \mathbb{C}[X] & \xrightarrow{\pi^G} & \mathbb{C}[X]^G \\ \downarrow \eta_G & & \downarrow \eta_G^G \\ \mathbb{C}[V] & \xrightarrow{\pi^G} & \mathbb{C}[V]^G \end{array}$$

and surjective η_G . Therefore, the Noether map η_G^G is surjective. This means that if we have a degree bound for the generators of the invariants $\mathbb{C}[X]^G$, then we also have one for the generators of $\mathbb{C}[V]^G$, because by construction

$$\beta(\mathbb{C}[X]^G) \geq \beta(\mathbb{C}[V]^G).$$

Recall that G acts via permutation on X . Indeed, it acts by simultaneous permutation of the rows if we write out the variables x_{ij} as a matrix (x_{ij}) . Therefore, it is contained in Σ_d , the symmetric group on d letters that permutes simultaneously the rows of the matrix (x_{ij}) . We obtain integral extensions

$$\mathbb{C}[X]^{\Sigma_d} \subset \mathbb{C}[X]^G \subset \mathbb{C}[X].$$

The same reasoning as above shows that there exists a splitting

$$\pi^{\Sigma_d} : \mathbb{C}[X]^G \rightarrow \mathbb{C}[X]^{\Sigma_d}.$$

Hence, we can enlarge our diagram above and get the following with split inclusions

$$\begin{array}{ccccc} \mathbb{C}[X]^{\Sigma_d} & \hookrightarrow & \mathbb{C}[X]^G & \hookrightarrow & \mathbb{C}[X] \\ & & \downarrow \eta_G^G & & \downarrow \eta_G \\ & & \mathbb{C}[V]^G & \hookrightarrow & \mathbb{C}[V]. \end{array}$$

The restriction

$$\eta_G^G| : \mathbb{C}[X]^{\Sigma_d} \rightarrow \mathbb{C}[V]^G$$

remains surjective, because we have obtained a map

$$E : \mathbb{C}[V] \rightarrow \mathbb{C}[X]^{\Sigma_d}, \quad x_j \mapsto \sum_{i=1}^d x_{ij} \forall j,$$

such that $\pi^G = \frac{1}{d} \eta_G^G| \circ E$. Since π^G is surjective, so is $\eta_G^G|$. This means that if f_1, \dots, f_k generate $\mathbb{C}[X]^{\Sigma_d}$ as a \mathbb{C} -algebra, then

$$\eta_G^G|(f_1), \dots, \eta_G^G|(f_k)$$

generate $\mathbb{C}[V]^G$ as an algebra. We derive that

$$\beta(\mathbb{C}[X]^{\Sigma_d}) \geq \beta(\mathbb{C}[V]^G).$$

So, we have reduced the problem to finding the invariants of the symmetric group acting on X by simultaneously permuting the rows of the matrix (x_{ij}) . To quote the original: *Nach dem bekannten Satz über die symmetrischen Funktionen von Größenreihen ist also $f(x)$ ganz und rational durch die symmetrischen Elementarfunktionen dieser Reihen darstellbar, d.h. durch die Koeffizienten ... der ‚Galoisschen Resolvente‘* (see p. 89 in [48]). This means that $\mathbb{C}[X]^{\Sigma_d}$ is generated by polarized symmetric functions. They are the following.

Let $I = (i_1, \dots, i_n) \in \mathbb{N}_0 \times \dots \times \mathbb{N}_0$ be a multi-index¹⁵ such that $|I| = i_1 + \dots + i_n \leq d$. Then choose i_j different elements $r(j)_1, \dots, r(j)_{i_j}$ from the j th row $\{x_{1j}, \dots, x_{dj}\}$ for $j = 1, \dots, n$. We consider the product

$$\prod_{I, |I| \leq d} (1 + r(1)_{i_1} t_1 + \dots + r(n)_{i_n} t_n) \in \mathbb{C}[X][t_1, \dots, t_n],$$

¹⁵ $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ denotes the nonnegative integers.

where the t_1, \dots, t_n are formal variables. If we distribute and collect terms, we obtain the sum

$$\sum_{I, |I| \leq d} \sigma(I) t^I, \quad \sigma \in \Sigma_d,$$

$t^I = t_1^{i_1} \dots t_n^{i_n}$. The coefficients $\sigma(I)$ are Σ_d -invariant polynomials of degree at most d . They are called **polarized symmetric functions**.¹⁶ Thus, we have proven the following result.

THEOREM 2.1 (Emmy Noether [50]): *If $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{C})$ is a faithful representation of a finite group G of order $d = |G|$, then $\mathbb{C}[V]^G$ is generated by elements of degree at most d .* \odot

This degree bound on the generators is called **Noether's bound**.

EXAMPLE 2.2 : Recall the defining representation of the dihedral group D_{2k} from the introduction. We showed that the ring of invariants

$$\mathbb{C}[x, y]^{D_{2k}} = \mathbb{C}[xy, x^k + y^k]$$

is generated by two polynomials xy and $x^k + y^k$. Emmy Noether's result gives us another way to verify this: We check all polynomials up to degree $2k$. We find precisely these two and algebraic expressions in them. This is certainly trivial for a computer algebra program, and for small k even not so hard to do by hand.

REMARK: Implicitly, Noether's bound (as well as any other degree bound) gives also a rough estimate on the *number* of generators. This is indeed an even more difficult question than the one we are discussing here. In the terminology of algebraic geometry, this amounts to finding the embedding dimension. We refer to [47] for more information on this topic.

But where did Emmy Noether use the complex numbers in her proof?¹⁷ Well, let us go through her proof again replacing \mathbb{C} by an arbitrary field \mathbb{F} . First, we need that the Noether map η_G^G is surjective. This remains true as long as we can invert the group order $|G|$.¹⁸ Then we need that $\eta_G^{\Sigma_d}$ is surjective. For that we need that the order of the symmetric group Σ_d is invertible, in other words the characteristic of the ground field must be zero or larger than d . Finally, how about the invariants of the symmetric group Σ_d acting on $\mathbb{F}[X]$? Hermann Weyl helps out with his first main theorem of invariant theory (see, e.g., Theorem 3.4.1 in [63] or Chapter 2 in [71]). The ring of invariants $\mathbb{F}[X]^{\Sigma_d}$ is still generated by the polarized symmetric functions. So, we have extended Emmy Noether's result to the case where the ground field has characteristic zero or strictly larger than the group order (see Corollary 3.3.3 in [63]).

Let us introduce some more terminology here. We say that we are in the **nonmodular case** if the group order is invertible in the ground field. If the characteristic is zero or strictly larger than the group order, we are in the **strong nonmodular case**. If the characteristic is neither zero nor larger than the group order but does not divide the group order either, we are in the **weak nonmodular case**. Finally, if the characteristic divides the group order, we are in the **modular case**.

So, how about the (weak) nonmodular case when¹⁹ $d = |G| \in \mathbb{F}^\times$? Emmy Noether's proof does

¹⁶ Among these we find the elementary symmetric functions in the elements of one row, if we choose the i_j 's to be zero except for one j . Moreover, the image $\eta_G^{\Sigma_d}(\sigma(I)) = c(I)$ are Σ_d -invariant (and a fortiori G -invariant) polynomials in $\mathbb{F}[V]$. They are called **polarized orbit Chern classes**.

¹⁷ Interesting enough, in her original paper she does not mention the ground field at all.

¹⁸ The Noether map is not surjective if $|G|$ is not invertible in the field \mathbb{F} . However, its image still characterizes the ring of invariants in the sense that its integral closure is the full invariant ring (see [45]).

¹⁹ We denote by \mathbb{F}^\times the invertible elements in \mathbb{F} .

not extend to this case. Indeed, this has been a long outstanding question and was solved only a few years ago (independently and simultaneously in [19] and [21]).

THEOREM 2.3 (Peter Fleischmann [19], John Fogarty [21]): *Let $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of a finite group G . Let $|G| \in \mathbb{F}^\times$. Then Noether's bound*

$$\beta(\mathbb{F}[V]^G) \leq |G|$$

holds.

PROOF: We present the proof due to David J. Benson ([4]).

The **Hilbert ideal**

$$\mathfrak{h}(\rho) = \overline{(\mathbb{F}[V]^G)} \subseteq \mathbb{F}[V]$$

is the ideal in $\mathbb{F}[V]$ generated by all homogeneous invariants of positive degree. This ideal can be generated by elements of degree at most group order $|G|$ as we explain next.

We start by showing that any polynomial in $\mathbb{F}[V]$ of degree at least $|G|$ is an element of $\mathfrak{h}(\rho)$. Choose $|G|$ elements $\{f_g \mid g \in G\}$ in $\mathbb{F}[V]$ of positive degree and index them by the elements of G . Then

$$\prod_{g \in G} (hg(f_g) - f_g) = 0$$

for every group element $h \in G$. Summing over all $h \in G$, distributing and collecting terms gives

$$(\star) \quad \sum_{S \subseteq G} (-1)^{|G \setminus S|} \left(\sum_{h \in G} \prod_{g \in S} h(gf_g) \right) \left(\prod_{g \in G \setminus S} f_g \right) = 0,$$

where S runs through all subsets of G . The summand corresponding to the empty set is

$$(-1)^{|G|} |G| \prod_{g \in G} f_g.$$

All other summands are elements of the Hilbert ideal, because the factor

$$\left(\sum_{h \in G} \prod_{g \in S} h(gf_g) \right) \in \mathbb{F}[V]^G$$

is invariant. Solving for $(-1)^{|G|} |G| \prod_{g \in G} f_g$ and dividing by the (nonzero!) coefficient tells us that any polynomial of degree at least $|G|$ is an element of the Hilbert ideal.

Let

$$\mathfrak{a} = (\{f \in \mathfrak{h}(\rho) \mid \deg(f) \leq d\}) \subseteq \mathfrak{h}(\rho)$$

be the subideal of the Hilbert ideal generated by all polynomials $f \in \mathfrak{h}(\rho)$ of degree at most order of G . We need to show that $\mathfrak{a} = \mathfrak{h}(\rho)$. To this end, let $f \in \mathfrak{h}(\rho)$ of degree larger than $|G|$. Let $x^I = x_1^{i_1} \dots x_n^{i_n}$ be a term of f . Then we can write

$$x^I = x^J x^K,$$

where $\deg(x^J) = |G|$ and $\deg(x^K) > 0$. Then the first factor x^J is by the preceding calculation in the Hilbert ideal $\mathfrak{h}(\rho)$. Since \mathfrak{a} and $\mathfrak{h}(\rho)$ coincide in degree $|G|$, we have that $x^J \in \mathfrak{a}$ and hence $x^I \in \mathfrak{a}$. Since this is valid for every summand of f , we derive that $f \in \mathfrak{a}$ as desired.

The rest of the proof works more or less as in D. Hilbert's classical finiteness proof (see [27]). The projection operator

$$\pi^G : \mathbb{F}[V] \rightarrow \mathbb{F}[V]^G$$

that we introduced above is surjective. It remains surjective in positive degrees, when we restrict the domain to the invariants $\overline{\mathbb{F}[V]^G}$ of positive degree. Since the ideal $(\overline{\mathbb{F}[V]^G})$ is contained in the Hilbert ideal $\mathfrak{h}(\rho)$, we obtain an epimorphism

$$\pi^G : \mathfrak{h}(\rho) \rightarrow \overline{\mathbb{F}[V]^G}.$$

The projection operator is an $\mathbb{F}[V]^G$ -module homomorphism. Therefore, the ideal generators of the Hilbert ideal, which have degree at most $|G|$, map to module generators of the augmentation ideal. But those generate the ring of invariants as an algebra. \odot

The key in the preceding proof is the result that the Hilbert ideal is generated by polynomials in degrees at most $|G|$. This should be true in any characteristic.²⁰

PROBLEM 2.4 (Harm Derksen): Show that the Hilbert ideal is generated by polynomials of degree at most $|G|$ no matter what the characteristic of the ground field is.

Let us have a look at a simple example that shows that Noether's bound is sharp.

EXAMPLE 2.5 : Let $\rho : \mathbb{Z}/n \rightarrow \mathbb{C}^\times$ be the one-dimensional representation of the cyclic group of order n that maps a generator g to $\exp(\frac{2\pi i}{n})$. Then

$$\mathbb{C}[x]^{\mathbb{Z}/n} = \mathbb{C}[x^n],$$

and hence $\beta(\mathbb{C}[x]^{\mathbb{Z}/n}) = n = |\mathbb{Z}/n|$.

So, theoretically we have solved the problem. We have an a priori degree bound, which is even sharp. However, imagine you are looking at a representation of a group of order 1152 in degree 4^{100} , and you start to check degree-wise the invariance of polynomials. A monomial basis of the \mathbb{F} -vector space $\mathbb{F}[V]_{(k)}$ of polynomials of degree k consists of

$$\binom{4^{100} + k - 1}{k}$$

elements. *Even your most diligent computer would give up on that.*²¹ So, we ask for refinements of Noether's bound, say, for certain families of groups or of representations. This is the content of the next section.

§3. The Nonmodular Case II: Refinements and Relative Bounds

In this section we remain in the nonmodular case, i.e., we assume that the group order $|G|$ is invertible in the ground field \mathbb{F} . There are several ways to obtain improved bounds. They all rely on the idea of comparison and "worst case" studies.

THEOREM 3.1 ((Weak) Relative Noether Bound): *Let $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of a finite group. Let $H \leq G$ be a subgroup of G . Assume that either (i) $H \triangleleft G$ is a normal subgroup in G and the index $|G : H| \in \mathbb{F}^\times$ is invertible in the ground field, or (ii) the characteristic of the ground field \mathbb{F} does not divide the group order $|G|$. Then*

$$\beta(\rho) \leq |G : H| \beta(\rho|_H).$$

²⁰ See Conjecture 3.8.3 in [12].

²¹ At least for now.

PROOF: The proof of this relative result works as the proof of Theorem 2.3. We replace $\mathbb{F}[V]$ by $\mathbb{F}[V]^H$ and the Hilbert ideal $\mathfrak{b}(\rho)$ by the ideal in $\mathbb{F}[V]^H$ generated by the G -invariants of positive degree. The sum (\star) runs then over the subsets S of a set of coset representatives of H in G , and the polynomials f_g are indexed by coset representative gH . Finally, we also replace the projection map π^G by a relative version

$$\pi_H^G : \mathbb{F}[V]^H \longrightarrow \mathbb{F}[V]^G, f \mapsto \sum_g gf,$$

where the sum runs over a set of coset representatives of H in G . We refer to [58] and [47] Corollary 2.3.5 and Theorem 7.3.3 for details. \odot

Before we proceed let us note that the relative Noether bound should be true if only the index $|G : H|$ is invertible in the ground field.

PROBLEM 3.2 : Prove the relative Noether bound in general, i.e.,

$$\beta(\rho) \leq |G : H| \beta(\rho|_H)$$

whenever $H \leq G \xrightarrow{\circlearrowleft} \text{GL}(n, \mathbb{F})$ is a subgroup with index $|G : H| \in \mathbb{F}^\times$.

Now, if we can find a subgroup H such that the assumptions of Theorem 3.1 are satisfied and

$$\beta(\rho|_H) < |H|,$$

then we obtain also a better bound for $\beta(\rho)$. A candidate we should watch out for is given by the following result.

PROPOSITION 3.3 (Barbara Schmid [57]): *Let $|G|$ be invertible in the ground field. Then*

$$\beta(\rho) \leq |G| - 1$$

whenever G is noncyclic abelian.

Combining these two results gives sharper bounds whenever we can find a noncyclic abelian subgroup satisfying the assumptions of Theorem 3.1.

If $H \triangleleft G$ is a normal subgroup, then

$$\mathbb{F}[V]^G = \left(\mathbb{F}[V]^H \right)^{G/H},$$

i.e., the factor group G/H acts linearly on the ring of H -invariants. If the factor group G/H is noncyclic abelian, then we find the better bound²²

$$\beta(\mathbb{F}[V]^G) \leq (|G : H| - 1) \beta(\mathbb{F}[V]^H).$$

Finding chains of such subgroups gives even better bounds. This brings nilpotent groups into the picture. Denote by

$$Z(G) = \{g \in G \mid gh = hg \forall h \in G\}$$

the center of the group G . Set $Z^1(G) = Z(G)$ and define iteratively the higher centers $Z^j(G)$ by requiring

$$Z^{j+1}(G)/Z^j(G) = Z(G/Z^j(G)), \quad \forall j \geq 1.$$

²² Yes, we are using that Proposition 3.3 is true whenever a group (here G/H) acts linearly on a graded Noetherian \mathbb{F} -algebra (here $\mathbb{F}[V]^H$).

This leads to the upper or ascending central series of G

$$\{1\} = Z^0(G) \leq Z^1(G) \leq \dots \leq Z^j(G) \leq \dots \leq G.$$

A group G is called **nilpotent** if there exists an $s \in \mathbb{N}$ such that $Z^s(G) = G$. The smallest natural number s with this property is the **class of nilpotency**, denoted by $\text{nil}(G) = s$.

PROPOSITION 3.4 (Daniela Krause [35]): *Let G be a nonabelian nilpotent group of nilpotency class s . If $|G| \in \mathbb{F}^\times$, then*

$$\beta_{\mathbb{F}}(G) \leq |G| - 2^{s-1}.$$

PROOF: Since centers are normal subgroups, we apply the Relative Noether Bound, Theorem 3.1 and obtain

$$\beta(G) \leq \beta(Z^{s-1}(G)) \cdot \beta(G/Z^{s-1}(G)).$$

By Noether's Bound, Theorem 2.3, we know that

$$\beta(Z^{s-1}(G)) \leq |Z^{s-1}(G)|.$$

Since G is non-abelian, the last factor in the upper central series is not cyclic, but abelian.²³ Therefore, by Barbara Schmid's result, Proposition 3.3,

$$\beta(G/Z^{s-1}(G)) \leq |G/Z^{s-1}(G)| - 1.$$

Thus, combining these ineuqlities leads to

$$\begin{aligned} \beta(G) &\leq \beta(Z^{s-1}(G)) \cdot \beta(G/Z^{s-1}(G)) \\ &\leq |Z^{s-1}(G)| \cdot (|G/Z^{s-1}(G)| - 1) \\ &= |G| - |Z^{s-1}(G)|. \end{aligned}$$

Since all factor groups of the upper ascending central series are nontrivial, we obtain

$$|Z^j(G)| \geq 2|Z^{j-1}(G)| \quad \forall j = 1, \dots, s.$$

Hence, by induction on j , $|Z^{s-1}(G)| \geq 2^{s-1}$, and the result follows. \blacklozenge

In a similar way, by finding suitable chains of subgroups with at least one noncyclic abelian factor group, Daniela Krause gives improved bounds for the symmetric and alternating groups and for the classical and exceptional Coxeter groups (see [35] or Section 7.3 in [47]). Here are a few samples of her results.

EXAMPLE 3.5 (Daniela Krause [35]): For any representation such that the characteristic does not divide the group order we have

$$\begin{aligned} \beta(\Sigma_n) &\leq \frac{3}{4} |\Sigma_n| \quad \text{for } n > 3, \\ \beta(A_n) &\leq \frac{3}{4} |A_n| \quad \text{for } n > 3, \\ \beta(W(F_4)) &\leq \frac{9}{16} |W(F_4)| = 648, \\ \beta(W(G_2)) &\leq \frac{3}{4} |W(G_2)| = 9, \end{aligned}$$

where Σ_n denotes the symmetric group on n letters, A_n the alternating group on n letters, $W(F_4)$ the Weyl group of order 1152, and $W(G_2)$ the dihedral group of order 12.

²³ It is abelian because nilpotent groups of class one are abelian. It is not cyclic because $G/Z^{s-1}(G)$ is abelian and non-cyclic.

Indeed, some of the bounds given in the preceding example are valid in a more general context as the next result shows, see [16] and [58].

THEOREM 3.6 (Mátyás Domokos and Pál Hegedüs [16], Müfit Sezer [58]): *Let $|G|$ be invertible in \mathbb{F} . Then*

$$\beta_{\mathbb{F}}(G) \begin{cases} = |G| & \text{if } G \text{ is cyclic,} \\ \leq \frac{3}{4}|G| & \text{if } G \text{ is noncyclic of even order,} \\ \leq \frac{5}{8}|G| & \text{if } G \text{ is noncyclic of odd order.} \end{cases}$$

There is another set of improvements. In contrast to the discussion above we do not compare degree bounds for groups and their subgroups, but degree bounds for one single group but in different representations. The key is to look at the regular representation ρ_{reg} of a group G .

The next result was originally proved in characteristic zero (see [57]). The statement remains true in the strong nonmodular case but requires a completely new proof (see [65]).

THEOREM 3.7 (Barbara Schmid [57], Larry Smith [65]): *Let $\rho : G \hookrightarrow \text{GL}(n, \mathbb{F})$ be representation in the strong nonmodular case. Then*

$$\beta_{\mathbb{F}}(G) \leq \beta(\rho_{\text{reg}}).$$

This means that the regular representation realizes the worst case for the question of degree bounds. Therefore, if we find a bound for the regular representation, we have one for any strong nonmodular representation.

This makes it desirable to extend the preceding Theorem 3.7 to a more general context. The following is expected to be possible.

PROBLEM 3.8 (Larry Smith): Show that

$$\beta_{\mathbb{F}}(G) \leq \beta(\rho_{\text{reg}})$$

is true whenever the group order is invertible in the ground field.

We note that this has been proven quite recently for abelian groups, see [58].

§4. Inbetween: Permutation Groups

So, far we have looked only at representations $\rho : G \hookrightarrow \text{GL}(n, \mathbb{F})$ in the nonmodular case. Before turning to the modular case we consider permutation representations.

Denote by

$$\begin{aligned} e_1 &= x_1 + \cdots + x_n, \\ e_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n, \\ &\dots \\ e_n &= x_1 x_2 \cdots x_n \end{aligned}$$

the elementary symmetric polynomials in the variables x_1, \dots, x_n . The ring

$$\mathbb{F}[V]^{\Sigma_n} = \mathbb{F}[e_1, \dots, e_n]$$

is the ring of invariants of all permutation matrices, i.e., the ring of invariants of the symmetric group Σ_n acting on $\mathbb{F}[x_1, \dots, x_n]$ by permuting the variables. This is one of the oldest

known invariant rings; known certainly to Isaac Newton, and already in Edward Waring's work we find an algorithm that takes an arbitrary symmetric function and rewrites it as a polynomial in the elementary symmetric functions (see Problem I and III in Chapter 1 of [70]).

By its very definition, $\mathbb{F}[V]^{\Sigma_n}$ is some kind of universal object in the class of rings of invariants of permutation groups: If we take any **permutation group** G , i.e., a group G that acts via permutations on the variables x_1, \dots, x_n ,²⁴ then it must be contained in Σ_n , and hence

$$\mathbb{F}[V]^{\Sigma_n} \subseteq \mathbb{F}[V]^G.$$

In other words, the elementary symmetric functions are invariant under any permutation group.

Even though permutation representations are among those representations that have been studied from the beginning of time, they are still full of surprises. One of these surprises is **Göbel's bound**.

In 1984, Adriano M. Garsia and Dennis Stanton proved that in characteristic zero, the ring of invariants of a permutation representation on a set of n elements can be generated by polynomials of degree at most $\max\{\frac{n(n-1)}{2}, n\}$ (see [22]). About ten years later, Manfred Göbel showed in his diploma thesis that this bound is valid *no matter what the ground field is* (see [24], [53] or Corollary 3.4.3 in [47]).

THEOREM 4.1 (Adriano M. Garsia and Dennis Stanton [22], Manfred Göbel [24]): *Let $\rho : G \hookrightarrow \text{GL}(n, \mathbb{F})$ be a permutation representation of the group G . Then*

$$\beta(\rho) \leq \max\left\{\frac{n(n-1)}{2}, n\right\}.$$

For permutation representations, the investigation of many properties can be reduced to counting algorithms, because their rings of invariants are by construction generated by orbit sums of monomials as we explain next.

Let $x^I = x_1^{i_1} \cdots x_n^{i_n} \in \mathbb{F}[V]$ be a monomial. Then

$$g(x^I) = g(x_1)^{i_1} \cdots g(x_n)^{i_n}$$

for any $g \in G$. Since $g(x_i) = x_{g(i)}$, we obtain that $g(x^I)$ is a monomial. Its orbit sum is

$$o(x^I) = \sum_{g \in G} g(x^I).$$

Let

$$f = \sum_I x^I \in \mathbb{F}[V]^G$$

be an arbitrary invariant polynomial. Then

$$gf = \sum_I g(x^I) = \sum_{I'} o(x^{I'}),$$

where the second sum on the right runs over all I' such that $x^{I'}$ and $x^{I''}$ have disjoint orbits. Thus every invariant polynomial f is a sum of orbit sums of monomials.

This is also the key to Manfred Göbel's proof. He calls a monomial $x_1^{i_1} \cdots x_n^{i_n}$ **special** if the exponents satisfy the following condition: Reorder the exponents in nondecreasing order.

²⁴ Rather than *permutation groups* we should talk about *permutation representation* of a group G .

Without loss of generality we assume that

$$i_1 \leq i_2 \leq \dots \leq i_n.$$

We call $x_1^{i_1} \dots x_n^{i_n}$ special, if $i_j - i_{j-1} \leq 1$ and $i_1 = 0$. For example, the monomial $x_1^2 x_2 x_3^2 \in \mathbb{F}[x_1, x_2, x_3, x_4]$ is special because its exponents sequence is 0, 1, 2, 2 but the monomial $x_1^2 x_3^2$ is not special. Its exponent sequence 0, 0, 2, 2 has a “gap”. Likewise, the monomial $x_1 x_2 x_3 x_4$ is not special, because the exponent sequence 1, 1, 1, 1 does not start with 0. Note that a special monomial has by definition at most degree $\frac{n(n-1)}{2}$.

Then M. Göbel constructs an explicit algorithm, that rewrites an orbit sum of an arbitrary monomial as a polynomial in orbit sums of special monomials and the n th elementary symmetric function $e_n = x_1 \dots x_n$. This algorithm is very similar to the classical algorithm occurring in Carl F. Gauss’ work [23] that rewrites a polynomial invariant under the full symmetric group in terms of elementary symmetric functions.

Moreover, Göbel’s bound is sharp as the following example shows.

EXAMPLE 4.2 : Let $\rho : A_n \hookrightarrow \text{GL}(n, \mathbb{F})$ be the defining representation²⁵ of the alternating group A_n in n letters over any field \mathbb{F} . Then its ring of invariants is generated by the elementary symmetric functions e_1, \dots, e_n and an additional polynomial ∇_n

$$\mathbb{F}[V]^{A_n} = \mathbb{F}[e_1, \dots, e_n, \nabla_n],$$

where there is a quadratic relation among the generators. In odd (or zero) characteristic the invariant ∇_n may be taken to be the **discriminant** (or **Vandermonde determinant**)

$$\nabla_n = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

If $p = 2$, then it is the orbit sum of the monomial $x_1 x_2^2 \dots x_{n-1}^{n-1}$

$$\nabla_n = \sum_{g \in A_n} g(x_1 x_2^2 \dots x_{n-1}^{n-1}).$$

Note that ∇_n has degree $\frac{n(n-1)}{2}$ in both cases. (See Example 1 in Section 3.4 in [47] for a detailed discussion of this example.)

Although Göbel’s bound is independent of the ground field, in contrast to Noether’s bound, it does depend on the dimension n of the representation (or more precisely on the number n of variables being permuted). The fact that this is not a mere accident will become clearer in the next section.

§5. The Modular Case I: The Problem

We are in the modular case, when the characteristic p of the ground field divides the group order. We start with an example.

Let $\mathbb{Z}/2 \hookrightarrow \text{GL}(2, \mathbb{F})$ be the representation of the cyclic group of order 2 afforded by the matrix

$$\mathbf{M} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Its ring of invariants is the polynomial ring

$$\mathbb{F}[V]^{\mathbb{Z}/2} = \mathbb{F}[x, y]^{\mathbb{Z}/2} = \mathbb{F}[x + y, xy]$$

²⁵ So, we are looking at the permutation matrices that correspond to even permutations.

for every ground field because this is the symmetric group in two letters in its defining representation.

We double this representation. In other words, we consider the 4-dimensional representation afforded by

$$\begin{bmatrix} \mathbf{M} & \mathbf{0} \\ \mathbf{0} & \mathbf{M} \end{bmatrix}.$$

Then $\mathbb{Z}/2$ acts on $(V^*)^2 = \text{Span}_{\mathbb{F}}\{x_1, y_1, x_2, y_2\}$ by simultaneously interchanging the x 's and the y 's. The ring of invariants turns out to be a hypersurface

$$\mathbb{F}[V^2]^{\mathbb{Z}/2} = \mathbb{F}[x_1 + y_1, x_1y_1, x_2 + y_2, x_2y_2, x_1y_2 + x_2y_1],$$

where there is a relation of degree 4 among the generators (see [41]). So, the ring is no longer polynomial, and it is not enough to have the invariants of the two subrepresentations given by \mathbf{M} since

$$\mathbb{F}[x_1, y_1]^{\mathbb{Z}/2} \otimes_{\mathbb{F}} \mathbb{F}[x_2, y_2]^{\mathbb{Z}/2} \subsetneq \mathbb{F}[V^2]^{\mathbb{Z}/2}.$$

Note that the additional invariant $x_1y_2 + x_2y_1$ has degree 2.

Next we take three copies of our representation and ask for the ring of invariants of the 6-dimensional representation of $\mathbb{Z}/2$ afforded by the matrix

$$\begin{bmatrix} \mathbf{M} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{M} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{M} \end{bmatrix}.$$

The polynomials

$$\begin{aligned} \ell_i &= x_i + y_i \quad \text{for } i = 1, 2, 3, \\ q_i &= x_iy_i \quad \text{for } i = 1, 2, 3, \\ Q_i &= x_jy_k + x_ky_j \quad \text{for pairwise distinct } i, j, k \in \{1, 2, 3\}, \end{aligned}$$

generate the ring of invariants whenever the characteristic is not even (by Noether's bound, Theorem 2.3). Otherwise we need a cubic generator

$$c = x_1x_2x_3 + y_1y_2y_3.$$

To see this we need some preparation.

Let A be a nonnegatively graded Noetherian \mathbb{F} -algebra. Denote by $A_{(i)}$ the homogeneous part of A of degree i . Then the Poincaré series of A is the power series

$$P(A, t) = \sum_{i \geq 0} \dim_{\mathbb{F}}(A_{(i)}) t^i,$$

where $\dim_{\mathbb{F}}(A_{(i)})$ is the vector space dimension. Since a ring of invariants $\mathbb{F}[V]^G$ is a nonnegatively graded Noetherian \mathbb{F} -algebra, the Poincaré series tells us how many (\mathbb{F} -linearly independent) invariants in any given degree there are.²⁶ In 1897, T. Molien describes this infinite series for invariant rings just in terms of the groups elements (cf. Section 3.1 in [47] or the original [40])

THEOREM 5.1 (T. Molien [40]): *Let $\rho : G \hookrightarrow \text{GL}(n, \mathbb{F})$ be a permutation representation or*

²⁶ Since we are assuming that A is nonnegatively graded, so is $A^G \subseteq A$.

let $|G| \in \mathbb{F}^\times$. Then²⁷

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

Thus, the series can be calculated *without knowing* the invariant ring.

We apply this to our problem, and obtain

$$P(\mathbb{F}[V^3]^{\mathbb{Z}/2}, t) = 1 + 3t + 12t^2 + 28t^3 + \dots$$

(see Example 2 in Section 2.4 of [47]). This tells us that we need 3 generators in degree 1, namely the l_1, l_2, l_3 . Then we need 12 linearly independent invariants in degree 2. The different products of our linear generators are already 6, so the 6 generators q_i and Q_i , for $i = 1, 2, 3$, make the list complete. In degree 3, we need 28 linearly independent invariants. From what we have so far, we obtain 28 cubic invariants by building suitable products. However, the equation

$$l_1 l_2 l_3 - Q_1 l_1 - Q_2 l_2 - Q_3 l_3 = 2(x_1 x_2 x_3 + y_1 y_2 y_3) = 2c \equiv 0 \pmod{2}$$

shows that they are not linearly independent in characteristic 2. Hence we need the additional cubic generator c precisely in even characteristic.

Indeed, proceeding this way, and considering the $\mathbb{Z}/2$ -representation afforded by k copies of \mathbf{M} , leads to the following result.

THEOREM 5.2 (David Richman [54]): *With the above notation, we have that*

$$\beta(\mathbb{F}[V^k]^{\mathbb{Z}/2}) \geq k,$$

whenever the characteristic of \mathbb{F} is even.

It can be shown that the invariant polynomial $x_1 \dots x_k + y_1 \dots y_k$ is not in the subalgebra generated by the polynomials of lower degree, and can be taken as an algebra generator of degree k .²⁸

Note that the *lower* bound of the maximal degree of a generator increases with the dimension of the representation.²⁹ So, we cannot expect to have a degree bound in the modular case that is independent of the dimension of the representation.

On the other hand, we have the following two general upper bounds, see Theorem 3.8.11 in [12] and Theorem 16.4 in [30].

THEOREM 5.3 (Harm Derksen and Gregor Kemper [12]): *For $\dim(V) = n$ we have that*

$$\beta(\mathbb{F}[V]^G) \leq n(|G| - 1) + |G|^{n2^{n-1}} n^{2^{n-1}+1}.$$

The main input needed to obtain this bound is a result due to Grete Hermann (a student of Emmy Noether at Göttingen), who found upper degree bounds for generators of syzygy modules (see [26]).

The proof of the second general bound is actually just a by-product of some representation-theoretic results.

²⁷If the characteristic of \mathbb{F} is positive, then we need to use a characteristic zero lift of ρ in this formula.

²⁸Note that we get for $k = 1$ the regular representation of $\mathbb{Z}/2$, and it does not realize the worst case, cf. Section 3 and, in particular, Theorem 3.7 and Problem 3.8.

²⁹Indeed, much current research is focused on finding lower degree bounds in the modular case.

THEOREM 5.4 (Dikran B. Karagueuzian and Peter Symonds [30]): *For $\dim(V) = n$ and $|\mathbb{F}| = q$, one has*

$$\beta(\mathbb{F}[V]^G) \leq \begin{cases} \frac{q^n - 1}{q - 1}(nq - n - 1) & \text{if } n \geq 3 \\ 2q^2 - q - 2 & \text{if } n = 2. \end{cases}$$

It is interesting that the first general bound depends only on the group order and the degree of the representation, while the second depends on the degree of the representation and the size of the field. So, for large groups the latter bound should be stronger, while for large fields the former.

For theoretical purposes, it is good to know that there exist bounds depending only on the group order, the dimension of the representation, and the order of the ground field. In this sense, the preceding two results are the best that one could expect after looking at D. Richman's lower bound. However, both of them are extremely high, and thus useless for practical purposes.³⁰ This leaves us with the following problem.

PROBLEM 5.5 : Improve the bounds given in Theorems 5.3 and 5.4 as they stand in the general case, or for special situations, e.g., special representations, or special groups.

Most recently, the following partial answer was obtained.

THEOREM 5.6 (Mara D. Neusel and Müfit Sezer [46]): *If V is a projective G -module, then*

$$\beta(\mathbb{F}[V]^G) \leq \max\{n|G|, \binom{n|G|}{2}\}.$$

Recall that we have a relative bound. If $\text{Syl}_p(G) \subseteq G$ be a p -Sylow subgroup of G such that the assumptions of Theorem 3.1 hold, then

$$\beta(\mathbb{F}[V]^G) \leq |G : \text{Syl}_p(G)| \beta(\mathbb{F}[V]^{\text{Syl}_p(G)})$$

and therefore, the problem of finding degree bounds is reduced to a problem for representations of p -groups in characteristic p .

§6. The Modular Case II: p -Groups

We consider representations of p -groups P in characteristic p . The general upper bound given in Theorem 5.4 has been improved for p -groups in the very same paper, [30]. Again, it depends only on the degree of the representation and the size of the field.

THEOREM 6.1 (D. B. Karagueuzian and P. Symonds [30]): *For $\dim(V) = n$ and $|\mathbb{F}| = q$ we have that*

$$\beta(\mathbb{F}[V]^P) \leq \begin{cases} \frac{q^n - 1}{q - 1} - n & \text{if } n \geq 3 \\ q & \text{if } n = 2. \end{cases}$$

However, even though this bound is sharp as we will see in a moment, it is desirable to improve it for special representations, or certain nice groups.

A tempting path is to start with the smallest p -group, namely \mathbb{Z}/p , and consider its representations given by Jordan blocks \mathbf{J}_i of size i (so necessarily $2 \leq i \leq p$)

³⁰ Quite recently a new general degree bound has been found, see [11].

$$\mathbf{J}_i = \begin{bmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & 1 & \\ 0 & \dots & 0 & 1 & \end{bmatrix}.$$

The representations afforded by a Jordan block are indecomposable but they are not irreducible, because $\text{Span}_{\mathbb{F}}(v_1) \subseteq V$ is stable under the \mathbb{Z}/p -action.

If $i = 2$, then

$$\mathbf{J}_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

leads to the ring of invariants $\mathbb{F}[x, y]^{\mathbb{Z}/p} = \mathbb{F}[x^p - xy^{p-1}, y]$. Note that it is generated by the top orbit Chern classes

$$c_{\text{top}}(x) = \prod_{\alpha \in \mathbb{F}} (x - \alpha y) = x^p - xy^{p-1}, \quad \text{and} \quad c_{\text{top}}(y) = y$$

of x and y , i.e., the product of all elements in the orbit of x , resp. y , see Section 4.1 in [47]. This is the promised example that shows that Theorem 6.1 is sharp: take $|\mathbb{F}| = p$ and $n = 2$, then they predict the general bound p which is assumed in this representation of \mathbb{Z}/p .

For $i = 3$ our ring of invariants becomes a hypersurface

$$\mathbb{F}[x, y, z]^{\mathbb{Z}/p} = \mathbb{F}[c_{\text{top}}(x), c_{\text{top}}(y), z, Q]/(r),$$

where Q is an invariant of degree 2 and r a relation of degree $2p$ (see [41]). So, for the two smallest Jordan blocks the degree bound is the group order. Next, the rings of invariants for Jordan blocks of \mathbb{Z}/p of size 4 and 5 are explicitly calculated in [60]. We read off the degree bounds³¹

$$\beta(\mathbb{F}_p[V]^{\mathbb{Z}/p}) \leq \begin{cases} 2p-3 & \text{if } n=4, \\ 2p-2 & \text{if } n=5, \end{cases}$$

(see Corollaries 4.2 and 5.2 in [60]). This suggests that the degrees increase with the size of the Jordan blocks.

The proof of the following result relies on a close inspection of Koszul homology.

PROPOSITION 6.2 (Larry Smith [67]): *Let $\rho : \mathbb{Z}/p \hookrightarrow \text{GL}(n, \mathbb{F})$ be a faithful representation of \mathbb{Z}/p afforded by a single Jordan block. Let $n = 2, p-1$, or p . Then*

$$\beta(\mathbb{F}[V]^{\mathbb{Z}/p}) \leq \max \left\{ p, \begin{cases} \frac{n}{2}(p-1) & \text{if } n \text{ is even} \\ 1 + \frac{n-1}{2}(p-1) & \text{if } n \text{ is odd} \end{cases} \right\}.$$

This bound is sharp as the cases $n=2$ and $n=3$ show, and can be generalized to representations of \mathbb{Z}/p afforded by a matrix consisting of k Jordan blocks (see [67]).

Apart from the above, we have only a number of isolated examples. Note that since the general linear group $\text{GL}(n, \mathbb{F}_q)$ over a finite field with q elements ($q = p^s$ for some $s \in \mathbb{N}_0$) is itself finite, it has also a finite p -Sylow subgroup. Hence, every p -group P is a subgroup of $\text{Syl}_p(\text{GL}(n, \mathbb{F}_q))$, and

$$\mathbb{F}_q[V]^{\text{Syl}_p(\text{GL}(n, \mathbb{F}_q))} \subseteq \mathbb{F}_q[V]^P.$$

In other words, the invariants of the p -Sylow subgroup of $\text{GL}(n, \mathbb{F}_q)$ are present in every ring of invariants of a p -group.³²

³¹ The notation \mathbb{F}_p means that this result is only true for the prime field with $|\mathbb{F}_p| = p$ elements.

³² In the same way we find that the invariants of the general linear group $\text{GL}(n, \mathbb{F}_q)$ over a finite field \mathbb{F}_q form a set of universal

EXAMPLE 6.3 (Marie–José Bertin [5]): The ring of invariants of the p -Sylow subgroup $\text{Syl}_p(\text{GL}(n, \mathbb{F}_q))$ of the general linear group is given by

$$\mathbb{F}_q[V]^{\text{Syl}_p(\text{GL}(n, \mathbb{F}_q))} = \mathbb{F}_q[h_1, \dots, h_n],$$

where h_i is the top orbit Chern class of x_i , $i = 1, \dots, n$, i.e.,

$$h_i = \prod_{g \in P} g x_i$$

is the product of all elements in the orbit of x_i and has degree q^{n-i} . Note that this is a polynomial ring. Hence, $\mathbb{F}[V]^{\text{Syl}_p(\text{GL}(n, \mathbb{F}_q))} \hookrightarrow \mathbb{F}[V]^G$ forms a universal Noether normalization.

So, there is not much we know about degree bounds for representations of p -groups.

PROBLEM 6.4 : Find degree bounds for certain families of p -groups or for certain families of representations.

§7. The Modular Case III: Special Types of Rings

In contrast with the nonmodular case, the variety of rings in the modular case that can occur as invariant rings is large. Thus, it makes sense to investigate also special families of *rings* and not only groups or representations. We list some of the most important results of this type.

From the ring-theoretic point of view, the best type of ring that can occur as a ring of invariants is a **polynomial ring**, i.e.,

$$\mathbb{F}[V]^G = \mathbb{F}[f_1, \dots, f_n],$$

where f_1, \dots, f_n are algebraically independent. In this case, we have that

$$\deg(f_1) \cdots \deg(f_n) = |G|$$

and thus

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

see Corollary 4.5.4 in [47].

The following result deals with the next best cases: We call $\mathbb{F}[V]^G$ a **hypersurface** if

$$\mathbb{F}[V]^G = \mathbb{F}[f_1, \dots, f_{n+1}]/(r).$$

Gorenstein rings are a special case of hypersurfaces. Since the definition is a bit technical we refer to Corollary 5.7.4 in [47].

PROPOSITION 7.1 (H. Eddy A. Campbell, Anthony V. Geramita, Ian P. Hughes, R. James Shank, and David L. Wehlau [9]): *Let $\rho : G \hookrightarrow \text{GL}(n, \mathbb{F})$ be a faithful representation of a finite group.*

(1) *If the ring of invariants $\mathbb{F}[V]^G$ is a hypersurface, then*

$$\beta(\mathbb{F}[V]^G) \leq |G|.$$

(2) *If the ring of invariants $\mathbb{F}[V]^G$ is Gorenstein, then*

$$\beta(\mathbb{F}[V]^G) \leq n(|G| - 1).$$

This result is based on a very delicate Poincaré series calculation.

invariants present in every $\mathbb{F}[V]^G$ for subgroups $G \subseteq \text{GL}(n, \mathbb{F}_q)$, cf. Example 1.

Hypersurfaces and Gorenstein rings belong to the family of **Cohen–Macaulay rings**, see Page 115 in [47] for a definition. For that the following is known.

PROPOSITION 7.2 (Abraham Broer [8]): *Let $\mathbb{F}[V]^G$ be Cohen–Macaulay, and let*

$$\mathbb{F}[f_1, \dots, f_n] \hookrightarrow \mathbb{F}[V]^G$$

be a Noether normalization. Then

$$\beta(\rho) \leq \min \left\{ \begin{array}{l} \max \{ \deg(f_1), \dots, \deg(f_n), \deg(f_1) + \dots + \deg(f_n) - n \} \\ \max \{ |G|, (n - \dim_{\mathbb{F}}(V^*)^G) (|G| - 1) \} \end{array} \right\}.$$

As in the preceding result, this relies on a Poincaré series argument.

It is expected that the general degree bound for Cohen–Macaulay rings of invariants coincides with the classical Noether bound. Intuitively, this looks like a reasonable generalization of Noether’s bound, because in the classical nonmodular case a ring of invariants is always Cohen–Macaulay by a result due to Jack Eagon and Mel Hochster (see Theorem 5.5.2 in [47]).

PROBLEM 7.3 (Nelson Killius [33]): Show that $\beta(\mathbb{F}[V]^G) \leq |G|$ whenever the ring of invariants is Cohen–Macaulay.

Completely open is the situation when $\mathbb{F}[V]^G$ is not Cohen–Macaulay but has depth less than its Krull dimension. We saw already an example of this type, namely, David Richman’s $\mathbb{Z}/2$ (Theorem 5.2). Its ring of invariants $\mathbb{F}[V^k]^{\mathbb{Z}/2}$ is not Cohen–Macaulay for $k \geq 3$ (see [9]). This phenomenon (that the ring of invariants is no longer Cohen–Macaulay and) that the degrees increase with k always happens when we add up copies of permutation representations (see [31]). This leads to the following problem.

PROBLEM 7.4 : Let $U \leq V$ be G -modules. Show that

$$\beta(\mathbb{F}[V]^G) \geq k\Phi(\beta(\mathbb{F}[U]^G)),$$

where $\Phi(\beta(\mathbb{F}[U]^G))$ is some function of $\beta(\mathbb{F}[U]^G)$, and $k \in \mathbb{N}$.

In [61], a partial solution to this problem has been found:

PROPOSITION 7.5 (R. James Shank and David L. Wehlau [61]): *Let $U \leq V$ be \mathbb{Z}/p -modules. Then*

$$\beta(\mathbb{F}[U]^{\mathbb{Z}/p}) \leq \beta(\mathbb{F}[V]^{\mathbb{Z}/p}).$$

Finally, we do have a relative degree bound in the modular case that differs decisively from the relative bounds (Theorem 3.1 and Theorem 3.7) in the nonmodular case (see [66]³³).

PROPOSITION 7.6 (Larry Smith [66]): *Let $U \subseteq V$ be a subspace, and let $G_U = \{g \in G \mid gu = u \forall u \in U\}$ be the pointwise stabilizer subgroup of U in G . Then*

$$\beta(\mathbb{F}_q[V]^G) \geq \beta(\mathbb{F}_q[V]^{G_U}),$$

where \mathbb{F}_q denotes the finite field with q elements.

The original proof of this result makes use of the fact that rings of invariants over finite fields are unstable algebras over the Steenrod algebra. We refer to Chapters 10 and 11 in

³³ The proof in this reference is wrong, but it seems to be corrected by the author. However, the result is correct, since it has been (re)proved in [32].

[63], Chapters 8 – 10 in [47], or the introduction of [43] for an algebraic introduction of the Steenrod algebra, algebras over it and its use in invariant theory.

Concluding Remarks

In this article, where we have tried to explain problems, questions, and answers to just one problem in invariant theory

Find a bound on the degrees of the generators of a minimal generating set of $\mathbb{F}[V]^G$,

we used tools from a wide range of mathematics. We needed to know something about the groups involved and their representations. We used methods from combinatorics, in particular when dealing with permutation groups or over finite fields. We employed machinery developed in commutative algebra and algebraic geometry.³⁴ Group cohomology, homological algebra, local cohomology, and Steenrod technology, a child of algebraic topology, are also vital in the investigation of invariant theory.

The problem of degree bounds is only one in the rapidly growing³⁵ field of postmodern invariant theory.

There are many others to discover, some of which we mentioned in passing: about the number of generators (the embedding dimension), about constructing generators (e.g., polarized symmetric functions and orbit Chern classes), about the depth, about Poincaré series and how to calculate them, about systems of parameters and their construction, about homological properties, about vector invariants (which appeared here in David Richman's example and in Emmy Noether's proof of the finite generation of invariants), ...³⁶ We refer to Chapter 1 of [47] for a detailed overview over answers to these fascinating questions and what methods have been used to solve them.

Thus, invariant theory offers interesting, intriguing, and challenging problems, that require blending together results and methods from a broad range of mathematics to an exciting new field.

§8. Acknowledgement

Roger W. Barnard, Richard W. Beals, David J. Benson, Walter Feit, William H. Gustafson, Alexander Hahn, Michele Interfont, Dan C. Isaksen, Mark Johnson, Steven G. Krantz, Reinhard Laubenbacher, Anne Pilkington, Victor Protsak, George Seligman, Larry Smith, and Magdalena Toda read versions of this manuscript. Thank you.

I thank the referees for many good comments.

References

- [1] Michael F. Atiyah and Ian G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Co., Reading MA 1969.
- [2] Alejandro Adem and R. James Milgram, *Cohomology of Finite Groups*, Springer Verlag, New York 1994.
- [3] David J. Benson, *Polynomial Invariants of Finite Groups*, London Math. Soc. Lecture Series 190, Cambridge University Press, Cambridge 1993.

³⁴ Indeed, many of the *classical* results in commutative algebra were motivated by problems in invariant theory.

³⁵ Most of the results presented here are less than 15 years old!

³⁶ And we have not said a single word about rings of invariants of (finite) groups acting on other (graded) algebras than polynomial rings!

- [4] David J. Benson, private communication, Athens GA–Notre Dame IN 2000/2001.
- [5] Marie-José Bertin, *Anneaux d'invariants d'anneaux de polynômes en caractéristique p* , C. R. Acad. Sci. Paris 277 (Série A) (1973), 691–694.
- [6] George Boole, *Exposition of a General Theory of Linear Transformations, Part I*, Cambridge Mathematical Journal 3 (1843), 1–20.
- [7] George Boole, *Exposition of a General Theory of Linear Transformations, Part II*, Cambridge Mathematical Journal 3 (1843), 106–119.
- [8] Abraham Broer, *Remarks on the Invariant Theory of Finite Groups*, Preprint, Université de Montréal, 1997.
- [9] H. Eddy A. Campbell, Anthony V. Geramita, Ian P. Hughes, R. James Shank, and David L. Wehlau, *Non-Cohen–Macaulay Vector Invariants and a Noether Bound for a Gorenstein Ring of Invariants*, Canad. Math. Bull. 42 (1999), 155–161.
- [10] David P. Carlisle and Peter Kropholler, *Modular Invariants of Finite Symplectic Groups*, preprint, Manchester 1992.
- [11] Jianjun Chuai, *A New Degree Bound for Invariant Rings*, Proceedings of the AMS, to appear.
- [12] Harm Derksen and Gregor Kemper, *Computational Invariant Theory*, Encyclopaedia of Mathematical Sciences, Springer-Verlag, Heidelberg 2002.
- [13] Leonard E. Dickson, *A Fundamental System of Invariants of the General Modular Linear Group with a Solution of the Form Problem*, Transactions of the AMS 12 (1911), 75–98.
- [14] Leonard E. Dickson, *The Collected Mathematical Papers of Leonard Eugene Dickson*, 6 vols, ed. by A. A. Albert, Chelsea Pub. Co., The Bronx, New York 1975.
- [15] Mátyás Domokos, private communication, Budapest, Hungary–Notre Dame IN 2001.
- [16] Mátyás Domokos and Pál Hegedüs, *Noether's Bound for Polynomial Invariants of Finite Groups*, Archiv der Math. 74 (2000), 161–167.
- [17] C. S. Fisher, *The Death of a Mathematical Theory, a Study in the Sociology of Knowledge*, Archive for History of Exact Sciences 3 (1966/7), 137–159.
- [18] Leopold Flatto, *Invariants of Finite Reflection Groups*, L'Enseignement Mathématique 24 (1978), 237–292.
- [19] Peter Fleischmann, *The Noether Bound in Invariant Theory of Finite Groups*, Advances in Math. 156 (2000), 23–32.
- [20] Peter Fleischmann and Wolfgang Lempken, *On Degree Bounds for Invariant Rings of Finite Groups over Finite Fields*, pp. 33–41 in: Contemporary Mathematics 225, AMS, Providence RI, 1999.
- [21] John Fogarty, *On Noether's Bound for Polynomial Invariants of a Finite Group*, Electronic Research Announcements of the AMS 7 (2001), 5–7.
- [22] Adriano M. Garsia and Dennis Stanton, *Group Actions on Stanley–Reisner Rings and Invariants of Permutation Groups*, Advances in Math. 51 (1984), 107–201.
- [23] Carl Friedrich Gauss. *Demonstratio nova altera theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse*, Commentationes Göttingensis 3 (1816), reprinted in: *Werke 3. Band*, Königliche Gesellschaft der Wissenschaften, Göttingen 1876.
- [24] Manfred Göbel, *Computing Bases for Permutation Invariant Polynomials*, J. of Symbolic Computation 19 (1995), 285–291.
- [25] Paul Gordan, *Beweiss, dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist*, J. für die Reine und Angewandte Mathematik 69 (1868), 323–354.
- [26] Grete Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Annalen 95 (1926), 736–738.
- [27] David Hilbert, *Über die Theorie der Algebraischen Formen*, Math. Annalen 36 (1890), 473–534.
- [28] Ian Hughes and Gregor Kemper, *Symmetric Powers of Modular Representations, Hilbert Series and Degree Bounds*, Comm. in Algebra 28 (2000), 2059–2088.

- [29] Gordon James and Martin Liebeck, *Representations and Characters of Groups*, Cambridge Mathematical Textbooks, Cambridge University Press, Cambridge 1993
- [30] Dikran B. Karagueuzian and Peter Symonds, *The Module Structure of a Group Action on a Polynomial Ring: A Finiteness Theorem*, *J. of Algebra* 218 (1999), 672-692.
- [31] Gregor Kemper, *On the Cohen-Macaulay Property of Modular Invariant Rings*, *Journal of Algebra* 215 (1999), 330-351.
- [32] Gregor Kemper, *Loci in Quotients by Finite Groups, Pointwise Stabilizers and the Buchsbaum Property*, *J. Reine Angew. Math.* 547 (2002), 69-96.
- [33] Nelson Killius, *Some Modular Invariant Theory of Finite Groups with Particular Emphasis on the Cyclic Group*, talk at the Workshop on Computational Invariant Theory, IBFI, Dagstuhl, Germany 1996.
- [34] Felix Klein, *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert I, II*, Julius Springer Verlag, Berlin 1927.
- [35] Daniela Krause, *Die Noethersche Gradgrenze in der Invariantentheorie*, Diplomarbeit, University of Göttingen 1999.
- [36] Joseph Lagrange, *Recherches d'Arithmétique. Première partie*, Berl. Mém. 1773. reprinted in: *Oevres de Lagrange. tome troisième*, ed. by M. J.-A. Serret, Gauthier Villars, Paris 1869.
- [37] Sabine Meckbach, *Invarianten gewebeverstärkter Faser-Kunststoff-Verbunde*, preprint, Kassel 1997.
- [38] Wilhelm Franz Meyer, *Bericht über den gegenwärtigen Stand der Invariantentheorie*, *Jahresbericht der DMV* 1 (1892), 79-292.
- [39] Wilhelm Franz Meyer (ed.), *Enzyklopaedie der mathematischen Wissenschaften. Erster Band in 2 Teilen. Arithmetik und Algebra. Erster Teil*, B. G. Teubner Verlag, Leipzig 1898-1904.
- [40] Theodor Molien, *Über die Invarianten der linearen Substitutionsgruppen*, *Sitzungsber. König. Preuss. Akad. Wiss* (1897), 1152-1156.
- [41] Mara D. Neusel, *Invariants of some abelian p -Groups in Characteristic p* , *Proceedings of the AMS* 125 (1997), 1921-1931.
- [42] Mara D. Neusel, *The Invariants of the Symplectic Groups*, lecture notes, Appenzell 1998. (available at <http://hopf.math.purdue.edu>)
- [43] Mara D. Neusel, *Inverse Invariant Theory and Steenrod Operations*, *Memoirs of the AMS* 146, AMS, Providence RI. 2000.
- [44] Mara D. Neusel, *Localizations over the Steenrod Algebra. The lost Chapter*, *Mathematische Zeitschrift* 235 (2000), 353-378.
- [45] Mara D. Neusel, *Lots of Degree Bounds - or - On the Use of the \mathbf{T} -Functor in Invariant Theory*, preprint, Notre Dame 2000.
- [46] Mara D. Neusel and Müfit Sezer, *The Noether Map*, , preprint, Lubbock-Istanbul 2005.
- [47] Mara D. Neusel and Larry Smith, *Invariant Theory of Finite Groups*, *Mathematical Surveys and Monographs*, AMS, Providence RI 2002.
- [48] Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, *Mathematische Annalen* 77 (1916), 89-92.
- [49] Emmy Noether, *Invariante Variationsprobleme*, *Nachr. v. d. Ges. d. Wiss. zu Göttingen* (1918), 235-257. English Translation: *Invariant Variation Problems*, *Transport Theory Statist. Phys.* 1 (1971), No. 3, 186-207.
- [50] Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p* , *Nachr. v. d. Ges. d. Wiss. zu Göttingen* (1926), 28-35.
- [51] Peter J. Olver, *Classical Invariant Theory*, *London Math. Soc. Student Texts* 44, Cambridge University Press, Cambridge 1999.
- [52] Karen V. H. Parshall, *The One-Hundredth Anniversary of the Death of Invariant Theory?*, *The Mathematical Intelligencer* 12, No. 4 (1990), 10-16.

- [53] Victor Reiner, *On Göbel's Bound for Invariants of Permutation Groups*, Archiv der Math. 65 (1995), 475–480.
- [54] David R. Richman, *Invariants of Finite Groups over Fields of Characteristic p* , Advances in Math. 124 (1996), 25–48.
- [55] Gian-Carlo Rota, *Combinatorics, Representation Theory, and Invariant Theory: The Story of a ménage à trois*, Discrete Mathematics 193 (1998), 5–16.
- [56] Barbara J. Schmid, *Generating Invariants of Finite Groups*, C. R. Acad. Sci. Paris t. 308, Série I (1989), 1–6.
- [57] Barbara J. Schmid, *Finite Groups and Invariant Theory*, pp. 35–66 in: *Topics in Invariant Theory*, Séminaire d'Algèbre P. Dubriel et M.-P. Malliavin, Paris 1989/1990, Lecture Notes in Math. 1478, Springer-Verlag, Berlin, New York 1991.
- [58] Müfit Sezer, *Sharpening the Generalized Noether Bound in the Invariant Theory of Finite Groups*, J. of Algebra 254 (2002), 252-263.
- [59] Müfit Sezer, *Degree Bounds for Invariants of Certain Permutation Groups*, preprint, Purdue University 2002.
- [60] R. James Shank, *S.A.G.B.I. Bases for Rings of Formal Modular Seminvariants*, Comment. Math. Helv. 73 (1998), 548–565.
- [61] 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.
- [62] Neil J. A. Sloane, *Error-Correcting Codes and Invariant Theory: New Applications of a Nineteenth-Century Technique*, American Math. Monthly 84 (1977), 82–107.
- [63] Larry Smith, *Polynomial Invariants of Finite Groups*, second printing, A. K. Peters Ltd., Wellesley MA 1997.
- [64] Larry Smith, *Polynomial Invariants of Finite Groups: A Survey of Recent Developments*, Bulletin of the AMS 34 (1997), 211–250.
- [65] Larry Smith, *On a Theorem of Barbara Schmid*, Proceedings of the AMS 128 (2000), 2199–2201.
- [66] Larry Smith, *Lannes T-Functor and Invariants of Pointwise Stabilizers*, Forum Mathematicum 12 (2000), 461–476.
- [67] Larry Smith, *Homological Codimension of Modular Rings of Invariants and the Koszul Complex*, J. of Math. of Kyoto University 38 (1998), 727-747.
- [68] Richard P. Stanley, *Invariants of Finite Groups and their Applications to Combinatorics*, Bulletin of the AMS (3) 1 (1979), 475-511.
- [69] Stephen Wandzura and Hong Xiao, *Quadrature Rules on Triangles in \mathbb{R}^2* , research report, Yale University 1998.
- [70] Edward Waring, *Meditationes algebraicae, 3rd edition, 1782*, english translation by Dennis Wachs, American Math. Society, Providence RI 1991.
- [71] Hermann Weyl, *The Classical Groups*, second edition, Princeton University Press, Princeton 1946.

Mara D. Neusel

Department of Mathematics and Statistics, Texas Tech University, Mailstop 4-1042, Lubbock TX 79409, USA

mara.d.neusel@ttu.edu