The Curves Seminar at Queen's, Volume XII, in: Queen's Papers in Pure and Applied Math. **114** (1998), 5–26

Computational Invariant Theory

Gregor Kemper
IWR, Universität Heidelberg, Im Neuenheimer Feld 368
69 120 Heidelberg, Germany
email Gregor.Kemper@iwr.uni-heidelberg.de

February 10, 1998

Introduction

In the fall of 1997 I gave a series of lectures at Queen's University on algorithms in invariant theory of finite groups. This article is an expanded version of the material presented there. The main topic is the calculation of the invariant ring of a finite group acting on a polynomial ring by linear transformations of the indeterminates. By "calculation" I mean finding a finite system of generators for the invariant ring, and (optionally) determining structural properties of it. In this exposition particular emphasis is placed on the case that the ground field has positive characteristic dividing the group order. We call this the **modular case**, and it is important for several reasons. First, many theoretical questions about the structure of modular invariant rings are still open. I will address the problems which I consider the most important or fascinating in the course of the paper. Thus it is very helpful to be able to compute modular invariant rings in order to gain experience, formulate or check conjectures, and gather some insight which in fortunate cases leads to proofs. Furthermore, the computation of modular invariant ring can be very useful for the study of cohomology of finite groups (see Adem and Milgram [1]). This exposition also treats the non-modular case (characteristic zero or coprime to the group order), where computations are much easier and the theory is for the most part settled. There are also various applications in this case, such as the solution of algebraic equations or the study of dynamical systems with symmetries (see, for example, Gatermann [11], Worfolk [26]).

This is not a research paper, and so there is no claim of originality. In fact, most of the material is covered by the papers [14,15,18]. The goal is to give a coherent exposition of what is scattered through several original papers, which I hope is readable and assumes as little knowledge as possible.

There are several implementations of the algorithms treated in this text. The most efficient of these is contained in the Magma system (see Kemper and Steel [18] and Bosma et al. [6]). There is an older implementation in Maple written by myself, which can be obtained by anonymous ftp from the site `ftp.iwr.uni-heidelberg.de` under `/pub/kemper/INVAR2`. A further implementation in Singular has been written by Agnes Heydtmann (email `agnes@math.uni-sb.de`).

We will consider the following situation: K is a field, V is a finite dimensional vector space. Let $x_1, \ldots, x_n$ be a basis of V. Then we write $K[V]$ for the polynomial ring $K[x_1, \ldots, x_n]$ over K with the x_i as indeterminates. More conceptually, $K[V]$ can be defined as the symmetric algebra of V: $K[V] = S(V)$. Let $G \leq \mathrm{GL}(V)$ be a linear group on V. The action on V can be extended to an action of G on $K[V]$ by automorphisms of K-algebras. The invariant ring $K[V]^G$ is the set of all polynomials which are invariant under the action of G:

$$K[V]^G = \{f \in K[V] \mid \sigma(f) = f \ \forall \sigma \in G\}.$$

It is immediately clear that $K[V]^G$ is an algebra over K.

Example. Let $K = \mathbb{R}$, $V = \mathbb{R}^2$ and consider the orthogonal group $G = \mathrm{O}_2(\mathbb{R})$. Clearly $f_2 = x_1^2 + x_2^2$ is an invariant. Now take any invariant $f \in K[V]^G$. Then f must be constant on all orbits under G, i.e., under all circles about the origin. Hence f must be a function of the radius. This already makes it very plausible that f can be written as a polynomial in f_2, which is indeed the case for any invariant f. Hence $K[V]^G$ is generated by f_2 as an algebra over K.

Now consider the group $H \leq G$ generated by the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Clearly f_2 is an invariant under H, too, and we find additional invariants

$$f_4 = x_1^2 x_2^2 \quad \text{and} \quad g_4 = x_1 x_2 (x_1^2 - x_2^2).$$

It turns out that in this example $K[V]^H$ is generated by f_2, f_4, and g_4. We will see in the sequel how this can be seen.

In both examples finite generating systems of the invariant ring as a K-algebra were given. This is and has always been a classical goal of invariant theory. The question whether a finite system of generators always exists is known as Hilbert's 14th problem. The general answer turns out to be "no", as was shown by Nagata's counter example [19]. In fact, one has to assume that G is a reductive group in order to get the invariant rings of all representations of G to be finitely generated. This result was achieved by the combined effort of Hilbert [12], Nagata [20] and Popov [22]. In particular, all finite groups are reductive, and it was Noether [21] who already in 1926 gave a non-constructive proof that $K[V]^G$ is finitely generated if G is a finite group. In the following we will always restrict ourselves to the case of finite groups G. Our goal is to give algorithms to calculate a finite system of generators. We will follow a two-step approach, which consists of the computation of primary and secondary invariants. These are dealt with in Sections 2 and 3. Section 4 is devoted to the calculation of several properties of invariant rings. But first we have to see how invariants can be calculated at all.

1 Homogeneous components

The invariant ring $K[V]^G$ is not finite dimensional as a vector space over K. But we have a natural decomposition of $K[V]^G$ into its homogeneous components, which are finite dimensional and thus more accessible to computations: call a polynomial $f \in K[V]$ **homogeneous of degree** d if in all monomials of f the sum of the exponents is d. Equivalently, f is homogeneous of degree d if it lies in the d-th symmetric power $S^d(V)$ of V. The homogeneous polynomials of degree d form a vector space which we denote by $K[V]_d$ $(= S^d(V))$, and we have

$$K[V] = \bigoplus_{d \geq 0} K[V]_d.$$

The monomials of degree d are a basis of $K[V]_d$, hence $\dim(K[V]_d) = \binom{n+d-1}{n-1}$, where $n = \dim(V)$. Now observe that the action of G preserves the homogeneous components. Hence we also get a decomposition of the invariant ring

$$K[V]^G = \bigoplus_{d \geq 0} K[V]_d^G$$

into its homogeneous components. This section is devoted to the calculation of a basis of $K[V]_d^G$ for a given d. This is the most basic task in computational invariant theory, and often the bottle neck of the algorithms that are discussed later.

1.1 The linear algebra method.

Let $H \leq G$ be a subgroup of G whose invariants of degree d are known (typically, the trivial group), and take a set $S(G/H) \subseteq G$ such that H together with $S(G/H)$ generates G. Take the $|S(G/H)|$-fold direct sum of $K[V]$, whose components are indexed by the elements of $S(G/H)$, and consider the map

$$K[V]^H \to \bigoplus_{\sigma \in S(G/H)} K[V],\ f \mapsto (\sigma(f) - f)_{\sigma \in S(G/H)}.$$

The kernel of this map is $K[V]^G$. Moreover, the map is K-linear (in fact it is a homomorphism of modules over $K[V]^G$), and it preserves the grading. Restriction to the degree-d components yields a linear map $K[V]^H_d \to K[V]^{|S(G/H)|}_d$ whose kernel is $K[V]^G_d$. This mapping is explicitly given, so its kernel can be effectively calculated by solving a system of linear equations over K. In the case $H = 1$, the number of unknowns in this system is $\binom{n+d-1}{n-1}$, and the number of equations is $|S(G/H)| \cdot \binom{n+d-1}{n-1}$. This can become enormous for large values of n and d.

1.2 The Reynolds operator.

A further method to calculate the homogeneous component $K[V]^G_d$ is by means of the Reynolds operator, which is only available in the non-modular case. More generally, let $H \leq G$ be a subgroup such that the index $[G : H]$ is not divisible by the characteristic p of K. Then the *relative Reynolds operator* is defined as

$$\pi^G_H \colon K[V]^H \to K[V]^G,\ f \mapsto \frac{1}{[G:H]} \sum_{\sigma \in G/H} \sigma(f),$$

where G/H denotes a set of left coset representatives of H in G. This is independent of the choice of the coset representatives, and it is easily checked that π^G_H is a projection of modules over $K[V]^G$. In particular, the images under π^G_H of a basis of $K[V]^H_d$ generate the desired vector space $K[V]^G_d$. It is again a problem of linear algebra to select a basis of $K[V]^G_d$ from a generating set. In the non-modular case there is a choice between using the Reynolds operator or the linear algebra method to calculate homogeneous invariants. In Kemper and Steel [18], the authors analyzed the complexities of both approaches. The general tendency is that the Reynolds operator performs better for small $|G|$ and large d.

2 Homogeneous systems of parameters

The first strategic goal in the calculation of an invariant ring is the construction of a homogeneous system of parameters. This is best treated in the context of graded algebras. So suppose that R is a finitely generated **graded algebra** over K, i.e., R is a finitely generated commutative associative K-algebra with unity with a direct sum decomposition

$$R = \bigoplus_{d \geq 0} R_d$$

such that $R_i \cdot R_j \subseteq R_{i+j}$, and moreover $R_0 = K$. As explained in the previous section, invariant rings are graded algebras in this sense, and in fact the theory of graded algebras received much of its impetus from the study of invariant rings. It probably goes without saying that a nonzero element $f \in R_d$ is called **homogeneous** of degree d, written as $\deg(f) = d$. Moreover, we write $R_+ = \oplus_{d>0} R_d$ for the unique homogeneous maximal ideal of R. We will also consider graded R-modules, i.e., modules M over R with a direct sum decomposition

$$M = \bigoplus_{d \geq N} M_d$$

with $N \in \mathbb{Z}$ such that $R_i M_j \subseteq M_{i+j}$. The following version of Nakayama's lemma is of crucial importance.

Lemma 2.1. *Let R be a graded K-algebra and M a graded R-module. Then for a subset $S \subseteq M$ of homogeneous elements the following two conditions are equivalent:*

(a) S generates M as an R-module.

(b) S generates M/R_+M as a vector space over K. Here R_+M is the submodule of M generated by the elements $a \cdot g$ with $a \in R_+$.

In particular, a generating set S for M is of minimal cardinality if no proper subset of S generates M.

Proof. Clearly if S generates M, it also generates M/R_+M as a K-vector space.

Now suppose that S generates M/R_+M and let $g \in M$ be homogeneous of some degree d. Then by assumption

$$g = \sum_{i=1}^{m} \alpha_i g_i + \sum_{j=1}^{r} a_j h_j$$

with $g_1, \ldots, g_m \in S$, $\alpha_i \in K$, $a_j \in R_+$ and $h_j \in M$. By multiplying out homogeneous parts and omitting those summands which are not of degree d, we can assume that the a_j and h_j are homogeneous with $\deg(a_j h_j) = d$. Hence $\deg(h_j) < d$ and h_j lies in the submodule spanned by S by induction on d, which works since $\{N, N+1, N+2, \ldots\}$ is a well-ordered set. Hence g lies in the module spanned by S.

The last remark on minimality follows from the corresponding property of vector spaces. □

We write $\dim(R)$ for the Krull dimension of R.

Definition 2.2. *Let $n = \dim(R)$. A set $\{f_1, \ldots, f_n\} \subseteq R_+$ of homogeneous elements of positive degree is called a* **homogeneous system of parameters** *if R is finitely generated as a module over the subalgebra $A = K[f_1, \ldots, f_n]$ generated by the f_i.*

If $R = K[V]^G$ is an invariant ring, the members of a homogeneous system of parameters are also called **primary invariants**.

Note that $\dim(R)$ is the minimal number n such that $f_1, \ldots, f_n \in R$ can exist with the property that R is a finitely generated $K[f_1, \ldots, f_n]$-module, since this implies $\dim(R) = \dim(K[f_1, \ldots, f_n]) \leq n$. (A finite extension of a ring has the same dimension, see Eisenbud [9, Proposition 9.2].) We have equality if and only if $f_1, \ldots, f_n$ are algebraically independent over K. This shows that the elements of a homogeneous system of parameters are always algebraically independent, so $A = K[f_1, \ldots, f_n]$ is isomorphic to a polynomial ring. Using Lemma 2.1, we get the following geometric characterization, which is the key to all methods to construct homogeneous systems of parameters.

Proposition 2.3. *Let $f_1, \ldots, f_n \in R_+$ be homogeneous elements with $n = \dim(R)$. Then the following statements are equivalent:*

(a) $\{f_1, \ldots, f_n\}$ is a homogeneous system of parameters.

(b) $\dim(R/(f_1, \ldots, f_n)) = 0$.

(c) $\dim(R/(f_1, \ldots, f_i)) = n - i$ for $i = 1, \ldots, n$.

If $R = K[V]^G$ is the invariant ring of a finite group, then the above statements are equivalent to

(d) $\mathcal{V}_{\bar{K}}(f_1, \ldots, f_n) = \{0\}$, where $\mathcal{V}_{\bar{K}}(f_1, \ldots, f_n)$ is defined as $\{v \in \bar{K} \otimes_K V \mid f_i(v) = 0$ for $i = 1, \ldots, n\}$ and $\bar{K}$ is an algebraic closure of K.

We will try to give a proof here which uses only some very basic facts from commutative algebra. It is intertwined with the proof of the following:

Theorem 2.4 (Noether Normalization)**.** *If R is a finitely generated graded algebra, then a homogeneous system of parameters exists.*

Proof of Proposition 2.3 and Theorem 2.4. By Lemma 2.1, $\{f_1, \ldots, f_n\}$ is a homogeneous system of parameters if and only if the quotient algebra $R' := R/(f_1, \ldots, f_n)$ has finite dimension as a K-vector space. This is equivalent to the condition that $R'_d = 0$ for d sufficiently large, or that R'_+ is the radical ideal of the zero-ideal. This shows the equivalence of (a) and (b) in Proposition 2.3.

We prove Theorem 2.4 by induction on $n = \dim(R)$. If $n = 0$, then by the above the empty set is a homogeneous system of parameters. Suppose that $n > 0$ and let $P_1, \ldots, P_r$ be the associated prime ideals of the zero-ideal with $\dim(R/P_i) = n$. By the prime avoidance lemma (see Eisenbud [9, Lemma 3.3]), there exists a homogeneous element $f_1 \in R_+$ with $f_1 \notin P_i$ for all i, and it follows $\dim(R/(f_1)) < n$. Now the theorem follows by induction.

Clearly the statement (c) from Proposition 2.3 is stronger than (b), so we must show that it is also implied by (a) and (b). If fact, if $\{f_1, \ldots, f_n\}$ is a homogeneous system of parameters, then $R_i := R/(f_1, \ldots, f_i)$ is finitely generated as a module over $K[\overline{f_{i+1}}, \ldots, \overline{f_n}]$ where the bars denote the classes modulo $(f_1, \ldots, f_i)$, hence $m := \dim R_i \leq n - i$ by the remark after Definition 2.2. On the other hand, by Theorem 2.4 there exists a homogeneous system of parameters $\{\overline{g_1}, \ldots, \overline{g}_m\}$ in R_i, hence R is finitely generated over $K[f_1, \ldots, f_i, g_1, \ldots, g_m]$ and therefore $i + m \geq n$. With the above we obtain $\dim(R_i) = n - i$.

To prove the equivalence of (d), we first note that $K[V]$ is finitely generated as a module over $K[V]^G$. In fact, $f \in K[V]$ is a zero of the monic polynomial

$$\prod_{\sigma \in G} (X - \sigma(f)) \in K[V]^G[X].$$

It follows that $\{f_1, \ldots, f_n\} \subset K[V]^G_+$ is a homogeneous system of parameters for $K[V]^G$ if and only if it is a homogeneous system of parameters fro $K[V]$, which is equivalent to $\dim(K[V]/(f_1, \ldots, f_n)) = 0$, or $|\mathcal{V}_{\bar{K}}(f_1, \ldots, f_n)| < \infty$. The last condition is equivalent to (d), since if $\mathcal{V}_{\bar{K}}(f_1, \ldots, f_n)$ contains a nonzero point, it also contains the line joining this point and 0 by homogeneity. □

We can see now that in the example from the Introduction the invariants f_2 and f_4 form a homogeneous system of parameters. We note the following as a by-product of the above proof:

Proposition 2.5. *The polynomial ring $K[V]$ is finitely generated as a module over $K[V]^G$. In particular,*

$$\dim(K[V]^G) = \dim_K(V).$$

2.1 Dade's algorithm.

It is important to note that there are many choices of a homogeneous system of parameters. For example, one can substitute any member of a homogeneous system of parameters by a power of itself. As we will see in the next section, it is crucial for the efficiency of subsequent calculations that a homogeneous system of parameters is chosen whose degrees are as small as possible. In particular, one usually wants to minimize the product $\prod_{i=1}^n \deg(f_i)$ (see Propositions 3.1 and 4.1). An algorithm for the construction of a homogeneous system of parameters for $K[V]^G$ was given by Dade (see Stanley [25]). It is based on the following observation.

Proposition 2.6. *Let $n = \dim(V)$ and suppose that $l_1, \ldots, l_n \in V^* \setminus \{0\}$ are linear forms such that*

$$l_i \notin \bigcup_{\sigma_1, \ldots, \sigma_{i-1} \in G} \langle \sigma_1(l_1), \ldots, \sigma_{i-1}(l_{i-1}) \rangle_{K-\text{vector space}} \quad \text{for} \quad i = 2, \ldots, n.$$

Let f_i be the product over all l in the G-orbit of l_i, then $\{f_1, \ldots, f_n\}$ is a homogeneous system of parameters of $K[V]^G$.

Proof. We show that condition (d) from Proposition 2.3 is satisfied. Take $v \in \mathcal{V}_{\bar{K}}(f_1, \ldots, f_n)$. Then $(\sigma_i(l_i))(v) = 0$ for some $\sigma_i \in G$. But the assumption says that $\sigma_1(l_1), \ldots, \sigma_n(l_n)$ forms a basis of V^*, hence $v = 0$. □

It is clear how Proposition 2.6 can be turned into an algorithm, provided that the ground field K is large enough to make the avoidance of a union of at most $|G|^{n-1}$ proper subspaces possible. This algorithm is simple and quick, but the main drawback is that it tends to produce invariants whose degrees are of the same order of magnitude as $|G|$. For some experimental data on this see Kemper [15]. In that paper, various other approaches for the calculation of a homogeneous system of parameters are also explored, with the outcome that a computable criterion to decide whether a given degree vector $d_1, \ldots, d_n$ gives the degrees of some homogeneous system of parameters is required in order to obtain an algorithm which always produces an optimal homogeneous system of parameters.

2.2 An algorithm for optimal homogeneous systems of parameters.

The following provides a criterion for the existence of a homogeneous systems of parameters of given degrees.

Theorem 2.7 (Kemper [15]). *Let R be a graded algebra of Krull dimension n over an infinite field K and let $d_1, \ldots, d_k \in \mathbb{N} = \{1, 2, 3, \ldots\}$. Then the following are equivalent:*

(a) There exist homogeneous $f_1, \ldots, f_k \in R$ with $\deg(f_i) = d_i$ such that

$$\dim(R/(f_1, \ldots, f_k)) = n - k.$$

(b) For each subset $I \subseteq \{1, \ldots, k\}$ the inequality

$$\dim\left(R/(R_{d_i} \mid i \in I)\right) \leq n - |I|$$

holds. Here $(R_{d_i} \mid i \in I)$ denotes the ideal in R generated by the union of all homogeneous components R_{d_i} with $i \in I$.

The implication "(a) ⇒ (b)" also holds if K is a finite field.

Proof. First we prove that (a) implies (b). In fact, if $\dim(R/(f_1, \ldots, f_k)) = n - k$, then $f_1, \ldots, f_k$ can be extended to a homogeneous system of parameters by Theorem 2.4 and Proposition 2.3, hence Proposition 2.3(c) implies $\dim(R/(f_i \mid i \in I)) = n - |I|$ for any $I \subseteq \{1, \ldots, k\}$. But the ideal $(R_{d_i} \mid i \in I)$ is bigger than $(f_i \mid i \in I)$, and the inequality in (b) follows.

Now we prove the converse by induction on k. For $k = 0$, (a) is clearly satisfied. Assume $k > 0$ and write $d_R(I) = \dim\left(R/(R_{d_i} \mid i \in I)\right)$ for $I \subseteq \{1, \ldots, k\}$. Also write $\mathrm{Ass}_{min}(I)$ for the set of all associated prime ideals $P \subseteq R$ of $(R_{d_i} \mid i \in I)$ with $\dim(R/P) = n - |I|$. Then $\mathrm{Ass}_{min}(I)$ is a (possibly empty) finite set. For $I \subseteq \{1, \ldots, k-1\}$ and $P \in \mathrm{Ass}_{min}(I)$ we have $R_{d_k} \not\subseteq P$, since otherwise $(R_{d_i} \mid i \in I \cup \{k\}) \subseteq P$, so

$$d_R(I \cup \{k\}) \geq \dim(R/P) = n - |I| > n - |I \cup \{k\}|$$

in contradiction to (b). Therefore $R_{d_k} \cap P$ is a proper subspace of R_{d_k}. Hence by the infinity of K there exists $f_k \in R_{d_k}$ such that for all $I \subseteq \{1, \ldots, k-1\}$ and all $P \in \mathrm{Ass}_{min}(I)$ we have $f_k \notin P$. With $R' := R/(f_k)$, this implies that $d_{R'}(I) \leq n - |I| - 1$. In particular, $\dim(R') = n - 1$ (take $I = \emptyset$ and observe that f_k can be extended to a homogeneous system of parameters), hence the conditions in (b) hold for R' and $k' = k - 1$ and the proof is complete by induction. □

The purpose of Theorem 2.7 was to obtain an effective criterion for $d_1, \ldots, d_n$ to appear as the degrees of a homogeneous system of parameters, so now we explain how the conditions from (b) can be checked algorithmically in the case that $R = K[V]^G$. First, the ideals $(K[V]^G_{d_i} \mid i \in I) \subseteq K[V]^G$ for $I \subseteq \{1, \ldots, n\}$ can be calculated since K-bases for the subspaces $K[V]^G_{d_i}$ can be obtained by the methods of Section 1. Moreover, Proposition 2.5 implies that the dimension of an ideal $\mathcal{I} \subseteq K[V]^G$ equals the dimension of the ideal $(\mathcal{I}) \subseteq K[V]$ generated by $\mathcal{I}$ in $K[V]$. So we need an algorithm to compute dimensions of ideals $\mathcal{I} \subset K[V] = K[x_1, \ldots, x_n]$ in a polynomial ring. Such an algorithm is provided by Gröbner bases. Indeed, let B be a Gröbner basis of $\mathcal{I}$ with respect to any term order which refines the order given by the total degree. Then Becker and Weispfenning [4, Lemma 9.23 and Theorem 9.27] give a simple combinatorial procedure to calculate the dimension of $K[x_1, \ldots, x_n]/\mathcal{I}$: it is the maximal cardinality of a subset $I \subseteq \{x_1, \ldots, x_n\}$ such that every lead monomial of a polynomial from B involves a variable x_i which is not in I.

We obtain the following rough idea of an algorithm for the construction of a optimal homogeneous system of parameters.

(1) Loop through all degree vectors $(d_1, \ldots, d_n) \in \mathbb{N}^n$, ordered by rising values of $\prod_{i=1}^n d_i$, until one is found which satisfies the conditions in (b) of Theorem 2.7.

(2) Loop through all $f_1 \in R_{d_1}$ until f_1 is found such that $(d_2, \ldots, d_n)$ satisfies the conditions in (b) of Theorem 2.7, with R replaced by $R/(f_1)$.

(3) By recursion, obtain $f_2, \ldots, f_n$ of degrees $d_2, \ldots, d_n$ such that $f_1, \ldots, f_n$ is the desired homogeneous system of parameters.

(4) If the loop through R_{d_i} fails at some level in the recursion (which by Theorem 2.7 can only happen if K is finite), go back into the loop (1) and choose a new degree vector $(d_1, \ldots, d_n)$.

To make the algorithm more precise, one has to specify a procedure to enumerate the (possibly infinite) vector space R_{d_i} in such a way that for a nonzero polynomial f on R_{d_i} a vector is found after finitely many steps where f takes a nonzero value. For details, we refer to [15] and remark here that this is not a problem either in theoretical or in practical terms. While it is clear that the above algorithm terminates and produces a homogeneous system of parameters with a minimal degree product, it still appears quite appalling, since it involves up to 2^n Gröbner basis computations for the tests of the conditions from (b) of Theorem 2.7 for each degree vector, and a further minimum of 2^n Gröbner basis computations for the recursive construction of the f_i.

However, with a few modifications the algorithm becomes quite feasible. Most importantly, some strong and easily testable restrictions are applied on degree vectors before they are passed to the recursive loops. I will discuss such restrictions below (Section 2.3). Furthermore, in the recursive loops as few of the conditions from (b) of Theorem 2.7 as possible are applied. Thus a refined algorithm is obtained which is given in detail in [15]. I sometimes compare this refined algorithm to an assembly line which produces a package containing polynomials which eventually will become a homogeneous system of parameters. There are n workers and a foreman, and at the start the foreman chooses a degree vector $(d_1, \ldots, d_n)$ which satisfies the applicable restrictions. He hands a barrel containing the elements of R_{d_i} to the i-th worker, and the assembly starts with each worker tossing a random element f_i from his barrel into the package and shoving it down the line. Only the last worker performs the appropriate dimension test, and if it fails, he pushes the package back to his predecessor. Then each worker applies just enough conditions from (b) of Theorem 2.7 to find out whether the failure was his fault (i.e., the package could have traveled further down the line with a better choice of f_i), and in that case puts in a better f_i. Otherwise, he pushes the package back up. If the package travels back to the first worker and he decides that the failure was not due to him (namely, some condition from (b) of Theorem 2.7 on the degrees $(d_1, \ldots, d_n)$ was false), then the foreman has to choose new degrees d_i.

The justification for such an approach is that the subset of $R_{d_1} \times \cdots \times R_{d_n}$ consisting of those $(f_1, \ldots, f_n)$ which form a homogeneous system of parameters is Zariski-open, and that the restrictions on $(d_1, \ldots, d_n)$ yield a good chance that it is non-empty. Therefore the refined algorithm probabilistically only requires one Gröbner basis computation. The refined algorithm is implemented in Magma, and experience shows that it works quite well.

2.3 Hilbert series and restrictions on degree vectors.

Since R is assumed to be a finitely generated graded algebra, the K-dimension of each homogeneous component R_d is finite. The **Hilbert series** of R is the formal power series

$$H(R,t) = \sum_{d \geq 0} \dim_K(R_d) \cdot t^d \in \mathbb{C}[[t]].$$

Let $f_1, \ldots, f_n$ be a homogeneous system of parameters of degrees $d_1, \ldots, d_n$. We can calculate the Hilbert series of $A = K[f_1, \ldots, f_n]$ by using the fact that A is isomorphic to a polynomial ring, in other words, $A \cong K[f_1] \otimes_K \cdots \otimes_K K[f_n]$, and the fact that the Hilbert series is multiplicative with respect to tensor products. The result is

$$H(A,t) = \frac{1}{(1-t^{d_1}) \cdots (1-t^{d_n})}. \tag{2.1}$$

By looking at a free resolution of R as a module over A (see Section 4.3), we conclude that the Hilbert series of R can then be written as

$$H(R,t) = \frac{f(t)}{(1-t^{d_1}) \cdots (1-t^{d_n})} \quad \text{with} \quad f(t) \in \mathbb{Z}[t]. \tag{2.2}$$

Multiplying this by $(1-t)^n$ and substituting $t = 1$ yields the value $f(1)/(d_1 \cdots d_n)$, hence $H(R,t)$ has a pole at $t = 1$ of order at most n. Therefore we have a Laurent expansion

$$H(R,t) = \frac{a_0}{(1-t)^n} + \frac{a_1}{(1-t)^{n-1}} + \ldots$$

about $t = 1$, with $a_0 = f(1)/(d_1 \cdots d_n)$. Since $H(R,t)$ is coefficient-wise bounded from below by $H(A,t) = \prod_{i=1}^n (1-t^{d_i})^{-1}$, the coefficient a_0 must be nonzero. It is often called the **degree** of R, and written as $\deg(R) = a_0$. Since $f(1)$ is an integer, we have seen that the product $d_1 \cdots d_n$ is a multiple of $1/\deg(R)$. The degree of R is often known even if the Hilbert series is not. In the case that R is the invariant ring $K[V]^G$, we have $\deg(K[V]^G) = 1/|G|$ by Smith [24, Theorem 5.5.3]. We have obtained:

Proposition 2.8. *If $d_1, \ldots, d_n$ are the degrees of a homogeneous system of parameters of $K[V]^G$, then the product $d_1 \cdots d_n$ is divisible by $|G|$.*

This poses a restriction on the degrees $d_1, \ldots, d_n$ which is always applicable. A stronger restriction is obtained by using Equation (2.2) directly in cases where the Hilbert series is known. Indeed, picking the smallest d_i such that $H(R,t) \cdot \prod_{i=1}^n (1-t^{d_i})$ is a polynomial with integral coefficients often yields the actual degrees of a homogeneous system of parameters. In the non-modular case, one even knows that the coefficients of $f(t)$ are non-negative (see Equation (3.1) on page 10). Now if $R = K[V]^G$ and the characteristic of K is zero, then the Hilbert series can be calculated without touching a single invariant by Molien's marvelous formula

$$H(K[V]^G,t) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det(1-t\sigma)}. \tag{2.3}$$

Observe that this formula is even nicer than it looks at a first glance, since the expression $\det(1-t\sigma)$ only depends on the conjugacy class of σ in G (even in $\mathrm{GL}(V)$). In fact, Molien's formula can be evaluated from the knowledge of the character of the representation and the power maps of G alone. It is now time to look at an example.

Example 2.9.

(a) We consider the permutation group G of order 4 generated by $(1,2)(3,4)$ and $(1,4)(2,3)$ and its invariants over $K = \mathbb{Q}$. Molien's formula yields

$$H(K[V]^G, t) = \frac{1}{4}\left(\frac{1}{(1-t)^4} + \frac{3}{(1-t^2)^2}\right) = \frac{t^2-t+1}{(1-t)^2(1-t^2)^2} = \frac{1+t^3}{(1-t)(1-t^2)^3},$$

so $(1,2,2,2)$ is the smallest possible degree vector for primary invariants. Indeed, we find

$$f_1 = x_1 + x_2 + x_3 + x_4, \qquad f_2 = (x_1 - x_2 + x_3 - x_4)^2,$$
$$f_3 = (x_1 - x_2 - x_3 + x_4)^2, \quad f_4 = (x_1 + x_2 - x_3 - x_4)^2.$$

(b) Now take the abelian group G of order 8 generated by the matrices

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & i \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{C}).$$

This is an example of Stanley (see Sloane [23]). Molien's formula yields

$$H(K[V]^G, t) = \frac{1}{(1-t^2)^3},$$

so the degree vector $(d_1, d_2, d_3) = (2,2,2)$ meets the above restrictions and is minimal with that property. But $K[V]_2^G$ is generated by x_1^2, x_1x_2 and x_2^2, so we obtain the Krull dimension $\dim(K[V]^G/(K[V]_2^G)) = 1$. But the condition in Theorem 2.7(b) for $I = \{1,2,3\}$ is $\dim(K[V]^G/(K[V]_2^G)) \leq 3 - |I| = 0$, hence there are no primary invariants of degrees $(2,2,2)$. The degree vector with the second-lowest product is $(d_1, d_2, d_3) = (2,2,4)$, and here the algorithm readily finds primary invariants

$$f_1 = x_1^2, \quad f_2 = x_2^2, \quad f_3 = x_3^4.$$

As we have seen here and will see in the sequel, the knowledge of the Hilbert series is extremely helpful, so we ask for generalizations of Molien's formula. In the non-modular case ($\mathrm{char}(K)$ does not divide $|G|$), Molien's formula still holds, but we have to form the determinants in Equation (2.3) by Brauer-lifting the eigenvalues of $\sigma \in G$ to complex roots of unity. Moreover, if G acts as a permutation group on a basis of V, we can use Molien's formula by "pretending" that the representation is in characteristic 0. A common generalization is the case where V is a trivial source module. For details, we refer to Kemper [17]. In that paper, the so-called extended Hilbert series $\widetilde{H}(K[V], G, t)$ is also discussed. This is the formal power series whose coefficients are not the dimensions of $K[V]_d^G$ but the multiplicities of the trivial module K as a composition factor of $K[V]_d$. It is shown how $\widetilde{H}(K[V], G, t)$ can be calculated from the knowledge of the Brauer character table of G, and that Equation (2.2) holds for $\widetilde{H}(K[V], G, t)$ as well. Thus we get a similar restriction on the degrees of primary invariants in the modular case as well.

A further restriction which does not originate from the Hilbert series and is applicable in the general case of a finitely generated graded algebra R is the following. Suppose that $d_1, \ldots, d_n$ are the degrees of a homogeneous system of parameters $f_1, \ldots, f_n$, with $d_1 \leq \ldots \leq d_n$. For $d \in \mathbb{N}$ let $\mathcal{J}_d$ be the ideal in R generated by all components R_i with $1 \leq i \leq d$. Then

$$\dim(R/\mathcal{J}_{d_i}) \leq \dim(R/(f_1, \ldots, f_i)) = n - i,$$

hence

$$d_i \geq \min\{d \mid \dim(R/\mathcal{J}_d) \leq n - i\}. \tag{2.4}$$

This provides lower bounds for the degrees d_i, which in many cases turn out to be sharp. We will look at an example in Section 5.

3 Secondary invariants

In this section we assume that primary invariants $f_1, \ldots, f_n \in K[V]^G$ have been constructed, so $K[V]^G$ is generated by homogeneous invariants $g_1, \ldots, g_m$ as a module over $A = K[f_1, \ldots, f_n]$. Such generators g_i will be called **secondary invariants**. Together with the primary invariants, the g_i generate $K[V]^G$ as an algebra over K. It should be emphasized that neither primary nor secondary invariants are uniquely determined, and that being a primary or a secondary invariant is not an intrinsic property of an invariant. These notions merely describe the role of some invariants in a special choice of a generating system. This section is devoted to the task of finding secondary invariants. Looking for homogeneous generators of $K[V]^G$ as a module over A is equivalent to looking for generators of $K[V]^G/A_+K[V]^G$ as a vector space over K (Lemma 2.1). It follows that a system of secondary invariants which is minimal in the sense that no generator can be omitted is also minimal in the sense that it has minimal cardinality, and moreover the degrees of such a system is uniquely determined. We have entirely different algorithms for the modular and non-modular case.

3.1 The non-modular case

We assume that the characteristic of K is not a divisor of the group order $|G|$. As we shall see, this has several beneficial effects on the efficiency of our algorithms. First, the invariant ring is always **Cohen-Macaulay**, i.e., it is free as a module over $A = K[f_1, \ldots, f_n]$ (see Hochster and Eagon [13]). This property is independent of the choice of the homogeneous system of parameters. From the above remark, it follows that any system $g_1, \ldots, g_m$ of secondary invariants from which none can be omitted is a system of free generators. Let $e_1, \ldots, e_m$ be the degrees of the g_i. Then it follows from the additivity of the Hilbert series with respect to direct sums and from Equation (2.1) that

$$H(K[V]^G, t) = \frac{t^{e_1} + \cdots + t^{e_m}}{(1 - t^{d_1}) \cdots (1 - t^{d_n})}, \tag{3.1}$$

where as usual $d_i = \deg(f_i)$. Furthermore, we can easily calculate the Hilbert series by Molien's formula (2.3) (with a possible Brauer-lift). Thus comparing Equations (3.1) and (2.3) yields the complete information about the degrees of the secondary invariants! Also, comparing (3.1) and (2.2) shows that $f(1) = m$, hence $1/|G| = \deg(K[V]^G) = m/(d_1 \cdots d_n)$. We have proved:

Proposition 3.1. *If $K[V]^G$ is Cohen-Macaulay, then the (minimal) number of secondary invariants is $\prod_{i=1}^n \deg(f_i)/|G|$.*

In order to find the g_i most efficiently, we use Lemma 2.1 again. Let $g_1, \ldots, g_m \in K[V]^G$ be homogeneous invariants, with $m = \prod_{i=1}^n d_i/|G|$. Then the g_i are secondary invariants if and only if they generate $K[V]^G/A_+K[V]^G$ as a vector space over K. Since the number of g_i is correct, this is equivalent to the condition that the g_i are linearly independent modulo $A_+K[V]^G$. $A_+K[V]^G$ is the ideal in $K[V]^G$ generated by $f_1, \ldots, f_n$, but one cannot calculate with an ideal in $K[V]^G$ before $K[V]^G$ itself is known. To circumvent this problem, consider the map

$$K[V]^G \to K[V]/(f_1, \ldots, f_n),\ f \mapsto f + (f_1, \ldots, f_n),$$

where $(f_1, \ldots, f_n)$ is now an ideal in the polynomial ring $K[V]$. Clearly $A_+K[V]^G$ lies in the kernel. Conversely, an element f in the kernel has the form $f = h_1f_1 + \cdots + h_nf_n$, and applying the Reynolds operator π^G yields $f = \pi^G(f) = \pi^G(h_1)f_1 + \cdots + \pi^G(h_n)f_n \in A_+K[V]^G$. Therefore we have an embedding

$$K[V]^G/A_+K[V]^G \hookrightarrow K[V]/(f_1, \ldots, f_n),$$

and conclude that $g_1, \ldots, g_m$ are secondary invariants if and only if they are linearly independent modulo the ideal $\mathcal{I} := (f_1, \ldots, f_n)$ in $K[V]$. Now let B be a Gröbner basis of $\mathcal{I}$ with respect to any term order, and denote the normal form with respect to B by N_B. Such a Gröbner basis has

already been calculated in the process of finding the primary invariants f_i, so there is no extra cost involved. Then for $\alpha_1, \ldots, \alpha_m \in K$ we have

$$\alpha_1 g_1 + \cdots + \alpha_m g_m \in \mathcal{I} \quad \Longleftrightarrow \quad \alpha_1 N_B(g_1) + \cdots + \alpha_m N_B(g_m) = 0,$$

so all we have to do is check the linear independence of the normal forms of the g_i.

We arrive at the following algorithm:

(1) Let B be a Gröbner basis of the ideal $(f_1, \ldots, f_n) \subseteq K[V]$ generated by the primary invariants. (B was already calculated when the f_i were constructed.)

(2) Calculate the degrees $e_1, \ldots, e_m$ by using Molien's formula (2.3) and comparing to (3.1).

(3) For $i = 1, \ldots, m$ perform the following two steps:

(4) Calculate a basis of the homogeneous component $K[V]^G_{e_i}$ by using the methods from Section 1.

(5) Select an element g_i from this basis such that the normal form $N_B(g_i)$ lies outside the K-vector space generated by the polynomials $N_B(g_1), \ldots, N_B(g_{i-1})$.

(6) The invariants $g_1, \ldots, g_m$ are secondary invariants.

One further optimization can be achieved by trying to use products of secondary invariants of smaller degrees as new secondary invariants. This is very often successful and has two benefits: it can save the calculation of homogeneous components $K[V]^G_{e_i}$ for some large e_i, and it produces a minimal system of generators of $K[V]^G$ as an algebra over $A = K[f_1, \ldots, f_n]$ as a by-product.

Example 3.2.

(a) We can now finish the computation of the invariant ring from Example 2.9(a). From the Hilbert series we see that the secondary invariants are of degrees 1 and 3. Using the above algorithm yields secondary invariants

$$g_1 = 1, \quad g_2 = x_1^3 + x_2^3 + x_3^3 + x_4^3.$$

(b) In Aslaksen et al. [2], the authors considered the permutation representation on 6 symbols of the symmetric group $G = S_4$ given by $(1,4,6,3)(2,5)$ and $(2,4)(3,5)$. The ground field is $K = \mathbb{Q}$. Molien's formula yields

$$H(K[V]^G, t) = \frac{1 + t^3 + t^4 + t^5 + t^6 + t^9}{(1-t)(1-t^2)^2(1-t^3)^2(1-t^4)}.$$

Indeed, we find primary invariants of degrees 1,2,2,3,3,4. As secondary invariants we obtain

$$1,\ g_3,\ g_4,\ g_5,\ g_3^2,\ g_4 g_5,$$

where each g_i has degree i. Note that we only had to compute invariants of degrees up to 5. The complete computation takes about one second in Magma on a Sun workstation, and confirms the results from [2].

(c) A three-dimensional representation of the group $G = A_5$ over $K = \mathbb{R}$ is given by

$$(1,2,4) \mapsto \begin{pmatrix} 1 & (1+\sqrt{5})/2 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}, \quad (1,2,3,4,5) \mapsto \begin{pmatrix} -(1+\sqrt{5})/2 & -(1+\sqrt{5})/2 & 0 \\ 0 & 0 & -1 \\ (1+\sqrt{5})/2 & 1 & 1 \end{pmatrix}.$$

The Hilbert series is

$$H(K[V]^G, t) = \frac{1 + t^{15}}{(1-t^2)(1-t^6)(1-t^{10})},$$

and Magma finds primary invariants of degrees 2,6,10 and secondary invariants of degrees 0 and 15 in about half a second.

3.2 The modular case

Almost everything that we used in the non-modular case is missing in the modular case: the Cohen-Macaulay property fails in general, there is no Molien's formula and no Reynolds operator. Neither is there any a priori bound known on the degrees of secondary invariants. In that case, we have a completely different approach to the calculation of secondary invariants which is nevertheless very straightforward.

First, choose a subgroup $H \leq G$ with $\mathrm{char}(K) \nmid |H|$ (for example, the trivial group). Then use the algorithm from Section 3.1 to calculate (a minimal set of) secondary invariants $h_1, \ldots, h_r \in K[V]^H$ *with respect to the primary invariants* $f_1, \ldots, f_n$ *that were chosen for* G. Since $K[V]^H$ is Cohen-Macaulay, the h_i define an isomorphism $A^r \to K[V]^H$ between a free module of rank r over $A = K[f_1, \ldots, f_n]$ and the invariant ring of H. If we assign the degrees of the h_i to the free generators of A^r, this isomorphism becomes degree-preserving. Now take a set $S(G/H) \subseteq G$ which generates G together with H, and consider the map

$$K[V]^H \to \bigoplus_{\sigma \in S(G/H)} K[V], \ f \mapsto (\sigma(f) - f)_{\sigma \in S(G/H)},$$

whose kernel is $K[V]^G$ (see Section 1). Observe that this map is a homomorphism of A-modules. The polynomial ring is Cohen-Macaulay (take $\{x_1, \ldots, x_n\}$ as a homogeneous system of parameters), hence it is a free module over A whose rank is $\prod_{i=1}^n \deg(f_i)$ by Proposition 3.1. Hence $\oplus_{\sigma \in S(G/H)} K[V] \cong A^k$ with $k = |S(G/H)| \cdot \prod_{i=1}^n \deg(f_i)$ (often an enormous number). We obtain the following commutative diagram with exact rows, where the map $A^r \to A^k$ is defined by the commutativity and M is its kernel.

$$\begin{array}{ccccccc} 0 & \longrightarrow & K[V]^G & \longrightarrow & K[V]^H & \longrightarrow & \bigoplus_{\sigma \in S(G/H)} K[V] \\ & & \uparrow \wr & & \uparrow \wr & & \uparrow \wr \\ 0 & \longrightarrow & M & \longrightarrow & A^r & \longrightarrow & A^k \end{array} \tag{3.2}$$

Observe that each map in the diagram is a degree-preserving homomorphism of graded A-modules.

Suppose we can calculate generators for the module M. Then we will obtain secondary invariants as the images of these generators under the map $A^r \to K[V]^H$, which is given by the secondary invariants h_i of H. Now $A = K[f_1, \ldots, f_n]$ is isomorphic to a polynomial algebra, and $A^r \to A^k$ is a homomorphism of free modules over A. But there are standard techniques (involving Gröbner bases) to calculate kernels of such maps. We will give a brief account of how these techniques work, but before doing so let us summarize the algorithm for the computation of secondary invariants in the modular case.

(1) Choose a subgroup $H \leq G$ with $\mathrm{char}(K) \nmid |G|$ and calculate secondary invariants $h_1, \ldots, h_r \in K[V]^H$ for H with respect to the primary invariants $f_1, \ldots, f_n$ that were chosen for G. The h_i define a map $A^r \to K[V]^H$, where as usual $A = K[f_1, \ldots, f_n]$.

(2) Calculate generators for $K[V]$ as an A-module. These give a map $A^k \to \oplus_{\sigma \in S(G/H)} K[V]$, where $S(G/H) \subseteq G$ together with H generates G.

(3) Calculate the preimage under the map $A^k \to \oplus_{\sigma \in S(G/H)} K[V]$ of each $(\sigma(h_i) - h_i)_{\sigma \in S(G/H)}$ $(i = 1, \ldots, r)$. This is done by writing down a general element of A^k of degree equal to $\deg(h_i)$ with unknown coefficients, mapping it into $\oplus_{\sigma \in S(G/H)} K[V]$, equating to $(\sigma(h_i) - h_i)_{\sigma \in S(G/H)}$, and solving for the unknown coefficients. This is a system of inhomogeneous linear equations over K.

(4) The preimages calculated in step (3) define the map $A^r \to A^k$ from the diagram (3.2). Calculate generators of its kernel M using the method described below.

(5) Use linear algebra to omit generators of M which are redundant. By Lemma 2.1, this will result in a system of generators with minimal cardinality.

(6) Apply the map $A^r \to K[V]^H$ to the generators of M. The result is a set of minimal secondary invariants for $K[V]^G$.

The calculation of syzygy modules

Suppose that A is a polynomial ring in variables $t_1, \ldots, t_n$ and $\varphi\colon A^r \to A^k$ is a homomorphism between free A-modules, given by the images $v_1, \ldots, v_r$ of the free generators of A^r. We are interested in the kernel M of φ, which is also called the **syzygy module** of the v_i. We give a short summary of a technique for computing generators of M which can be found (with proofs) in Becker and Weispfenning [4, Section 6.1]. The first step is the calculation of a Gröbner basis of the submodule in A^k generated by the v_i. This requires some explanation: in A^k, a monomial is a vector with only one nonzero component which is a monomial in A in the usual sense. We can now fix a term order on the monomials in A^k (where usually precedence is given to the term in A over the position in the vector) and then talk about the leading monomial of a nonzero vector $v \in A^k$. Now a Gröbner basis is calculated by the usual Buchberger algorithm, with the modification that s-polynomials are only formed from vectors whose leading monomials "meet" at the same position in the vector.

So suppose that a Gröbner basis $w_1, \ldots, w_s \in A^k$ of the module generated by the v_i has been calculated. Then for a pair $i, j \in \{1, \ldots, s\}$ where the leading monomials of w_i and w_j meet, the s-polynomial has the normal form 0 with respect to $w_1, \ldots, w_s$, since this is a Gröbner basis. Therefore we have an equation

$$\operatorname{spoly}(w_i, w_j) - \sum_{\nu=1}^{s} a_\nu w_\nu = 0$$

with $a_\nu \in A$, i.e., we have a syzygy $r_{i,j} \in A^s$ of the w_i. Let R be the set of all syzygies obtained in this way. It can be shown that R generates the syzygy module of the w_i. But we are interested in the syzygies of the v_i, and this requires a further step.

Since the w_i and the v_i generate the same submodule of A^k, there exist matrices $C \in A^{s\times r}$ and $D \in A^{r\times s}$ such that

$$\begin{pmatrix} w_1 \\ \vdots \\ w_s \end{pmatrix} = C \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix} = D \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_s \end{pmatrix}.$$

The matrix C can be obtained by tracing the formation of the w_i during the Buchberger algorithm, and D is computed by taking the normal forms of the v_i with respect to $w_1, \ldots, w_s$ (which are 0) and keeping track of the coefficients. Now usually DC is not the identical matrix I_r, but we have

$$(DC - I_r) \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix} = 0.$$

Hence the rows of $DC - I_r$ give a set R' of syzygies of the v_i. Finally, the union

$$R' \cup \{(a_1 \ldots a_s) \cdot C \mid (a_1 \ldots a_s) \in R\}$$

is the desired generating set of the syzygy module M of the v_i (see Becker and Weispfenning [4, Theorem 6.4]). So again the hard work lies in the computation of a Gröbner basis.

Returning to the algorithm for the computation of secondary invariants in the modular case, it is worth noting that in many examples the linear algebra involved in step (3) is much more expensive than the calculation of the syzygy module in step (4).

Example 3.3. We look at two examples now.

(a) Let G be the permutation group of order 2 on 6 symbols, generated by $(1,2)(3,4)(5,6)$, and take K to be $\mathbb{F}_2$. Denote the variables of $K[V]$ by $x_1, y_1, x_2, y_2, x_3, y_3$, so the action of G is by exchanging x_i and y_i. We find primary invariants

$$x_i + y_i \quad \text{and} \quad x_i y_i \quad (i = 1, 2, 3).$$

Using the above algorithm, Magma finds the following minimal set of secondary invariants:

$$1, \quad x_i y_j + x_j y_i \quad (1 \le i < j \le 3) \quad \text{and} \quad x_1 x_2 x_3 + y_1 y_2 y_3.$$

The complete computation takes less than 1/10 seconds. Note that in this example the number of secondary invariants (5) exceeds the product of the degrees of the primary invariants divided by the group order (4), hence by Proposition 3.1 $K[V]^G$ is not Cohen-Macaulay.

(b) Let G be the 3-modular reduction of the Weyl group of type H_4. This is a subgroup of order 14 400 of $\mathrm{GL}_4(\mathbb{F}_9)$. We will calculate the invariant ring of this group in Section 5. Here we look at a p-Sylow subgroup P of G, for $p = 3$. P has order 9 and can be generated by the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ w+1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ w & 0 & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ w & -w & w & 1 \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_9),$$

where $w^2 - w - 1 = 0$. The computation of primary and secondary invariants by Magma takes about 4 seconds. The result are primary invariants of degrees 1,2,3,9 and secondary invariants of degrees 0,3,4,7,8,11. In this example, the number of secondary invariants equals $\prod_{i=1}^{n} \deg(f_i)/|G|$. As we will see in Proposition 4.1, this means that $K[V]^G$ is Cohen-Macaulay.

4 Properties of the invariant ring

One of the main reasons for computing invariant rings is that one wants to study their structural properties. This is especially interesting in the modular case, where many theoretical questions are still open, and computations help to gain experience, counter examples, ideas for conjectures and in fortunate cases also for proofs. In this section we will see how most interesting properties of invariant rings can easily be extracted from the data which are available after the calculation of primary and secondary invariants. The first three subsections concern only the modular case, and the last two are also interesting in the non-modular case.

4.1 The Cohen-Macaulay property

We have already seen that in the non-modular case all invariant rings of finite groups are Cohen-Macaulay, and we have seen an example in the modular case where $K[V]^G$ is not Cohen-Macaulay (Example 3.3(a)). In that example, we used Proposition 3.1, and we will now explain why the converse of this proposition also holds. Indeed, the polynomial ring $K[V]$ is Cohen-Macaulay, and so by Proposition 3.1 it is a free module of rank $d = \prod_{i=1}^{n} d_i$ over $K[f_1, \ldots, f_n]$, where the f_i are primary invariants and the d_i their degrees. Hence $K(V)$, the field of fractions of $K[V]$, is a vector space of dimension d over the rational function field $K(f_1, \ldots, f_n)$ generated by the f_i. The invariant field $K(V)^G$ is an intermediate field between $K(f_1, \ldots, f_n)$ and $K(V)$, and the index $[K(V) : K(V)^G]$ is equal to $|G|$ by Galois theory. Hence $[K(V)^G : K(f_1, \ldots, f_n)] = d/|G|$. (This

provides another proof of the fact that $|G|$ divides the degree product of the primary invariants, which we used in Section 2.) Now it is easily seen that a system of secondary invariants always generates $K(V)^G$ as a vector space over $K(f_1, \ldots, f_n)$, hence such a system must have at least $d/|G|$ elements, and more than $d/|G|$ will be linearly dependent over $K[f_1, \ldots, f_n]$. Thus we have proved:

Proposition 4.1. *Let m be the minimal number of secondary invariants with respect to primary invariants of degrees $d_1, \ldots, d_n$. Then*

$$m \geq \frac{d_1 \cdots d_n}{|G|},$$

and equality holds if and only if $K[V]^G$ is Cohen-Macaulay.

This provides a criterion which involves no further computations at all to check the Cohen-Macaulay property. For example, we see that the invariant ring in Example 3.3(b) is Cohen-Macaulay.

Experience so far seems to suggest that "most" modular invariant rings are not Cohen-Macaulay. Several classes of linear groups whose invariant rings are not Cohen-Macaulay are given in Kemper [16]. For example, if the characteristic p of K divides $|G|$ and the rank of $\sigma - 1$ is sufficiently large for all elements $\sigma \in G$ of order p, then $K[V]^G$ is not Cohen-Macaulay.

4.2 Free resolutions and depth

If the invariant ring is not Cohen-Macaulay, then there are linear relations between the secondary invariants with coefficients in the algebra $A = K[f_1, \ldots, f_n]$ generated by the primary invariants. The methods to deal with them apply in the more general situation of graded algebras. So as in Section 2, let R be a finitely generated graded algebra over $R_0 = K$, and let $A = K[f_1, \ldots, f_n]$ be the subalgebra generated by a homogeneous system of parameters. Assume that, as in Section 3.2, we have calculated R as a module over A by giving generators of a submodule $M \subseteq A^r$ which is isomorphic to R (see diagram 3.2). Then to calculate relations over A between the generators is again the computation of a syzygy module. Indeed, giving m generators for $M \subseteq A^r$ is the same as giving a homomorphism $A^m \to A^r$ whose image is $M \cong R$. But we saw in Section 3.2 how kernels of such maps can be calculated. So let $S \subseteq A^m$ be the kernel, then we have an exact sequence $0 \to S \to F_0 \to R \to 0$, where we have written F_0 for the free module A^r to get a more convenient notation. Since all maps are degree-preserving, S is a graded module, hence by Lemma 2.1, a generating system for S of minimal cardinality can be obtained by deleting superfluous generators. Now we can continue in the same way and calculate minimal relations between the generators of S, which leads to an exact sequence $0 \to S' \to F_1 \to F_0 \to R \to 0$. By Hilbert's syzygy theorem (see, for example, Benson [5, Theorem 4.2.2]), this process stops after at most n steps, so we will finally arrive at an exact sequence of graded A-modules with degree-preserving maps

$$0 \longrightarrow F_l \longrightarrow \ldots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow R \longrightarrow 0, \tag{4.1}$$

where the F_i are all free modules. Such a sequence is called a **minimal free resolution** of R. The length l does not depend on the choice of the generators of the various kernels, as can be seen by applying Lemma 2.1. It requires some commutative algebra to show that l does not even depend on the choice of the homogeneous system of parameters (see Benson [5, Section 4.4]). The value l is called the **homological dimension** of R. Thus R is Cohen-Macaulay if and only if the homological dimension is zero, so it is fair to say that the homological dimension measures the deviation from being Cohen-Macaulay. Another invariant of R which is closely related to the homological dimension is its depth. Indeed, by the formula of Auslander and Buchsbaum (see Benson [5, Theorem 4.4.4]), we have

$$\operatorname{depth}(R) = n - l.$$

For all that matters here, this can be taken as the definition of the depth. Originally, the depth is defined as the maximal length of a regular sequence in R, i.e., a sequence $f_1, \ldots, f_d \in R_+$ of homogeneous elements such that f_i is not a zero divisor on $R/(f_1, \ldots, f_{i-1})$, for all $i = 1, \ldots, d$.

So we have seen that the depth of invariant rings of finite groups can be calculated algorithmically. Experience shows that this is an easy task compared to the bulk of work that goes into the calculation of primary and secondary invariants. There are few general results known about the depth of modular invariant rings. The paper of Ellingsrud and Skjelbred [10] gives a formula for the depth in the case of cyclic p-groups, where $p = \mathrm{char}(K)$. Recently Campbell et al. [8] found a generalization and an elementary proof of this formula. For example, the invariant ring considered in Example 3.3(a) has depth 5 and hence homological dimension 1.

4.3 The Hilbert series

If we have an exact sequence of finite dimensional vector spaces starting and ending with 0, then the dimension formula says that the alternating sum of the dimensions is zero. Hence the same is true if we consider graded modules and their Hilbert series. So from (4.1) we obtain

$$H(R,t) = \sum_{i=0}^{r} (-1)^i H(F_i, t).$$

Observe that the free generators of F_i must be of the right degrees to make the maps in (4.1) degree-preserving. If these degrees are $e_{i,1}, \ldots, e_{i,s_i}$, then

$$H(F_i,t) = (t^{e_{i,1}} + \cdots + t^{e_{i,s_i}}) \cdot H(A,t) = \frac{t^{e_{i,1}} + \cdots + t^{e_{i,s_i}}}{(1-t^{\deg(f_1)}) \cdots (1-t^{\deg(f_n)})}$$

(see Equation (2.1)).

Another method to calculate the Hilbert series of an invariant ring appears by considering diagram 3.2 again. If $N \subseteq A^k$ is the image of the map $A^r \to A^k$, then

$$H(K[V]^G, t) = H(A^r, t) - H(N, t) = H(A^r, t) - H(A^k, t) + H(A^k/N, t).$$

But $H(A^r, t)$ and $H(A^k, t)$ are known, and $H(A^k/N, t)$ can be computed by a combinatorial algorithm (Bayer and Stillman [3]) from a Gröbner basis of N. Now fortunately a Gröbner basis of N has already been calculated as the first step in the syzygy calculation leading to M.

One reason why it is interesting to know the Hilbert series of a graded algebra R is that one can use it to check the so-called Gorenstein property: R is **Gorenstein** if and only if it is Cohen-Macaulay and the Hilbert series satisfies

$$H(R, 1/t) = (-1)^{\dim(R)} t^l \cdot H(R,t)$$

for some $l \in \mathbb{Z}$. For example, the invariant rings in Example 3.2(a)–(c) and Example 3.3(b) are Gorenstein.

4.4 Minimal algebra-generators and β

Let R be a graded algebra over $R_0 = K$ and $g_1, \ldots, g_r \in R_+$ homogeneous. Then it is seen as in the proof of Lemma 2.1 that $g_1, \ldots, g_r$ generate R as an algebra over K if and only if they generate the ideal $R_+ \subseteq R$. Moreover, by Lemma 2.1 this is equivalent to the condition that the images of the g_i generate the quotient R_+/R_+^2 as a vector space over K. Hence a homogeneous system of algebra generators has minimal cardinality if no generator is superfluous, and then the number and degrees of the generators are uniquely determined. In particular the maximal degree $\beta(R)$ of a generator is well defined. One also sees that $\beta(R)$ remains unchanged under extensions of the ground field,

i.e., if we pass from R to $R \otimes_K L$ for $L \geq K$ a field extension. Equivalently, $\beta(R)$ is the minimal number d such that R is generated as a K-algebra by homogeneous elements of degrees $\leq d$.

It is clear that the invariant ring $K[V]^G$ is generated as a K-algebra by the primary and secondary invariants. Although the secondary invariants are minimal module-generators, they are not minimal algebra-generators. For example, 1 is always a secondary invariant, but it is redundant as an algebra-generator. To test whether a given generator f within a system S of homogeneous algebra-generators is redundant is a linear algebra problem. The procedure is to set up a general element of the same degree as f in the algebra generated by $S \setminus \{f\}$ with unknown coefficients, equating to f and extracting the corresponding system of linear equations by comparison of coefficients. The system is solvable if and only if f can be omitted from S. Starting with S as the union of the primary and secondary invariants, one thus gets a minimal system of algebra-generators, and by the above, $\beta(K[V]^G)$ is its maximal degree.

Example 4.2. In Example 3.2, we have $\beta(K[V]^G) = 3, 5, 15$ in part (a),(b),(c), respectively. In Example 3.3(a), it is easily checked that the secondary invariant $x_1x_2x_3+y_1y_2y_3$ cannot be expressed in terms of invariants of lower degree, hence $\beta(K[V]^G) = 3$. This shows that Noether's degree bound (which says that $\beta(K[V]^G) \leq |G|$ if $\mathrm{char}(K) > |G|$) does not hold in the modular case. In Example 3.3(b), we obtain minimal algebra generators of degrees 1,2,3,3,4,9, so the secondary invariants of degrees 7,8,11 are redundant. We obtain $\beta(K[V]^G) = 9 = |G|$, which confirms a conjecture made by the author that Noether's degree bound holds if the invariant ring is Cohen-Macaulay.

4.5 Syzygies

Suppose we have generators $h_1, \ldots, h_r$ of a K-algebra R. Then we have a presentation of R if we know the kernel $\mathcal{I}$ of the map

$$\Phi\colon K[t_1, \ldots, t_r] \to R,\ t_i \mapsto h_i,$$

where the t_i are indeterminates. It is one of the basic tasks in invariant theory to compute generators of $\mathcal{I}$ as an ideal in the polynomial ring $K[t_1, \ldots, t_r]$. The elements of $\mathcal{I}$ are usually called **syzygies**. When we were talking about syzygies in the preceding sections of this text, we meant elements in the kernel of a map of modules, not algebras. But in fact we deal with a special case here, since R becomes a module over $K[t_1, \ldots, t_r]$ via Φ, and then Φ is a module-homomorphism. We have shown how kernels of maps between free modules over a polynomial ring can be computed. But here the situation is different since R is usually not free, so we need different methods. Before explaining them, we remark that if R is a graded algebra and the h_i are homogeneous, then $\mathcal{I}$ becomes a homogeneous ideal if we set $\deg(t_i) = \deg(h_i)$.

The Gröbner basis method

Suppose now that $R \subseteq K[x_1, \ldots, x_n]$ is a subalgebra of a polynomial ring. Then the standard method to calculate syzygies is the following. Form the ideal

$$\mathcal{J} = (h_1 - t_1, \ldots, h_r - t_r) \subseteq K[x_1, \ldots, x_n, t_1, \ldots, t_r]$$

and calculate a Gröbner basis B of $\mathcal{J}$ with respect to a term order with the property that x_i is greater than any monomial in the t_j's for $i = 1, \ldots, n$. For example, one can use the lexicographical term order with $x_1 > \ldots > x_n > t_1 > \ldots > t_r$. Then it is easy to see that the intersection $B_{\mathbf{t}} = B \cap K[t_1, \ldots, t_r]$ generates the desired ideal $\mathcal{I} = \ker(\Phi)$ (see Becker and Weispfenning [4, Proposition 6.15]). If the h_i are homogeneous polynomials, then the syzygies in $B_{\mathbf{t}}$ are also homogeneous (with the proper choice of degrees of the t_i), since the Buchberger algorithm preserves homogeneity. Hence by Lemma 2.1 one obtains a generating set for $\mathcal{I}$ of minimal cardinality by omitting superfluous generators from $B_{\mathbf{t}}$. This can be done by the usual linear algebra methods.

The linear algebra method

Now we make the more restrictive assumption that R is a graded algebra and that the set $\{h_1, \ldots, h_r\}$ is the union of a homogeneous system of parameters $\{f_1, \ldots, f_n\}$ and a generating set $\{g_1, \ldots, g_m\}$ of R as a module over $A = K[f_1, \ldots, f_n]$. This is the situation that we have after primary and secondary invariants have been calculated. Since the f_i are algebraically independent, we are looking for the kernel $\mathcal{I}$ of the map

$$A[t_1, \ldots, t_m] \to R, \ t_i \mapsto g_i,$$

where the t_i are again indeterminates. Suppose that $S \subseteq \mathcal{I}$ is a set of relations containing

(a) generators for the A-module $\mathcal{I} \cap (\oplus_{i=1}^m A \cdot t_i)$ of A-linear relations between the g_i, and

(b) for each $1 \leq i \leq j \leq m$ a relation of the form $t_i t_j - f_{i,j}$ with $f_{i,j} \in \oplus_{k=1}^m A \cdot t_k$.

Then it is easy to show that S generates $\mathcal{I}$ (see Kemper and Steel [18, Proposition 12]). In other words, all that we have to know are the linear relations between the g_i with coefficients in A and the representation of each product $g_i g_j$ as an element of $\oplus_{k=1}^m A \cdot g_k$. We explained in Section 4.2 how the linear relations can be calculated. The representation of a product $g_i g_j$ or, more generally, a homogeneous element $f \in R$ of degree d, say, as an element of $\oplus_{i=1}^m A \cdot g_i$ can be calculated by equating f to a general element of $\oplus_{i=1}^m A \cdot g_i$ of degree d with unknown coefficients and solving the resulting inhomogeneous system of linear equations over K. This approach usually performs better than the Gröbner basis method. Nevertheless, the computation of relations can sometimes be quite expensive.

It is often important to obtain a *minimal* system of generators for the ideal $\mathcal{I}$. If R is a graded algebra, Lemma 2.1 applies again and tells us that it is enough to omit superfluous generators. If the linear algebra method is used, one can go a bit further by detecting superfluous relations even before calculating them: it is quite easy to decide whether the ideal generated by the relations that have already been computed at some point contains a relation giving the desired representation for a product $g_i g_j$. In fact, this again comes down to the solution of a system of linear equations.

R is said to be a **complete intersection** if the minimal number of generators of $\mathcal{I}$ is $r - \dim(R)$, where r is the number of algebra-generators of R and $\dim(R)$ is the Krull dimension. In other words, the dimension of the variety $\mathcal{V}_{\bar{K}}(r_1, \ldots, r_i)$ decreases by 1 with each new generating relation r_i as it enters into the ideal. If R is graded, then this property is independent of the choice of the generators and of the minimal generating relations. In Example 3.2(a) and (c) the invariant rings are complete intersections.

5 Using ad hoc methods

It often happens in "real life" situations that the algorithms given in the above sections require too much time or memory to be feasible anymore. Then one has to put ones hope in ad hoc methods, which in some cases work and produce the invariant ring, and depend on a mixture of experience, luck and naive optimism. In order to give a feeling of some of the methods that can be applied, we look at an example of a linear group for which the standard algorithms fail. This group G is the 3-modular reduction of the Weyl group of type H_4 of order 14 400. G is a subgroup of $\mathrm{GL}_4(\mathbb{F}_9)$ and can be generated by the full permutation group S_4 together with the matrices

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -1 & -1 & \zeta^2 \\ -1 & 0 & -1 & \zeta^2 \\ -1 & -1 & 0 & \zeta^2 \\ \zeta^2 & \zeta^2 & \zeta^2 & -1 \end{pmatrix},$$

where $\zeta \in \mathbb{F}_9$ is an element of order 8. G is a group generated by reflections, but since its order is a multiple of the characteristic of K, the invariant ring need not be isomorphic to a polynomial ring. In Example 3.3(b) we have calculated the invariant ring of a p-Sylow subgroup of G, for $p = 3$, and seen that this invariant ring is Cohen-Macaulay. It follows by a theorem of Campbell et al. [7] that the invariant ring $K[V]^G$ of G is also Cohen-Macaulay. In order to compute it, we first need to find primary invariants.

5.1 Finding primary invariants

We first use the inequality (2.4) to get an idea of the degrees d_i that primary invariants can have. The computation of the homogeneous components $K[V]_d^G$ is feasible up to degrees around $d = 40$, and (2.4) yields

$$d_1 \geq 2,\ d_2 \geq 10, \quad \text{and} \quad d_3 \geq 36$$

but no information on the last degree d_4. By trying random invariants f_2, f_{10}, f_{36} of degrees 2, 10 and 36 we are lucky enough to arrive at an ideal (f_2, f_{10}, f_{36}) of dimension 1, so there is only one further primary invariant missing. We have

$$f_2 = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad f_{10} = x_1^{10} + x_2^{10} + x_3^{10} + x_4^{10},$$

but f_{36} is much more complicated. By Proposition 3.1 the degree d_4 of the missing primary invariant must be a multiple of $|G|/(d_1 d_2 d_3) = 20$. We already know that $d_4 > 20$, and we rule out the possibility $d_4 = 40$ by using (2.4) again. So our hope is that we will find a last primary invariant f_{60} of degree 60. However, it is impossible due to time and storage problems to compute all invariants of degree 60. Instead, we try to construct f_{60} by using Steenrod operations.

Steenrod operations are a very helpful tool in modular invariant theory, and we explain their definition by following Smith [24]. Suppose $K = \mathbb{F}_q$ is a finite field. Then we take an additional indeterminate T and define a homomorphism $P\colon K[V] \to K[V][T]$ of K-algebras by sending x_i to $x_i + x_i^q \cdot T$. It is easily checked that P commutes with the action of $\mathrm{GL}(V)$ on $K[V]$. For $f \in K[V]$, write

$$P(f) = \sum_{i \geq 0} \mathcal{P}^i(f) \cdot T^i.$$

Then $\mathcal{P}^i(f)$ is the i-th Steenrod operation of f. It follows from the $\mathrm{GL}(V)$-compatibility of P than Steenrod operations of invariants are again invariants. It is also easy to check that for a homogeneous f

$$\deg(\mathcal{P}^i(f)) = \deg(f) + i(q-1)$$

if $\mathcal{P}^i(f)$ is nonzero, and $\mathcal{P}^i(f) = 0$ if $i > \deg(f)$.

We continue the construction of primary invariants. First note that $f_{10} = -\mathcal{P}^1(f_2)$. Now $f_{60} = \mathcal{P}^3(f_{36})$ has the desired degree 60, and indeed we are lucky enough to find that the ideal generated by f_2, f_{10}, f_{36} and f_{60} has dimension 0. Thus a complete system of primary invariant is found.

5.2 Finding secondary invariants

Since we know that $K[V]^G$ is Cohen-Macaulay, the number of secondary invariants must be $d_1 d_2 d_3 d_4/|G| = 3$ by Proposition 3.1. However, it is impossible to run the standard algorithm given in Section 3.2 for this group, and it is a very hard calculation to produce the secondary invariant by linear algebra methods. Instead we choose another approach. The first secondary invariant is always $g_1 = 1$. Now we consider the dimensions of the homogeneous components $K[V]_d^G$ and compare them to the dimensions of A_d, where $A = K[f_2, f_{10}, f_{36}, f_{60}]$. This way, we find that $d = 22$ is the first degree where these dimensions differ, hence there exists an invariant $g_{22} \in K[V]^G \setminus A$ of degree 22, which is the second secondary invariant. It is quite easy to find such a g_{22} by linear

algebra, but g_{22} is too long to be printed here. Now we are optimistic and guess that the third (and last) secondary invariant is g_{22}^2. Assuming that this is true, we must have $g_{22}^3 \in A + A \cdot g_{22} + A \cdot g_{22}^2$. Indeed we quickly find the relation

$$g_{22}^3 + (f_2^{11} - f_2 f_{10}^2) g_{22}^2 + (f_2^{17} f_{10} - f_2^7 f_{10}^3 - f_2^{12} f_{10}^2 + f_2^4 f_{36} + f_2^2 f_{10}^4) g_{22} + \\ + f_2^{18} f_{10}^3 - f_2^{28} f_{10} + f_{10}^3 f_{36} + f_2^{15} f_{36} - f_2^{13} f_{10}^4 - f_2^5 f_{10}^2 f_{36} + f_2^8 f_{10}^5 - f_2^3 f_{60} = 0 \quad (5.1)$$

by linear algebra. Let $R = K[f_2, f_{10}, f_{36}, f_{60}, g_{22}]$ be the K-algebra generated by $f_2, f_{10}, f_{36}, f_{60}$ and g_{22}, then we claim that $K[V]^G = R$. We will use the following proposition for this purpose.

Proposition 5.1. *Suppose that $R \leq K[V]^G$ is a subalgebra of an invariant ring of a finite group. Then $R = K[V]^G$ if and only if the following three conditions hold:*

(a) The field of fractions $\mathrm{Quot}(R)$ *of R coincides with the invariant field $K(V)^G = \mathrm{Quot}(K[V]^G)$,*

(b) $K[V]^G$ is integral over R, and

(c) R is integrally closed (in its field of fractions).

Proof. First suppose that $R = K[V]^G$. Then clearly $\mathrm{Quot}(R) = \mathrm{Quot}(K[V]^G)$, hence (a) and (b) hold. Furthermore, if $f \in K(V)^G$ is integral over $R = K[V]^G$, then f is also integral over $K[V]$, hence $f \in K[V]$ since polynomial rings are integrally closed. It follows that $f \in K(V)^G \cap K[V] = K[V]^G$. Hence R is also integrally closed.

Now suppose that (a)–(c) hold for R, and take an invariant $f \in K[V]^G$. Then $f \in K(V)^G = \mathrm{Quot}(R)$ is integral over R, hence (c) implies that $f \in R$, so $R = K[V]^G$. □

Returning to our example, we first prove that the condition (a) from Proposition 5.1 holds. Indeed,

$$[K(V)^G : K(f_2, f_{10}, f_{36}, f_{60})] = \frac{2 \cdot 10 \cdot 36 \cdot 60}{|G|} = 3$$

(see before Proposition 4.1), so $g_{22} \notin K(f_2, f_{10}, f_{36}, f_{60})$ implies $\mathrm{Quot}(R) = K(V)^G$. Furthermore, $K[V]^G$ is integral over R since R contains a homogeneous system of parameters. The hardest part is the verification of condition (c). We first observe that Equation (5.1) gives a presentation of R, since the minimal polynomial of g_{22} over $K(f_2, f_{10}, f_{36}, f_{60})$ has the degree 3. Moreover, the relation shows that

$$R[f_2^{-1}] = K[f_2, f_{10}, f_{36}, g_{22}, f_2^{-1}]$$

is the localization of a unique factorization domain and hence itself a unique factorization domain. Now an elementary argument shows that if f_2 is a prime element in R, then R must also be a unique factorization domain, and then it is integrally closed. In order to prove that $f_2 \in R$ is a prime element, we consider the quotient ring $R/(f_2)$ and from Equation (5.1) find the presentation

$$R/(f_2) = K[f_{10}, f_{36}, f_{60}, g_{22}]/(g_{22}^3 + f_{10}^3 f_{36}).$$

Since the polynomial that is factored out is clearly irreducible, $R/(f_2)$ is a domain and hence f_2 is a prime element as claimed.

Thus we conclude that indeed $K[V]^G = R$, and $1, g_{22}, g_{22}^2$ are secondary invariants. In summary, we have seen that $K[V]^G$ is not a polynomial ring in spite of the fact that G is generated by reflections, but $K[V]^G$ is a complete intersection.

Using methods like these, Gunter Malle and I recently managed to classify all irreducible reflection groups that are not classical groups whose invariant rings are complete intersections.

References

[1] Alejandro Adem, R. James Milgram, *Cohomology of Finite Groups*, Springer-Verlag, Berlin, Heidelberg, New York 1994.

[2] Helmer Aslaksen, Shih-Piug Chan, Tor Gulliksen, *Invariants of S_4 and the Shape of Sets of Vectors*, Applicable Algebra in Engeneering, Communication and Computing **7** (1996), 53–57.

[3] Dave Bayer, Mike Stillman, *Computation of Hilbert Functions*, J. Symbolic Computation **14** (1992), 31–50.

[4] Thomas Becker, Volker Weispfenning, *Gröbner Bases*, Springer-Verlag, Berlin, Heidelberg, New York 1993.

[5] David J. Benson, *Polynomial Invariants of Finite Groups*, Lond. Math. Soc. Lecture Note Ser. **190**, Cambridge Univ. Press, Cambridge 1993.

[6] Wieb Bosma, John J. Cannon, Catherine Playoust, *The Magma Algebra System I: The User Language*, J. Symbolic Computation **24** (1997).

[7] H. E. A. Campbell, I. Hughes, R. D. Pollack, *Rings of Invariants and p-Sylow Subgroups*, Canad. Math. Bull. **34(1)** (1991), 42–47.

[8] H. E. A. Campbell, I. P. Hughes, G. Kemper, R. J. Shank, D. L. Wehlau, *Depth of Modular Invariant Rings*, submitted, 1997.

[9] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York 1995.

[10] Geir Ellingsrud, Tor Skjelbred, *Profondeur d'anneaux d'invariants en caractéristique p*, Compos. Math. **41** (1980), 233–244.

[11] Karin Gatermann, *Semi-Invariants, Equivariants and Algorithms*, Appl. Algebra Eng. Comm. Comput. **7** (1996), 105–124.

[12] David Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), 473–534.

[13] M. Hochster, J. A. Eagon, *Cohen-Macaulay Rings, Invariant Theory, and the Generic Perfection of Determinantal Loci*, Amer. J. of Math. **93** (1971), 1020–1058.

[14] Gregor Kemper, *Calculating Invariant Rings of Finite Groups over Arbitrary Fields*, J. Symbolic Computation **21** (1996), 351–366.

[15] Gregor Kemper, *Calculating Optimal Homogeneous Systems of Parameters*, submitted; IWR Preprint **97-08**, Heidelberg 1997.

[16] Gregor Kemper, *On the Cohen-Macaulay Property of Modular Invariant Rings*, IWR Preprint **97-38**, Heidelberg 1997.

[17] Gregor Kemper, *Hilbert Series and Degree Bounds in Invariant Theory*, submitted; IWR Preprint **97-45**, Heidelberg 1997.

[18] Gregor Kemper, Allan Steel, *Some Algorithms in Invariant Theory of Finite Groups*, in: P. Dräxler, G.O. Michler, C. M. Ringel, eds., *Proceedings of the Euroconference on Computational Methods for Representations of Groups and Algebras*, Progress in Mathematics, Birkhäuser, Basel (to appear).

[19] M. Nagata, *On the 14th Problem of Hilbert*, Amer. J. of Math. **81** (1959), 766–772.

[20] M. Nagata, *Lectures on the Fourteenth Problem of Hilbert*, Tata Institute of Fundamental Research, Bombay 1965.

[21] Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charkteristik p*, Nachr. Ges. Wiss. Göttingen (1926), 28–35.

[22] Vladimir L. Popov, *On Hilbert's Theorem on Invariants*, Dokl. Akad. Nauk SSSR **249** (1979), English translation Soviet Math. Dokl. **20** (1979), 1318–1322.

[23] N. J. A. Sloane, *Error-Correcting Codes and Invariant Theory: New Applications of a Nineteenth-Century Technique*, Amer. Math. Monthly **84** (1977), 82–107.

[24] Larry Smith, *Polynomial Invariants of Finite Groups*, A. K. Peters, Wellesley, Mass. 1995.

[25] Richard P. Stanley, *Invariants of Finite Groups and their Applications to Combinatorics*, Bull. Amer. Math. Soc. **1(3)** (1979), 475–511.

[26] Patrick A. Worfolk, *Zeros of Equivariant Vector Fields: Algorithms for an Invariant Approach*, J. Symbolic Computation **17** (1994), 487–511.