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, 1998 (to appear)

Some Algorithms in Invariant Theory of Finite Groups*

Gregor Kemper† and Allan Steel

Abstract

We present algorithms which calculate the invariant ring $K[V]^G$ of a finite group G. Our focus of interest lies on the modular case, i.e., the case where $|G|$ is divided by the characteristic of K. We give easy algorithms to compute several interesting properties of the invariant ring, such as the Cohen-Macaulay property, depth, the β-number and syzygies.

Introduction

This paper presents various algorithms for invariant theory of finite groups, which were implemented in the computer algebra system Magma [4 or 6] during a visit of the first author to Sydney. We focus on those algorithms which are new or which have never been written up before, and only sketch those that can already be found in the literature. Due to improvements of existing algorithms and a better usage of computational resources by the Magma system, this recent implementation generally produces much better timings than the Invar package which was implemented by the first author in Maple (see KEMPER [8]). For general reading on invariant theory, we refer the reader to the books by STURMFELS [11], BENSON [3], and SMITH [10].

As in the Invar package, the primary goal is the computation of the invariant ring of a given finite matrix group over a base field of arbitrary characteristic. Of particular interest is the **modular case**, i.e., the case where the characteristic of the base field K divides the group order, since in that case the structure of invariant rings is still not very well understood. We give easy algorithms to calculate properties of modular invariant rings, such as the Cohen-Macaulay property, depth, free resolutions, the Hilbert series, and the complete intersection property. Our approach to calculating the invariant ring is divided into two major steps: we first construct a system of **primary invariants**, i.e., homogeneous invariants $f_1, \dots, f_n$ which are algebraically independent, such that the invariant ring is a finitely generated module over $A = K[f_1, \dots, f_n]$. In the next step we calculate **secondary invariants**, which is just another term for generators of the invariant ring as an A-module.

Section 1 is concerned with the problem of how to produce invariants (of some given degree) most effectively. In the next section we come to the methods of finding primary and secondary invariants, where for the secondary invariants we offer completely different algorithms for each of the modular and the non-modular cases. In Section 4 we discuss how properties of the invariant ring can easily be calculated.

Let us fix some notation. Throughout this article, K will be a field (which in the implementation is assumed to be either an algebraic number field or a finite field) and $G \leq \mathrm{GL}_n(K)$ is a finite matrix group acting from the right on an n-dimensional vector space $V \cong K^n$ with basis $x_1, \dots, x_n$. Thus G also acts on the symmetric algebra $K[V] = S(V)$, which is the polynomial ring in the variables $x_1, \dots, x_n$. The invariant ring $\{f \in K[V] \mid f^\sigma = f \ \forall \sigma \in G\}$ is denoted by $K[V]^G$. Since the action of G preserves the natural grading on $K[V]$, this is a graded algebra over K.

All timings in the examples were obtained on a 200 MHz Sun Ultrasparc 2, running Solaris 5.5.1.

*This research was supported in part with the assistance of grants from the Australian Research Council.

†The first author thanks John Cannon and the Magma group for their hospitality during his stay in Sydney.

1 Calculating Homogeneous Invariants

The most basic task is to calculate homogeneous subspaces of invariants, i.e., vector spaces $K[V]_d^G$ consisting of all homogeneous invariants of degree d. All subsequent algorithms depend on effective methods for this. There are two basic approaches. The first one consists of the application of the **Reynolds operator**

$$\pi_G \colon K[V] \to K[V]^G,\ f \mapsto \frac{1}{|G|} \sum_{\sigma \in G} f^\sigma$$

on all (or a sufficient number of) monomials of degree d. This method is only available in the non-modular case. If G is a permutation group, one can take sums over orbits of monomials. Since G acts on the set of monomials in this case, the desired basis is given by all these sums, irrespective of the characteristic of K.

The second method, which we call the **linear algebra method**, exploits the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & K[V]^G \arrow[r] & K[V] \arrow[r] & \bigoplus_{\sigma \in S(G)} K[V] \\ & & f \arrow[r, mapsto] & (f^\sigma - f)_{\sigma \in S(G)} \end{tikzcd},$$

where $S(G)$ is a generating set for G. This sequence restricts to the homogeneous components. The map whose kernel is $K[V]_d^G$ is explicitly given, and hence $K[V]_d^G$ can be calculated by solving a homogeneous system of linear equations in $k = \dim(K[V]_d) = \binom{n+d-1}{n-1}$ unknowns. This method is available for any base field K.

In the non-modular case, both methods are at hand, so we need to assess the computational cost of them. The rank of the linear system involved in the linear algebra method is $\dim(K[V]_d) - \dim(K[V]_d^G)$. The following proposition gives a reasonable estimate for this rank.

Proposition 1. *Let $a_d = \dim(K[V]_d^G)$ and $b_d = \dim(K[V]_d)$. Then*

$$\lim_{N \to \infty} \frac{\sum_{d=0}^N a_d}{\sum_{d=0}^N b_d} = \frac{1}{|G|}.$$

Proof. We choose a maximal homogeneous subset S of $B := K[V]$ which is linearly independent over $A := K[V]^G$. By Galois theory, S has $|G|$ elements. Let M be the free A-module generated by S. Every homogeneous element of B can be written as a linear combination of elements of S with fractions from A as coefficients, whose denominators are all homogeneous. Since B is finitely generated over A, it suffices to take one homogeneous denominator a. In other words,

$$M \subset B \subset a^{-1} M.$$

Let $f(t) = \sum_{s \in S} t^{\deg(s)}$ and $e = \deg(a)$, then for the Hilbert series of A and B it follows

$$f(t) \cdot H(A,t) \le H(B,t) \le t^{-e} f(t) \cdot H(A,t) \quad \text{(coefficient-wise).}$$

Writing $f(t) = \sum_{i=0}^m c_i t^i$, we obtain for $N \in \mathbb{N}$

$$\sum_{d=0}^{N} \sum_{i=0}^{\min(m,d)} c_i a_{d-i} \le \sum_{d=0}^{N} b_d \le \sum_{d=0}^{N} \sum_{i=0}^{\min(m,d+e)} c_i a_{d+e-i}. \tag{1}$$

The left-hand side can be estimated as follows:

$$\begin{aligned} \sum_{d=0}^{N} \sum_{i=0}^{\min(m,d)} c_i a_{d-i} &= \sum_{i=0}^{m} \sum_{d=i}^{N} c_i a_{d-i} = \sum_{i=0}^{m} c_i \left(\sum_{d=0}^{N-i} a_d \right) \\ &\ge \left(\sum_{i=0}^{m} c_i \right) \left(\sum_{d=0}^{N-m} a_d \right) = |G| \cdot \sum_{d=0}^{N-m} a_d. \end{aligned}$$

Similarly, the right-hand side of Inequality (1) is bounded from above by $|G| \cdot \sum_{d=0}^{N+e} a_d$. Extending (1) by these estimates and dividing through the middle term yields

$$|G| \cdot \frac{\sum_{d=0}^{N-m} a_d}{\sum_{d=0}^{N} b_d} \leq 1 \leq |G| \cdot \frac{\sum_{d=0}^{N+e} a_d}{\sum_{d=0}^{N} b_d}.$$

Now the difference between the right-hand side and the left-hand side of this inequality converges to 0 as $N \to \infty$ since

$$\frac{\sum_{d=N-m+1}^{N+e} a_d}{\sum_{d=0}^{N} b_d} \leq (e+m) \cdot \frac{b_{N+e}}{\sum_{d=0}^{N} b_d} = (e+m) \cdot \frac{\binom{N+e+n-1}{n-1}}{\binom{N+n}{n}} \to 0.$$

Hence the limits of both sides are equal, and the result follows. □

The cost of the linear algebra method can now be estimated as follows: We have a linear system with $k = \binom{n+d-1}{n-1}$ unknowns and $s \cdot k$ equations (where s is the number of generators by which G is given), which has rank $k - k/|G|$. The cost of solving this by Gaussian echelonization and then back-substitution is

$$(s - 1/3)k^3 - (s - 1/2)k^2 + 5/6 \cdot k + O\left(\frac{k^2(k+s)}{|G|}\right)$$

arithmetic operations in the base field K, i.e., additions and multiplications equally distributed. In the case of small finite fields, Magma uses packed representations of matrices which speed up the solution of the linear system considerably.

To put up the linear system, we have to apply the group generators to all monomials of degree d. For each generator and each monomial, this means forming a product of d linear forms, which requires

$$2n \cdot \sum_{i=0}^{d-1} \binom{n+i-1}{n-1} = 2n \cdot \binom{n+d-1}{n} = 2dk$$

field operations. This is not the best way to evaluate all products, but it will yield a sufficiently good upper bound to see that the solution of the linear system is dominant. The total cost of the linear algebra method is thus estimated by

$$(s - 1/3)k^3 + ((2d-1)s + 1/2)\,k^2 + 5/6 \cdot k,$$

where, as before, $k = \binom{n+d-1}{d}$.

To assess the cost of applying the Reynolds operator to a monomial $t = x_1^{e_1} \cdots x_n^{e_n}$, we must first look at the stabilizer $G_t \leq G$ of t. Taking the sets $M_e = \{i \mid e_i = e\} \subset \{1, \ldots, n\}$ for $e = 1, \ldots, d$, we see by unique factorization that a $\sigma \in G$ lies in G_t if and only if for all e and for all $i \in M_e$ the ith row of σ only has one non-zero entry α_i which occurs at a column j with $j \in M_e$, and furthermore $\prod_{e=1}^{d} \prod_{i \in M_e} \alpha_i^e = 1$. This gives a very quick procedure to decide whether any given $\sigma \in G$ stabilizes t. On the other hand, we see that we cannot in general expect to have non-trivial stabilizers. Hence the cost of applying the Reynolds operator to m monomials can be estimated by

$$2mdk \cdot |G|.$$

The number m of applications of the Reynolds operator which are required depends on two factors: The first one is whether we want to calculate all invariants of degree d or maybe only one or a few, and the second one is luck. Whether or not the application of the Reynolds operator to just a few monomials will yield linearly independent invariants depends on the choice of these monomials but also on the choice of a basis of V. We shall see in Section 3.1 how the chances can be optimized in the special context of calculating secondary invariants. Certainly m lies between 1 and k. Making our estimates slightly coarser, we see that the break-even point for k lies somewhere between

$$\sqrt{\frac{2d \cdot |G|}{s}} \quad \text{and} \quad \frac{2d \cdot |G|}{s}$$

(where as above s is the number of generators by which G is given), depending on the value assumed for m. The Reynolds operator will perform better if $k = \binom{n+d-1}{n-1}$ exceeds this point. In order to take the speedup of the linear algebra method arising from packed representations (see above) into account, we assign a multiplicative constant depending only on K to the above break-even point.

In the case that G is a permutation group, the invariants are calculated in any case by using sums over orbits of monomials. Thus the above decision only comes into play when G is not a permutation group and $\operatorname{char}(K) \nmid |G|$. A set of monomials can be submitted to the algorithm with the effect that if the Reynolds operator is used, then it is applied to these monomials first. This will become important in Section 3.1.

2 Constructing Primary Invariants

The first major step in the calculation of an invariant ring is the construction of a system of primary invariants $f_1, \ldots, f_n$. These are not uniquely determined by the group, and a good choice of primary invariants turns out to be crucial for the effectiveness of the calculation of secondary invariants. In fact, if $d_1, \ldots, d_n$ are the degrees of the f_i, then there are $d_1 \cdots d_n/|G|$ secondary invariants in the Cohen-Macaulay case. In all cases, this is a lower bound. Furthermore, the maximum degree of a secondary invariant in the Cohen-Macaulay case is $d_1 + \cdots + d_n + a$, where a is the degree of the Hilbert series $H(K[V]^G, t)$ as a rational function in t (i.e., the degree of the numerator minus the degree of the denominator). Hence it is important that the $d_1, \ldots, d_n$ are chosen as small as possible. The Magma implementation has a new algorithm given by Kemper [9] which is guaranteed to yield an optimal system of primary invariants $f_1, \ldots, f_n$. This means that the product of the degrees of the f_i will be minimal, and among the systems of primary invariants having minimal degree product, $f_1, \ldots, f_n$ will have a minimal degree sum. We shall not repeat the entire algorithm from [9], but rather give an overview and discuss some important aspects.

Let us for the moment call a degree vector $(d_1, \ldots, d_n) \in \mathbb{N}^n$ **primary** if there exists a system $f_1, \ldots, f_n$ of primary invariants with $\deg(f_i) = d_i$. There are some very strong constraints on a primary degree vector. First, the Hilbert series of $K[V]^G$ must have the form

$$H(K[V]^G, t) = \frac{f(t)}{(1 - t^{d_1}) \cdots (1 - t^{d_n})} \tag{2}$$

with $f(t)$ a polynomial having integral coefficients (see Section 4.3). In particular, the product $d_1 \cdots d_n$ must be divisible by $|G|$, since the coefficient of $(1 - t)^{-n}$ in the Laurent expansion of $H(K[V]^G, t)$ about $t = 1$ is $1/|G|$ (see Smith [10, Theorem 5.5.3]). If the invariant ring is Cohen-Macaulay, the coefficients of $f(t)$ must be non-negative and are in fact the number of secondary invariants of the corresponding degrees. The constraint given by Equation (2) is applicable whenever the Hilbert series is known. In the non-modular case and in the case of a permutation group G, this can be calculated by Molien's formula. In the other cases, a further constraint is used, which follows from the fact that any system $f_1, \ldots, f_n$ of homogeneous invariants is a system of primary invariants if and only if

$$\dim\left(K[V]/(f_1, \ldots, f_n)\right) = 0, \tag{3}$$

where the dimension is the Krull-dimension. From this it follows by Krull's principal ideal theorem that $\dim\left(K[V]/(f_1, \ldots, f_i)\right) = n - i$ for all i.

Proposition 2 ([9]). *If $(d_1, \dots, d_n)$ is a primary degree vector with $d_1 \le d_2 \le \dots \le d_n$, then the inequality*

$$d_i \ge \min\{d \mid \dim\left(K[V]/(\textstyle\sum_{j=1}^{d} K[V]_j^G)\right) \le n - i\}$$

holds for all i.

This gives a lower bound for the d_i which can quite easily be evaluated since the calculation of Krull dimensions of ideals is available in Magma.

Example 3. Take $G = W_3(F_4)$, the 3-modular reduction of the Weyl group of type F_4. Historically, this is the first (modular) reflection group whose invariant ring is not a polynomial ring (Toda [12]). Setting $d_i = \min\{d \mid \dim\left(K[V]/(\sum_{j=1}^{d} K[V]_j^G)\right) \le n - i\}$, one obtains $(d_1, d_2, d_3, d_4) = (2, 4, 18, 24)$. It turns out that the first random try of invariants of these degrees already yields a system of primary invariants. Since these primary invariants are optimal, this already shows that $K[V]^G$ is not a polynomial ring. The total running time for this example (which is dominated by the time for calculating all invariants up to degree 24) is about 5 minutes.

If a degree vector satisfies the constraint given by Equation (2) or by Proposition 2, it is a primary degree vector in most cases. Moreover, being a system of primary invariants is a Zariski-open condition on a tuple $(f_1, \dots, f_n) \in K[V]_{d_1}^G \times \cdots \times K[V]_{d_n}^G$ (see [9]), hence a random choice $f_1, \dots, f_n$ of invariants of the degrees d_i will usually yield a system of primary invariants. Having such $f_1, \dots, f_n$, it is easy to check Equation (3) to see whether they provide primary invariants. It is hence a good strategy to get the best degree vector satisfying the above constraints which are applicable for the particular group, calculate random invariants of these degrees and test the condition (3). In most cases, this will yield an optimal system of primary invariants and only requires one Gröbner basis calculation (for the final dimension test), and a quite limited number of Gröbner basis calculations if Proposition 2 is used. However, the problem is that there are degree vectors which satisfy the constraints but are not primary. Furthermore, it might happen that a vast number of unlucky invariants of some degrees $d_1, \dots, d_n$ are tried without success even if $(d_1, \dots, d_n)$ is a primary degree vector. If K is a finite field, this can be excluded by simply looping over all homogeneous invariants of some degrees. Hence to obtain an algorithm which is guaranteed to yield an optimal system of primary invariants, we need a criterion which decides whether a degree vector is primary or not in the case that K is infinite. This is provided by the following proposition, which is the key to the general algorithm.

Proposition 4 ([9]). *Let $A = \oplus_{d=0}^{\infty} A_d$ be a graded commutative algebra over an infinite field $K = A_0$ and let $n \in \mathbb{N}_0$ and $d_1, \dots, d_k \in \mathbb{N}$. Then the following conditions are equivalent:*

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

$$\dim\left(A/(f_1, \dots, f_k)\right) \le n - k.$$

(b) For each subset $M \subset \{1, \dots, k\}$ we have

$$\dim\left(A \Big/ (\sum_{i \in M} A_{d_i})\right) \le n - |M|.$$

If K is a finite field, then the implication "(a) $\Rightarrow$ (b)" still holds.

Observe that the conditions in (b) can be checked algorithmically. In the proof of the implication "(b) $\Rightarrow$ (a)" the existence of a homogeneous element $f_1 \in A_{d_1}$ such that $A/(f_1)$ satisfies the conditions in (b) for the degree vector $(d_2, \dots, d_k)$ is shown. This f_1 can be found by a loop over elements of A_{d_1}. Then f_1 can be extended to a system $f_1, \dots, f_k$ with $\dim\left(A/(f_1, \dots, f_k)\right) \le n - k$. We thus arrive at the following method: Loop over all degree vectors $(d_1, \dots, d_n)$, ordered by rising products and sums, and check the conditions (b) from Proposition 4. When a degree vector is found which satisfies (b), recursively construct primary invariants $f_1, \dots , f_n$. If K is a finite field and on some recursion level no f_i has been found even after looping through the complete space A_{d_i}, then proceed to the next degree vector.

Clearly this approach always produces an optimal system of primary invariants, but it has the drawback that it requires $2^{n+1} - 1$ Gröbner basis calculations for the dimension test even if the first degree vector that is tested is actually a primary degree vector. The "random approach" described above is in a sense complementary to it and only requires one Gröbner basis calculation if successful. The actual algorithm implemented in Magma brings these two approaches together. It has an outer loop over degree vectors which satisfy the applicable constraints. For each such degree vector, a random choice of f_i is tested first. If that is unsuccessful, then increasingly more of the conditions from Proposition 4(b) are brought in. More precisely, if at some stage an f_1 is chosen which fails to be extendible to a system $f_1, \dots , f_k$, then the conditions for this k are brought in, which in the case of infinite K guarantees that the next f_1 will be extendible further. This algorithm combines the virtue of always producing an optimal system of primary invariants with probabilistically good running times. Indeed, we obtained quite good timings in comparison with other algorithms for the construction of primary invariants (see [9]).

3 Calculating Secondary Invariants

In this section we assume that primary invariants $f_1, \dots , f_n$ for G have been chosen and we set $A = K[f_1, \dots , f_n]$. The next task is to calculate secondary invariants, i.e., generators for $K[V]^G$ as a module over A. We have completely different algorithms for each of the modular and the non-modular cases.

3.1 The non-modular case

If $\text{char}(K) \nmid |G|$, we can easily calculate the Hilbert series $H(K[V]^G, t)$ by Molien's formula. Comparing this to Equation (2) gives us complete information about the number and degrees of secondary invariants which are needed. In particular, their number is $\deg(f_1) \cdots \deg(f_n)/|G|$. We then find secondary invariants by the following consideration: for any homogeneous invariants $g_1, \dots , g_m$ it is equivalent that they generate $R := K[V]^G$ as a module over A and that they generate the vector space $R/(f_1, \dots , f_n)_R$, where the index R means that we are taking an ideal in R. This is seen by an easy induction on degrees (Proposition 8 on page 10). But due to the Reynolds operator, the natural map

$$R/(f_1, \dots , f_n)_R \to K[V]/(f_1, \dots , f_n)$$

(with the right ideal taken in $K[V]$) is injective. Hence if $m = \deg(f_1) \cdots \deg(f_n)/|G|$, then $g_1, \dots , g_m$ are a complete set of secondary invariants if and only if they are linearly independent modulo $(f_1, \dots , f_n)$. Note that we can reduce the g_i modulo $(f_1, \dots , f_n)$ by using a Gröbner basis, which has already been calculated for doing the dimension test involved in constructing the primary invariants.

A further optimization ensues from the fact that the Reynolds operator π_G is a homomorphism of modules over $K[V]^G$ and in particular of modules over A. Hence all secondary invariants can be obtained by applying π_G to a basis of $K[V]$ over A. But such a basis is obtained by taking a basis of $K[V]/(f_1, \dots , f_n)$, which can be chosen to consist of monomials. Restricting the set of monomials in such a way, we can substantially increase the chances of finding suitable invariants by just a few applications of π_G.

The algorithm, which is listed as Algorithm 5 on the next page, does not only calculate a minimal system of secondary invariants, but it also produces a subset of *irreducible* secondary invariants such that each secondary invariant is a power product of the irreducible ones. Here a secondary invariant is called **irreducible** if it cannot be written as a polynomial expression in the primary invariants and the other secondary invariants, and 1 is considered as the empty power product. Hence the subset M of irreducible secondary invariants produced by Algorithm 5 is a minimal system of generators of $K[V]^G$ as an algebra over A. The calculation of a subset of irreducible secondary invariants has several important benefits: first, we gain more insight into the structure of the invariant ring. Second, fewer "fresh" invariants, especially of high degrees, have to be calculated. Third, the calculation of syzygies will be considerably simpler (see Section 4.5).

```
Input: Primary invariants $f_1, \dots, f_n$.
Output: Secondary invariants $g_1, \dots, g_m$, and a subset $M$ of irreducible secondary invariants such
    that each $g_i$ is a power product of the elements of $M$.
Begin
    Calculate a Gröbner basis $B$ of $(f_1, \dots, f_n)$ w.r.t. any term order, and monomials $m_1, \dots, m_r$
        forming a basis of $K[V]/(f_1, \dots, f_n)$.
    Obtain numbers $k_0, \dots, k_e \in \mathbb{N}_0$ from $(1 - t^{d_1}) \cdots (1 - t^{d_n}) \cdot H(K[V]^G, t) = \sum_{i=0}^{e} k_i t^i$, where
        $d_i = \deg(f_i)$.
    Set $M := \emptyset$ and $m := 1$.
    For $d = 0, \dots, e$ do
        Set $k := 0$ and $h := 0$ ($h$ will be a linear polynomial in indeterminates $t_1, \dots, t_{k_d}$ with
            coefficients in $K[V]$).
        For all power products $g$ of elements of $M$ having degree $d$ do
            If $k = k_d$ then break.
            Calculate the normal form $g_{red}$ of $g$ w.r.t. $B$.
            If the linear system $g_{red} = h(t_1, \dots, t_{k_d})$ is not solvable for the $t_i$-variables then
                set $g_m := g$, $m := m + 1$, $k := k + 1$, and $h := h + g_{red} \cdot t_k$.
        end for
        For $i = 1, 2, \dots$ do
            If $k = k_d$ then break.
            Calculate the $i$th linearly independent invariant $g$ of degree $d$, using the monomials
                $m_1, \dots, m_r$ if the Reynolds operator is applied (see Section 1).
            Calculate the normal form $g_{red}$ of $g$ w.r.t. $B$.
            If the linear system $g_{red} = h(t_1, \dots, t_{k_d})$ is not solvable for the $t_i$-variables then
                set $g_m := g$, $m := m + 1$, $k := k + 1$, $h := h + g_{red} \cdot t_k$, and $M := M \cup \{g\}$.
        end for
    end for
end.
```

Algorithm 5: Calculate secondary invariants in the non-modular case

Example 6.

(a) A three-dimensional representation of $G = A_5$ is given by the generators

$$\begin{pmatrix} 1 & 0 & -\alpha \\ 0 & 0 & -1 \\ 0 & 1 & -\alpha \end{pmatrix}, \begin{pmatrix} -1 & -1 & \alpha \\ -\alpha & 0 & \alpha \\ -\alpha & 0 & 1 \end{pmatrix},$$

where $\alpha^2 - \alpha - 1 = 0$ and $K = \mathbb{Q}(\alpha)$. The Hilbert series is calculated by Molien's formula to be

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

Trying the first invariants of degree 2, 6 and 10 yields primary invariants at once. The first of the basis monomials $m_1, \ldots, m_r$ obtained in the first step of Algorithm 5 having degree 15 is $x_2^2 x_3^{13}$, and applying the Reynolds operator to it yields the missing secondary invariant of degree 15. The entire calculation takes less than half a second.

(b) We consider the group $G \leq \mathrm{GL}_4(\mathbb{C})$ of order 36 generated by the matrices

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

where $\zeta = e^{2\pi i/3}$. The Hilbert series is

$$H(K[V]^G, t) = \frac{1 + 2t^3 + 3t^6 + 2t^9 + t^{12}}{(1 - t^3)^2 (1 - t^6)^2}.$$

Again in less than 2 seconds, Magma finds primary invariants $x_1^3, x_3^3, x_2^6, x_4^6$ and secondary invariants $1, h_1 = x_1 x_2^2, h_2 = x_3 x_4^2, h_1^2, h_1 h_2, h_2^2, h_1^2 h_2, h_1 h_2^2, h_1^2 h_2^2$. The irreducible secondary invariants are h_1 and h_2. Observe that we only had to calculate invariants up to degree 6.

3.2 The modular case

In [8], the first author gave an algorithm for calculating secondary invariants in the modular case. Here we present a variant of this algorithm.

We first choose a subgroup $H \lneqq G$ (for example, $H = \{1\}$) and calculate secondary invariants $h_1, \ldots, h_r$ of H, where we take the primary invariants $f_1, \ldots, f_n$ of G as primary invariants for H also. This is done either by recursion or by the non-modular Algorithm 5. If $K[V]^H$ is not Cohen-Macaulay, it is useful to calculate the A-linear relations between the h_i also by the method described in Section 4.2. In other words, we calculate the kernel S of the map $A^r \to K[V]^H$ given by the h_i, where A^r is a free module over A with free generators to which we assign the degrees of the h_i. The map

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

has the kernel $K[V]^G$, where $S(G/H)$ is a subset of G which together with H generates G. We obtain the following commutative diagram of graded A-modules with exact rows and columns:

$$\begin{tikzcd}
 & 0 & 0 & 0 \\
0 \arrow[r] & K[V]^G \arrow[r] \arrow[u] & K[V]^H \arrow[r] \arrow[u] & \bigoplus_{\sigma \in S(G/H)} K[V] \arrow[u] \\
0 \arrow[r] & M \arrow[r] \arrow[u] & A^r \arrow[r] \arrow[u] & A^k \arrow[u] \\
0 \arrow[r] & M \cap S \arrow[r] \arrow[u] & S \arrow[u] & 0 \arrow[u] \\
 & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

Here $A^k \overset{\sim}{\longrightarrow} \bigoplus_{\sigma\in S(G/H)} K[V]$ is given by the fact that $K[V]$ is a free module of rank $\prod_{i=1}^n \deg(f_i)$ over A, hence k is $|S(G/H)|$ times this rank. The map $A^r \to A^k$ is defined by the commutativity, and M is its kernel. Observe that all maps in the above diagram are degree-preserving. Now by calculating generators for M, one obtains generators for $K[V]^G$, i.e., secondary invariants. But M is the kernel of a linear map between two free modules over the polynomial algebra A, so its generators can be calculated by the syzygy function of Magma.

In fact the effort of putting up the map $A^r \to A^k$ turns out to be comparable to or even greater than the effort of the actual syzygy calculation. To obtain this map, we have to find the representations of all $h_i^\sigma - h_i$ ($i = 1,\dots,r$, $\sigma \in S(G/H)$) as elements of $\bigoplus_{j=1}^l A\cdot m_j$, where the m_j are (free) generators of $K[V]$ as an A-module, which are pre-calculated. This is done by equating $h_i^\sigma - h_i$ to a general element of the homogeneous K-subspace of $\bigoplus_{j=1}^l A\cdot m_j$ of degree $d = \deg(h_i)$ with unknown coefficients. Comparing coefficients then leads to an inhomogeneous system of linear equations over K for these unknown coefficients, and solving it yields the desired representation.

In this situation it is quite common that calculations in the same degree, say d, occur very often. A significant speedup arises from the fact that all the related inhomogeneous systems can be solved with only one nullspace computation. The general element of the homogeneous K-subspace of degree d is formed only once and only a slight extension of the usual nullspace algorithm allows the determination of all of the desired representations simultaneously. Since only one construction and echelonization of the space is needed to determine all the representations it is *much* more efficient to use this method than to build and solve separate systems for each of the polynomials having degree d.

Example 7.

(a) We continue Example 3, where the primary invariants of the 3-modular reduction of the Weyl group of type F_4 have already been calculated. To calculate secondary invariants, we choose a Sylow subgroup of order 128 as the subgroup H, hence $r = 2\cdot 4\cdot 18\cdot 24/128 = 27$. It takes more than two hours to set up the map $A^r \to A^k$ and then only about two minutes to calculate its kernel. The result is secondary invariants of degrees 0, 10 and 20.

(b) The 6-dimensional indecomposable representation of the cyclic group Z_8 of order 8 over $K = \mathbb{F}_2$ is generated by the matrix

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

It takes 5.3 seconds to find (optimal) primary invariants of degrees 1, 2, 2, 2, 4, 8. Secondary invariants are then calculated in about 8 minutes. The resulting number of secondary invariants is 43 and their maximal degree is 13. To the best knowledge of the authors, invariant rings of indecomposable representations of cyclic groups of dimensions exceeding 5 have never been calculated before.

Since in the above algorithm the number r of secondary invariants for $K[V]^H$ is bounded from below by $\deg(f_1)\cdots\deg(f_n)/|H|$ with equality in the Cohen-Macaulay case, it is important that the subgroup H is chosen as large as possible. This will lead to a minimal number of linear systems to be solved for putting up the map $A^r \to A^k$, and it will minimize the effort of calculating the kernel of this map. By default, the Magma implementation chooses H as a p'-Sylow subgroup of maximal order with $p' \neq \mathrm{char}(K)$. Other subgroups can be submitted by the user. Another, complementary, approach is to calculate secondary invariants for a p-Sylow subgroup P of G first, where $p = \mathrm{char}(K)$, and then to obtain secondary invariants for $K[V]^G$ by using the relative Reynolds operator $\pi_{G/P}$: $K[V]^P \to K[V]^G$ (see, Campbell et al. [5] or Smith [10, p. 28]). This approach is in development. One could also calculate $K[V]^P$ by applying the algorithm recursively, where each step consists of an extension of the current subgroup by an index p. There is some experimenting involved as to what approach should be best, and the answer will probably depend very much on the special situation.

4 Properties of the Invariant Ring

In this section we discuss how some important properties of the invariant ring can be computed after primary and secondary invariants have been found. The properties dealt with in 4.1–4.3 are only relevant in the modular case. We use the fact that the algorithm from Section 3.2 yields the invariant ring $K[V]^G$ as the quotient $M/(M \cap S)$ of submodules of A^r.

4.1 Minimal secondary invariants and the Cohen-Macaulay property

We first make a general, well-known remark on generating systems of homogeneous modules.

Proposition 8. *Let $A = \sum_{d=0}^{\infty} A_d$ be a commutative graded algebra over a field $K = A_0$ and $M = \sum_{d=N}^{\infty} M_d$ a graded A-module with $N \in \mathbb{Z}$. Then it is equivalent for a subset $S \subset M$ of homogeneous elements that S generates M as an A-module and that S generates M/A_+M as a vector space over K. Here A_+M is the submodule of M generated by the elements $a \cdot g$ with $a \in A$ homogeneous of positive degree and $g \in M$.*

In particular, if M is finitely generated, it is equivalent for a homogeneous generating set to be minimal in the sense that no generator can be omitted and to have minimal cardinality.

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

Now suppose that S generates M/A_+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 $g_1, \ldots, g_m \in S$, $\alpha_i \in K$, $a_j \in A_+$ 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 assertion about minimality of generating systems now follows from the corresponding property of vector spaces. □

In the non-modular case, Algorithm 5 already yields a minimal system of secondary invariants, so we now turn to the modular case and use the notation from Section 3.2.

If $K[V]^H$ is Cohen-Macaulay, then $K[V]^G \cong M$, and a minimal system of generators for M yields a minimal system of secondary invariants of $K[V]^G$. Obtaining a minimal generating system for M from a possibly redundant one amounts to a series of membership tests of submodules, which are done by linear algebra. In general, however, $K[V]^G \cong M/(M \cap S) \cong (M+S)/S$. If B_1 generates S, then a subset $B_2 \subset M$ generates $M/(M \cap S)$ if and only if $B_1 \cup B_2$ generates $M + S$. Hence a minimal system of secondary invariants for $K[V]^G$ can be found by minimally completing B_1 to a system of generators for $M + S$. By default, this minimization is performed by the Magma implementation.

If m is the cardinality of a minimal system of secondary invariants, then $K[V]^G$ is Cohen-Macaulay if and only if

$$m = \frac{\deg(f_1) \cdots \deg(f_n)}{|G|} \tag{4}$$

(see, for example, Kemper [8, Proposition 12]). Hence checking the Cohen-Macaulay property is also an easy exercise once the primary and secondary invariants have been calculated.

4.2 Module-syzygies and depth

If $K[V]^G$ is not Cohen-Macaulay, then our minimal generating set of $K[V]^G$ over A will contain relations. Let us call these relations **module-syzygies** in order to avoid confusion with the syzygies treated in Section 4.5. We use the notation of Section 3.2 and complete a generating system of S to a generating system of $M + S$ in order to obtain a minimal system of secondary invariants (see above). This yields an epimorphism $F' \oplus F \to M + S \subset A^r$, where F and F' are free A-modules with F corresponding to the generators of S and F' corresponding to its completion. The kernel N of this epimorphism can be calculated by the standard syzygy function of Magma. We obtain the following commutative diagram of A-modules with exact rows and columns:

$$\begin{tikzcd}
& 0 & 0 & 0 & \\
0 \arrow[r] & N' \arrow[r] \arrow[u] & F' \arrow[r] \arrow[u] & M/(M \cap S) \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & N \arrow[r] \arrow[u] & F' \oplus F \arrow[r] \arrow[u] & M + S \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

Here $F' \oplus F \to F'$ is the first projection, and N' is the image of N under it. We have to show the exactness at F'. By the commutativity, any element from N' is mapped to 0 under $F' \to M/(M \cap S)$. Conversely, suppose that $v_2 \in F'$ is mapped to 0. Then it is mapped to an element $m \in M \cap S$ under $F' \to M$. Hence there exists $v_1 \in F$ which is mapped to m under $F \to S$, and $v_2 - v_1$ lies in N. Now $v_2 \in N'$ by construction.

As $K[V]^G \cong M/(M \cap S)$, N' consists exactly of the module-syzygies by the above diagram. So we see that module-syzygies can be calculated quite easily.

Carrying the calculations further in this way and calculating syzygies of N' and so on, we obtain a minimal free resolution

$$0 \longrightarrow F_r \longrightarrow \ldots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow K[V]^G \longrightarrow 0 \tag{5}$$

of $K[V]^G$ (as a graded A-module). Each step consists of a simple application of the standard syzygy function and a minimization of generators. If $F_r \neq 0$, then by the Auslander-Buchsbaum formula we obtain

$$\mathrm{depth}(K[V]^G) = n - r$$

(see Kemper [8]). All these calculations are relatively easy once the secondary invariants have been found.

Example 9. In Example 7(b), it is clear by the criterion (4) that the invariant ring of the 6-dimensional indecomposable representation of Z_8 over $\mathbb{F}_2$ cannot be Cohen-Macaulay. Hence the depth is at most 5. It takes 4.5 seconds to calculate a minimal free resolution of the invariant ring. This turns out to have the length $r = 3$, hence the depth is in fact $6 - 3 = 3$, in accordance with the famous result by Ellingsrud and Skjelbred [7], which says that the invariant ring of an indecomposable representation of a cyclic group always has depth 3 (provided that the dimension of the representation is at least 3).

4.3 The Hilbert series

There are two methods to obtain the Hilbert series of the invariant ring.

(a) If a free resolution (5) has been calculated, then

$$H(K[V]^G, t) = \sum_{i=0}^{r} (-1)^i H(F_i, t).$$

Note that all F_i occurring in (5) are graded free modules, where the grading is such that the homomorphisms are degree-preserving. If $d_1, \dots, d_r$ are the degrees of the free generators of an F_i, then

$$H(F_i, t) = \frac{t^{d_1} + \cdots + t^{d_r}}{(1 - t^{\deg(f_1)}) \cdots (1 - t^{\deg(f_n)})}.$$

(b) Since $H(K[V]^G, t) = H(M, t) - H(M \cap S, t)$ (again using the notation from Section 3.2), The Hilbert series can be obtained by calculating Gröbner bases for M and for $M \cap S$ and then computing the Hilbert series of these modules by an algorithm given by Bayer and Stillman [2]. This algorithm is purely combinatorial and only uses the leading monomials of the Gröbner bases. Note that in many cases $S = 0$ due to the choice of the subgroup H.

If a free resolution has been calculated, the method (a) amounts to a mere bookkeeping task. But according to our experience, the second method never takes any noticeable amount of time compared to the time required for the calculation of primary and secondary invariants. Hence the implementation uses method (b) in all cases.

Example 10. We consider the cyclic group G of order 7 generated by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \in \mathrm{GL}_5(\mathbb{F}_7).$$

The invariant ring is calculated in about 4 minutes. The degrees of the primary invariants are 1, 2, 2, 6, and 7. The subsequent calculation of the Hilbert series takes 4 seconds. The result is

$$H(K[V]^G, t) = \frac{t^{13} + 2t^{10} + 2t^9 + 4t^8 + 3t^7 + 3t^6 + 4t^5 + 2t^4 + 2t^3 + 1}{(1-t)(1-t^2)^2(1-t^6)(1-t^7)}.$$

This coincides with a result of Almkvist [1], which gives Hilbert series of all invariant rings of indecomposable representations of cyclic groups and in this case reads

$$H(K[V]^G, t) = \frac{1}{7} \sum_{\zeta \in \mu_7} \prod_{j=0}^{4} \frac{1}{1 - \zeta^{4-2j} t},$$

where the sum runs over the set μ_7 of the 7th complex roots of unity.

4.4 Fundamental invariants and β

Given homogeneous invariants $f_1, \dots, f_m \in K[V]^G$ it is equivalent that they generate $K[V]^G$ as a K-algebra and that they generate the ideal $K[V]^G_+ \trianglelefteq K[V]^G$ spanned by the invariants of positive degree. This observation, which is proved as Proposition 8, is in fact the starting point of Hilbert's proof of the finiteness theorem. Now by Proposition 8 the latter condition is in turn equivalent to saying that $f_1, \dots, f_m$ generate the quotient module $K[V]^G_+/(K[V]^G_+)^2$ as a vector space over K. So again we see that a system of generators of $K[V]^G$ as an algebra over K which is minimal in the sense that no element can be omitted also has minimal cardinality, and the degrees of its members are uniquely determined. The maximum of these degrees is often denoted by $\beta(V, G)$, and members of a minimal generating system are called **fundamental invariants**.

By taking the primary and the secondary invariants together, we have a system of generators for $K[V]^G$ as a K-algebra. It is in fact sufficient to take the irreducible secondary invariants if they have been calculated (see Section 3.1). This system can be minimized by taking the elements f in turn and for each one testing if f is contained in the algebra generated by the current system of fundamental invariants minus f. The test again comes down to a linear system over K, obtained by equating f to a general element of the K-subspace of degree-d elements of the algebra generated by the current fundamental invariants minus f. If it is solvable, then f can be omitted from the system of fundamental invariants. Again this method is optimized by collecting all relevant calculations of one degree into a single system of equations (see page 9).

Example 11. In Example 7(b), the minimal secondary invariants of the 6-dimensional indecomposable representation over $\mathbb{F}_2$ of the cyclic group Z_8 were calculated. When extracting fundamental invariants from these and the primary invariants, 9 secondary invariants, including those of degrees 12 and 13, can be omitted. Hence $\beta(V, G) = 11$ and the minimal number of algebra generators of the invariant ring is 40. The extraction of fundamental invariants takes about 4 minutes.

4.5 Syzygies

Sections 2 and 3 were devoted to finding generators of $K[V]^G$ as an algebra over K. In the non-modular case, these are given by the primary invariants and the irreducible secondary invariants $h_1, \dots, h_r$, where all secondary invariants $g_1, \dots, g_m$ are power products of the h_i. We write $g_i = p_i(h_1, \dots, h_r)$, where p_i are power products of indeterminates $t_1, \dots, t_r$. In the modular case, let $h_1, \dots, h_r$ be all secondary invariants which have degree > 0. We are now interested in algebraic relations between these generators, i.e., we are are looking for the kernel J of the homomorphism

$$A[t_1, \dots, t_r] \to K[V]^G, \ t_i \mapsto h_i$$

of graded K-algebras, where we set $\deg(t_i) = \deg(h_i)$. To calculate these relations is one of the basic tasks of invariant theory, since they define the quotient variety $V/G = \operatorname{Spec}(K[V]^G)$. Since the primary invariants are algebraically independent, there is no necessity to replace them by indeterminates in this paper, though they are of course represented symbolically in the Magma implementation. There is a standard Gröbner basis method using tag-variables for calculating this kernel. But Gröbner bases can be avoided since the following proposition reduces the calculation of syzygies to a pure linear algebra problem.

Proposition 12. *In the above situation, let $S \subset J$ be a set containing*

(a) generators for the module-syzygies, i.e., for the A-module $J \cap \oplus_{i=1}^m A \cdot p_i$,

(b) for each pair g_i and h_k such that $p_i \cdot t_k$ is none of the p_j, a relation of the form $p_i t_k - f_{i,k}$ with $f_{i,k} \in \oplus_{j=1}^m A \cdot p_j$.

Then J is spanned by S.

Proof. Let J' be the ideal generated by S. For a power product p of the t_j, let p_i be a maximal subproduct of p which is one of the p_j and write $D(p)$ for the length (i.e., number of factors) of p/p_i. We prove by induction on $D(p)$ that p is congruent to an element of $\oplus_{j=1}^m A \cdot p_j$ modulo J'. If $D(p) = 0$, we are done. Otherwise, $p = p_i \cdot t_k \cdot q$ for some k. By the assumption, $p_i \cdot t_k$ is congruent to an element of $\oplus_{j=1}^m A \cdot p_j$. But for all j we have $D(p_j \cdot q) \leq \operatorname{length}(q) < D(p)$, hence by induction all $p_j \cdot q$ lie in $\oplus_{j=1}^m A \cdot p_j$ modulo J', and so does p.

Now let $f \in A[t_1, \dots, t_r]$ be a polynomial which maps to 0 under $A[t_1, \dots, t_r] \to K[V]^G$. By the above, $f \equiv g \mod J'$ with $g \in \oplus_{j=1}^m A \cdot p_j$, hence g maps to 0, too. By the first assumption, g lies in J' and thus also $f \in J'$. □

The calculation of module-syzygies, which only exist in the modular case, was discussed in Section 4.2. Finding the representations of $g_i h_k$ is done by the following linear algebra method: We form a general degree-d element of $\sum_{j=1}^{m} A g_j$ (with unknown coefficients) and equate it to $g_i h_k$, where $d = \deg(g_i h_k)$. This is an inhomogeneous system of linear equations over K. Solving it will yield the desired representation. As above, a considerable speedup is achieved by doing all computations of one degree in a single linear system.

We can obtain a *minimal* generating set for J and at the same time avoid a considerable amount of computation by using the following strategy: First order the products $g_i h_k$ by rising degrees. Then for each product $g_i h_k$ of degree d, consider a general degree-d element of the ideal $J' \subset J$ generated by the relations obtained so far. It is again a linear algebra problem to decide if there exists a specialization of the unknown coefficients involved which yields the desired representation for $g_i h_k$. If such a specialization exists, then we do not have to calculate the representation, and no new generator has to be added to J.

It is of considerable interest to obtain a minimal generating system for J, since $K[V]^G$ is said to be a complete intersection if such a system has exactly r elements.

Example 13. The group $G = W_3(F_4)$ studied in examples 3 and 7(a) has secondary invariants 1 and g_{10} of degree 10, and a further secondary invariant of degree 20, for which g_{10}^2 can be taken. Since Equation (4) is fulfilled, they are linearly independent over A, and we only need one relation for g_{10}^3, and $K[V]^G$ is a complete intersection. The relation is found in 13 seconds, but it is too messy to be printed here.

On the other hand, consider the cyclic group $G \leq \mathrm{GL}_2(\mathbb{C})$ generated by $\begin{pmatrix} \zeta & 0 \\ 0 & \zeta \end{pmatrix}$ with $\zeta = e^{2\pi i/3}$. We find primary invariants $f_1 = x_1^3$ and $f_2 = x_2^3$, and secondary invariants 1, $h_1 = x_1 x_2^2$ and $h_2 = x_1^2 x_2$, from which h_1 and h_2 are irreducible. A minimal system of relations is

$$h_1^2 = f_2 h_2, \quad h_2^2 = f_1 h_1, \quad h_1 h_2 = f_1 f_2,$$

hence $K[V]^G$ is not a complete intersection.

References

[1] Gert Almkvist, *Invariants of* $\mathbf{Z}/p\mathbf{Z}$ *in Charcteristic* p, in: *Invariant Theory (Proc. of the 1982 Montecatini Conference)*, Lecture Notes in Math. **996**, Springer-Verlag, Heidelberg, Berlin 1983.

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

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

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

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

[6] John J. Cannon, Catherine Playoust, *Magma: A new computer algebra system*, Euromath Bulletin **2(1)** (1996), 113–144.

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

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

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

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

[11] Bernd Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Wien, New York 1993.

[12] H. Toda, *Cohomology mod 3 of the Classifying Space BF_4 of the Exceptional Group F_4*, J. Math. Kyoto Univ. **13** (1972), 97–115.

Gregor Kemper
IWR/Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 368
69120 Heidelberg
Germany
`Gregor.Kemper@iwr.uni-heidelberg.de`

Allan Steel
School of Mathematics and Statistics
University of Sydney
NSW 2006
Australia
`allan@maths.usyd.edu.au`