Invariants of finite groups and involutive division

C. F. Cid, W. Plesken

1 Introduction

The invariant ring of a finite matrix group is known to be well behaved for reflections groups and messy in general. Involutive division is a newly discovered tool in commutative algebra and in this note it is applied to the problem of finding a presentation of the ring of invariants of a finite matrix group. The first author has implemented the JANET-algorithm in MAPLE following [GeB 98a] and [GeB 98b]. The results of this are collected in two MAPLE-packages called INVOLUTIVE and JANET, the first dealing with polynomials and the second with linear partial differential equations. Both of these packages have a collection of other routines serving various purposes. There is also a loose connection with the MAPLE-package JETS by Mohammed Barakat, which deals with symmetries of differential equations, conservation laws etc.. Here we report on our experience with applying the package INVOLUTIVE to questions of invariant theory of finite groups. We outline an algorithm constructing a presentation of the ring of invariants of a finite complex matrix group and representing each invariant in a unique way as an expression in the generators. We also report on the limits with the present MAPLE implementation. As far as the invariant theory of finite groups proper is concerned, there are is a MAPLE-package available to perform the tasks discussed here, cf. [Kem 98] or [Kem 99], based on GROEBNER basis techniques and even a very effective implementation in MAGMA. The issue here is more to demonstrate the flexibility of involutive division and the JANET algorithm to these aims. Here we also restrict the discussion to the classical case of fields of characteristic zero, where MOLIEN's series is available.

We wish to thank Vladimir Gerdt for many discussions and his guidance with the implementation, Daniel Roberts for adding some functions to the system, and Mohammed Barakat for contributing some of the functions of his MAPLE package JETS, which turned out to be rather useful and to J.-F. Pommaret, whose book [Pom 94] got us interested in JANET's algorithm.

2 Summary of the relevant theory

In this section let $G \leq \mathrm{GL}(n, \mathbb{C})$ be a finite matrix group. Identify the natural G-module $\mathbb{C}^{n\times 1}$ with the $\mathbb{C}$-vector space $\mathbb{C}[x_1, \ldots, x_n]_1$ of homogeneous polynomials of degree 1 in the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$. In this way G acts on $\mathbb{C}[x_1, \ldots, x_n]$ by algebra automorphisms. The subring $\mathbb{C}[x_1, \ldots, x_n]^G$ of G-fixed points it the object of our interest. The oldest result on this is MOLIEN's formula for the dimensions of the

$$\mathbb{C}[x_1, \ldots, x_n]_i^G := \mathbb{C}[x_1, \ldots, x_n]_i \cap \mathbb{C}[x_1, \ldots, x_n]^G$$

where $\mathbb{C}[x_1, \ldots, x_n]_i$ is the $\mathbb{C}$-vector space of homogeneous polynomials of degree i with $i \in \mathbb{Z}_{\geq 0}$, This formula is given by

$$m_G(s) := \sum_{g\in G} \det(I_n - sg)^{-1} = \sum_{i=0}^{\infty} \mathrm{Dim}(\mathbb{C}[x_1, \ldots, x_n]_i^G) s^i.$$

It left hand side, the MOLIEN series can easily be evaluated using characters, as provided for by GAP Of course

$$\mathbb{C}[x_1, \ldots, x_n]^G = \bigoplus_{i=0}^{\infty} \mathbb{C}[x_1, \ldots, x_n]_i^G$$

is a graded ring, and EMMY NOETHER has shown that is is generated by the invariants of degree $\leq |G|$, cf. [Ben 93], where a relative version of this result is also proved: If $U \leq G$ is a subgroup whose ring of invariants is generated by invariants of degrees $\leq b$, then the ring of G-invariants is generated by invariants of degrees $\leq b|G:U|$. This will turn out to be useful.

Individual invariants can be obtained constructively as images under the projection operator

$$\pi : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_n]^G : p \mapsto \frac{1}{|G|} \sum_{g \in G} p \circ g.$$

Of course, if $|G|$ gets bigger, one will split up this sum into in iterated sum over transversals in a subgroup chain of G. Details can be found in [Sta 79], [Ben 93], [Stu 93].

3 Presentation for the ring of invariants

Keeping the notation of the last section, we now want to present an algorithm for finding a presentation of $\mathbb{C}[x_1, \ldots, x_n]^G$. More precisely, we want to outline an algorithm to find generators and unique expressions for each invariant in terms of these generators. Of course, we want to do with less generators than given by NOETHER's theoretical bound, possibly with the minimal number of generators possible, all generators being assumed to be homogeneous.

Problem 1: Given homogeneous invariants $i_1, \ldots, i_k \in \mathbb{C}[x_1, \ldots, x_n]^G$. Find the generating function for the

$$\mathrm{Dim}(\mathbb{C}[i_1, \ldots, i_k] \cap \mathbb{C}[x_1, \ldots, x_n]_i).$$

The classical approach to this is as follows: Look at the polynomial ring $\mathbb{C}[I_1, \ldots, I_k]$ and its epimorphisms onto $\mathbb{C}[i_1, \ldots, i_k]$ mapping the indeterminate I_l to the invariant polynomial i_l:

$$\sigma : \mathbb{C}[I_1, \ldots, I_k] \to \mathbb{C}[i_1, \ldots, i_k] : I_l \mapsto i_l.$$

Construct a free resolution of $\mathbb{C}[I_1, \ldots, I_k]$-modules of the kernel $\ker \sigma$ of this map. From general commutative algebra, this resolution is bound to determinate after at most n steps. Assigning appropriate degrees to the I_l (namely $\deg(i_l)$) and to the generators of the free modules, one gets the desired generating function above as an alternating sum of products of certain geometric series multiplied by powers of the variable s, for details see [Ben 93] . Technically this can be done by using JANET's algorithm for linear differential equations translated into polynomial equations by starting out with $x_1, \ldots, x_n, I_1, \ldots, I_k$ as indeterminates, and $I_1 - i_1, \ldots, I_k - i_k$ as relations and to use pure lexicographic order to eliminate the x_i. In this way, one gets generators for the kernel and can proceed from there to construct the free resolution, cf. We have an automatic function doing this. For instance the example 6.6 of $G = \langle -I_3 \rangle \leq \mathrm{GL}(3, \mathbb{C})$ of [Sta 79] runs completely automatically. There are two independent observations to make:

First the good news: with the JANET basis for $\ker \sigma$ it is no longer necessary to construct the free resolution: the generating function can be read off from the JANET basis of $\ker \sigma$.

And the bad news: There seem to be strict limits to this approach, the bottleneck being the performance of the JANET algorithm on the rather big system above involving the x_i and the I_j.

The first point is clarified by the following proposition, demonstrating the nice and clear structure of the JANET-approach.

Proposition 3.1 *Let $p_1, \ldots, p_r$ be a* JANET *basis of $\ker \sigma$ in the degree-lexicographical order and let $M(p_l)$ be the subset of $\{I_1, \ldots, I_k\}$ of multiplicative variables for p_l. Assign the degree $d_j := \deg(i_j)$ to I_j and let D_l be the resulting degree for the leading monomial of p_l. Then the* HILBERT *series of $\mathbb{C}[i_1, \ldots, i_k]$ is given by*

$$\sum_i \mathrm{Dim}(\mathbb{C}[i_1, \ldots, i_k] \cap \mathbb{C}[x_1, \ldots, x_n]_i) s^i = \prod_{j=1}^{n} \frac{1}{1 - s^{d_j}} - \sum_{l=1}^{r} s^{D_l} \prod_{I_j \in M(p_l)}^{n} \frac{1}{1 - s^{d_j}}$$

Proof: The TAYLOR expansion at $s = 0$ of $\prod_{j=1}^{n} \frac{1}{1-s^{d_j}}$ is the generating function for the number of monomial is $\mathbb{C}[I_1, \ldots, I_k]$ according to the degrees. $s^{D_l} \prod_{I_j \in M(p_l)}^{n} \frac{1}{1-s^{d_j}}$ counts the homogeneous generators of $\ker \sigma$, which are multiples of p_l by multiplicative variables. Each $\mathbb{C}$-basis vector of $\ker \sigma$ has a unique representation as a product of some p_l by multiplicative variables. Hence the sum of the $s^{D_l} \prod_{I_j \in M(p_l)}^{n} \frac{1}{1-s^{d_j}}$ has to be subtracted from the complete $\prod_{j=1}^{n} \frac{1}{1-s^{d_j}}$ to obtain the generating function for the monomials which map onto a basis of $\mathbb{C}[i_1, \ldots, i_k]$. q. e. d.

Please note, the last result also indicates an alternative of computing the HILBERT series, which is commonly used in the JANET approach, even if the the generators are not homogeneous: One simply assign the degree 1 to each indeterminate I_i and the same formula yields the answer. At the moment we have not pursued the point further, how to read off a free resolution from the JANET data, cf.

Coming to the second point of slow performance for the elimination of the x_j. This we have overcome by a simple use of linear algebra. Here is the algorithm to produce elements and finally generators of the kernel. This algorithm has been implemented by D. Roberts in MAPLE as part of the package INVOLUTIVE. Recall that we assigned degrees $d_l = \deg(i_l)$ to the generators I_l of $\mathbb{C}[I_1, \ldots, I_k]$ thus defining a new grading for the polynomial ring $\mathbb{C}[I_1, \ldots, I_k]$. Denote the homogeneous components of degree i of $\mathbb{C}[I_1, \ldots, I_k]$ by $\mathbb{C}[I_1, \ldots, I_k]_i$.

Algorithm 3.2 *Input: Homogeneous polynomials $i_1, \ldots, i_k \in \mathbb{C}[x_1, \ldots, x_n]$ and a degree $d \in \mathbb{N}$.*
Output: For each $i, 0 \leq i \leq d$ (linearly independent) elements $b_1^{(i)}, \ldots, b_{\delta(i)}^{(i)} \in \mathbb{C}[I_1, \ldots, I_k]_i$ such that

$$(\sigma(b_1^{(i)}), \ldots, \sigma(b_{\delta(i)}^{(i)}))$$

is a $\mathbb{C}$-basis for

$$\sigma(\mathbb{C}[I_1, \ldots, I_k]_i) = \mathbb{C}[i_1, \ldots, i_k]_i$$

and elements $p_1^{(i)}, \ldots, p_{\rho(i)}^{(i)} \in \mathbb{C}[I_1, \ldots, I_k]_i$ such that

$$p_1^{(1)}, \ldots, p_{\rho(1)}^{(1)}, \ldots p_{\rho(i)}^{(i)}$$

multiplied by the monomials of $\mathbb{C}[I_1, \ldots, I_k]$ of appropriate degrees generate the kernel of σ restricted to $\mathbb{C}[I_1, \ldots, I_k]_i$ as a $\mathbb{C}$-vector space.
Algorithm: Assume that the data for $\mathbb{C}[I_1, \ldots, I_k]_j$ for $j = 1, \ldots, i-1$ are available already as sequences $b^{(j)}$ and $p^{(j)}$. Form the set

$$R_i := \{I_l | d_l = i\} \cup \{b_r^{(j)} b_s^{(i-j)} | 1 \leq j \leq \frac{i}{2}, 1 \leq r \leq \rho(j), 1 \leq s \leq \rho(i-j)\} \subset \mathbb{C}[I_1, \ldots, I_k]_i.$$

Select $b_1^{(i)}, \ldots, b_{\rho(i)}^{(i)} \in R_i$ maximal with the property that $(\sigma(b_1^{(i)}), \ldots, \sigma(b^{(i)})$ is $\mathbb{C}$-linearly independent in $\mathbb{C}[i_1, \ldots, i_k]_i$, i. e. is a $\mathbb{C}$-basis of $\mathbb{C}[i_1, \ldots, i_k]_i$. Each of the remaining elements r of R_i yields an element of the form $r - \sum a_s(r) b_s^{(i)} \in \ker \sigma$ with unique $a_s(r) \in \mathbb{C}$ as an element of the sequence $p^{(i)}$.

This rather obvious algorithm serves two purposes: to compute the dimensions of the $\mathbb{C}[i_1, \ldots, i_k]$ and to produce relations, which ultimately will generate $\ker \sigma$. The delicate point of course is the choice of the parameter d, which in general might have to be chosen rather big. It seems however that the case of invariant rings is not so bad behaved. On the other hand, one can easily construct examples, outside the range of invariant theory, where the JANET algorithm with lexicographic elimination order is faster than the above algorithm. The slow performance of the later occurs usually if the invariants are complicated, e. g. more than 2 variables and substantial degrees and many summands.

Summerizing we end up with a presentation which might not contain enough relators. Two situations are possible: One has enough generators. This case is favourable and treated below. Or some generators are missing. Even if the above algorithm does not go far enough to detect this, it is most unlikely that the resulting HILBERT series is equal to the MOLIEN series, e. g. that the missing relators compensate the missing generators.

NOETHER's result that the invariants of degree $\leq |G|$ has a relative version, cf. has a relative variant, as follows: If $U \leq G$ is a subgroup whose ring of invariants is generated by invariants of degrees $\leq b$, then the ring of G-invariants is generated by invariants of degrees $\leq b|G:U|$. With this result and the help of the above algorithm one can often get a reasonable bound d in 3.2 until where one has to check. Hence we are left with an easier problem.

Problem 2 : Given homogeneous invariants $i_1, \ldots, i_k$ generating $\mathbb{C}[x_1, \ldots, x_n]^G$. Find a presentation for $\mathbb{C}[x_1, \ldots, x_n]^G$ in these generators.

Now the setup above can be used to construct relators, use the JANET's algorithm for computing the HILBERT series and thus obtain a proof that the presentation is complete, in case HILBERT and MOLIEN series agree, and to rerun algorithm 3.2, in case there are coefficients in the HILBERT series which are bigger than the corresponding coefficients in the MOLIEN series. Ultimately this procedure has to come to an end. It can easily be arranged that one gets a minimal set of generators.

4 Examples

As a first example we reproduce a MAPLE-session using the package INVOLUTIVE to find a presentation of the ring of invariants of the matrix group

$$O := \langle \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \rangle$$

and it subgroup G of determinant 1 elements. Here is the MAPLE-session with complete details. The commands are self explanatory in view of the last section.

First group: O:=(C_2 wr C2) wr C_2 of degree 4.

Problem: Find presentation for the ring I(O) of invariants of O.

Note the group O contains a reflection subgroup of index 2 the ring of invariants of which is generated by x^2+y^2,z^2+u^2,x^2*y^2,z^2*u^2. By the refinement of Noether's Theorem the O-invariants up to degree 8 generate the ring of O- invariants.

```
> restart;
> with(jets): with(Involutive):
```

GAP yields the following Molien series for O:

```
> m0 := (1+s^6) / ((1-s^8)*(1-s^4)^2*(1-s^2));
```

$$mO := \frac{1+s^6}{(1-s^8)\,(1-s^4)^2\,(1-s^2)}$$

```
> taylor(m0, s=0, 20);
```

$$1 + s^2 + 3\,s^4 + 4\,s^6 + 8\,s^8 + 10\,s^{10} + 16\,s^{12} + 20\,s^{14} + 29\,s^{16} + 35\,s^{18} + \mathrm{O}(s^{20})$$

```
> var_erz := [[], [p1=x^2+y^2+z^2+u^2], [],
> [p2=x^4+y^4+z^4+u^4, p3=x^2*y^2+z^2*u^2], [],
> [p4=x^6+y^6+z^6+u^6],[], [p5=x^8+y^8+z^8+u^8]];
```

$var\_erz := [[],\ [p1 = x^2 + y^2 + z^2 + u^2],\ [],\ [p2 = x^4 + y^4 + z^4 + u^4,\ p3 = x^2\,y^2 + z^2\,u^2],\ [],$
$[p4 = x^6 + y^6 + z^6 + u^6],\ [],\ [p5 = x^8 + y^8 + z^8 + u^8]]$

```
> l := relations(var_erz, 12):
```

$$0; 1; 0; 3; 0; 4; 0; 8; 0; 10; 0; 16$$

These numbers are the dimensions of the spaces of invariants of degrees 1 to 12 which generated by the products of the invariants p1, .. ,p5. Since these numbers agree with the coefficients in the expansion of the Molien series, we have proved now that the ring of O-invariants is generated by p1, .. ,p5. Clearly none of the generators can be omitted. We also obtain the following relations among the pi's:

```
> l[1];
```

$$[\frac{3}{8}\,p1^2\,p2^2 + \frac{1}{2}\,p2\,p5 - \frac{1}{3}\,p1\,p2\,p4 + \frac{1}{2}\,p1^2\,p3\,p2 + \frac{2}{9}\,p1^3\,p4 - \frac{1}{6}\,p1^4\,p2 - \frac{1}{2}\,p1^2\,p3^2 - \frac{1}{4}\,p1^2\,p5 - p1\,p3\,p4 - \frac{1}{2}\,p2^2\,p3 + \frac{1}{72}\,p1^6 + p3^3 + p3\,p5 - \frac{1}{9}\,p4^2 - \frac{1}{4}\,p2^3 + \frac{1}{2}\,p2\,p3^2]$$

```
> J:=InvolutiveBasis(l[1], l[2]);
```

$$J := [27\,p1^2\,p2^2 + 36\,p2\,p5 - 24\,p1\,p2\,p4 + 36\,p1^2\,p3\,p2 + 16\,p1^3\,p4 - 12\,p1^4\,p2 - 36\,p1^2\,p3^2 - 18\,p1^2\,p5 - 72\,p1\,p3\,p4 - 36\,p2^2\,p3 + p1^6 + 72\,p3^3 + 72\,p3\,p5 - 8\,p4^2 - 18\,p2^3 + 36\,p2\,p3^2]$$

```
> h0 := PolHilbertSeriesNeu(l[3], s);
```

$$hO := \frac{1}{(1-s^2)\,(1-s^4)^2\,(1-s^6)\,(1-s^8)} - \frac{s^{12}}{(1-s^2)\,(1-s^4)^2\,(1-s^6)\,(1-s^8)}$$

```
> simplify(m0-h0);
```

$$0$$

Since the Hilbert series agrees with the Molien series and since we started out with generators, we have proved that the relator above yields a presentation for the ring of invariants of O.

We now proceed to the subgroup G of O consisting of all matrices of determinant 1 in O.
Problem: Find a presentation for the ring I(G) of invariants of G.

GAP yield the following Molien series.

```
> mG := (1+s^6+s^8+s^14) / ((1-s^8)*(1-s^4)^2*(1-s^2));
```

$$mG := \frac{1+s^6+s^8+s^{14}}{(1-s^8)\,(1-s^4)^2\,(1-s^2)}$$

```
> taylor(mG,s=0,28);
```

$$1 + s^2 + 3\,s^4 + 4\,s^6 + 9\,s^8 + 11\,s^{10} + 19\,s^{12} + 24\,s^{14} + 37\,s^{16} + 45\,s^{18} + 63\,s^{20} + 76\,s^{22} + 101\,s^{24} + 119\,s^{26} + \mathrm{O}(s^{28})$$

Since 1+s^6+s^8+s^14= (1+s^6)(1+s^8) we expect that I(G) viewed as I(O)-module to be free with basis

1 and some G-invariant of degree 8. To find a suitable invariant of degree 8 one factors the Jacobi determinant of

p1,p2,p3, p5 to find the G-invariant p6.

```
> var_erz := [[], [p1=x^2+y^2+z^2+u^2], [],
> [p2=x^4+y^4+z^4+u^4, p3=x^2*y^2+z^2*u^2], [],
> [p4=x^6+y^6+z^6+u^6], [], [p5=x^8+y^8+z^8+u^8,
> p6=x*u*y*z*(u-z)*(u+z)*(x-y)*(x+y)]];
```

$$var\_erz := [[], [p1 = x^2+y^2+z^2+u^2], [], [p2 = x^4+y^4+z^4+u^4,\ p3 = x^2\,y^2+z^2\,u^2], [],$$
$$[p4 = x^6+y^6+z^6+u^6], [],$$
$$[p5 = x^8+y^8+z^8+u^8,\ p6 = x\,u\,y\,z\,(u-z)\,(u+z)\,(x-y)\,(x+y)]]$$

```
> l := relations(var_erz, 16):
```

$$0; 1; 0; 3; 0; 4; 0; 9; 0; 11; 0; 19; 0; 24; 0; 37;$$

Comparing these dimensions with the coefficients of the Molien series makes us suspect that p1 to p6 generate I(G). However, this is no proof this time. We also have obtained a list of 21 relations, too long to be reproduced here:

```
> nops(l[1]);
```

$$21$$

```
> JG:=InvolutiveBasis(l[1],l[2]):
> nops(JG);
```

$$24$$

Whereas the coefficients in the original relations (contained in l[1]) were rather small, quite a few coefficients in the Janet basis get rather big (30 digits and more).

```
> hG := PolHilbertSeriesNeu(l[3], s);
```

$$\begin{aligned} hG := & \frac{1}{(1-s^2)(1-s^4)^2(1-s^6)(1-s^8)^2} - \frac{s^{16}}{(1-s^4)^2(1-s^6)(1-s^8)^2} \\ & - \frac{s^{12}}{(1-s^2)(1-s^4)^2(1-s^6)(1-s^8)^2} - \frac{s^{20}}{(1-s^4)(1-s^6)(1-s^8)^2} \\ & - \frac{s^{18}}{(1-s^4)^2(1-s^6)(1-s^8)^2} - \frac{s^{24}}{(1-s^6)(1-s^8)^2} - \frac{s^{24}}{(1-s^4)(1-s^6)(1-s^8)^2} \\ & - \frac{s^{22}}{(1-s^4)(1-s^6)(1-s^8)^2} - \frac{s^{28}}{(1-s^4)(1-s^6)(1-s^8)^2} \\ & - \frac{s^{28}}{(1-s^4)^2(1-s^6)(1-s^8)^2} - \frac{s^{26}}{(1-s^4)^2(1-s^6)(1-s^8)^2} - \frac{s^{28}}{(1-s^6)(1-s^8)^2} \\ & - 2\frac{s^{32}}{(1-s^4)(1-s^6)(1-s^8)^2} - \frac{s^{26}}{(1-s^4)(1-s^6)(1-s^8)^2} \\ & - \frac{s^{30}}{(1-s^4)(1-s^6)(1-s^8)^2} - \frac{s^{36}}{(1-s^4)(1-s^6)(1-s^8)^2} - \frac{s^{34}}{(1-s^4)(1-s^6)(1-s^8)^2} \\ & - \frac{s^{40}}{(1-s^4)(1-s^6)(1-s^8)^2} - \frac{s^{38}}{(1-s^4)(1-s^6)(1-s^8)^2} - \frac{s^{44}}{(1-s^4)(1-s^6)(1-s^8)^2} \\ & - \frac{s^{42}}{(1-s^4)(1-s^6)(1-s^8)^2} - \frac{s^{48}}{(1-s^4)^2(1-s^6)(1-s^8)^2} \\ & - \frac{s^{46}}{(1-s^4)(1-s^6)(1-s^8)^2} - \frac{s^{50}}{(1-s^4)^2(1-s^6)(1-s^8)^2} \end{aligned}$$

```
> simplify(mG-hG);
```

$$0$$

Hence we believe that we have a presentation for I(G). But the final proof now goes as follows: Obviously I(O)1 +I(O)p6 is a free I(O)-module of rank 2 contained in I(G). We want to show equality. But this follows from comparing the Molien series mG of I(G) with (1+s^8)mO, which turn out to be equal. Note now we know that I(G) is generated by p1 to p6 and hence we have a presentation for I(G).

The next (rather small) example is to demonstrate how much one can do, if one follows the obvious approach outlined at the beginning of the last section, by getting a JANET basis or involutive basis, as it is called in the polynomial case in the package for the generators x_i and I_j with relators $I_j - i_j$ in the notation of the alst section. The group chosen here is

$$G := \langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \rangle \leq H := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \rangle$$

Note, H is a reflection group, which keeps things easy. Here comes the MAPLE-session with comments:

```
> with(jets): with(Involutive):
```

The ring I(G) of invariants of G (isomorphic to C_4) is clearly generated by x^2+y^2, x^2*y^2,x^3*y-y^3*x.

Below we finde an involutive basis for the three relations given in L in the lexicographic ordering. Note that q4 comes earlier in this orderring than p2 and p4, corresponding to the H-invariants x^2+y^2, x^2*y^2.

```
> L:=[p2-(x^2+y^2),p4-x^2*y^2, q4-(x^3*y-y^3*x)];
```

$$L := [p2 - x^2 - y^2,\ p4 - x^2\,y^2,\ q4 - x^3\,y + y^3\,x]$$

```
> Lvars:=[x,y,q4,p2,p4];
```

$$Lvars := [x,\ y,\ q4,\ p2,\ p4]$$

```
> B:=InvolutiveBasis(L,Lvars,1);
```

$$\begin{aligned}
B := [&q4^2 - p2^2\,p4 + 4\,p4^2,\ y\,q4^2 - y\,p4\,p2^2 + 4\,y\,p4^2,\ y^2\,q4^2 - p2^2\,p4\,y^2 + 4\,p4^2\,y^2,\\
&y^3\,q4^2 - p2^2\,p4\,y^3 + 4\,p4^2\,y^3,\ p4 - y^2\,p2 + y^4,\\
&-p2\,y^3\,q4 + y\,p2^2\,q4 - p2^2\,x\,p4 + 4\,x\,p4^2 - 2\,p4\,y\,q4,\ x\,q4 + y^3\,p2 - y\,p2^2 + 2\,y\,p4,\\
&4\,y\,x\,p4 - 2\,y^2\,q4 + p2\,q4 - y\,x\,p2^2,\ -x\,y\,q4 - 2\,y^2\,p4 + p2\,p4,\\
&-2\,y^2\,x\,p4 + y^3\,q4 - y\,p2\,q4 + p2\,x\,p4,\ 2\,x\,p4 - x\,y^2\,p2 - y\,q4,\\
&-x\,y^2\,q4 - 2\,y^3\,p4 + y\,p4\,p2,\ q4 + 2\,y^3\,x - y\,x\,p2,\ p2 - x^2 - y^2]
\end{aligned}$$

There are three possibilities for the normal form of a polynomial p in x and y with respect to the involutive basis B: Either the normal form only involves p2 and p4, which is tantamount to p being an H-invariant, or it also involves q4, saying that p is G-invariant but not H-invariant, or it involves some x or y, in which case it is not H-invariant.

```
> PolInvReduce((x^2+(x^2-y^2)^3)^2+(y^2+(x^2-y^2)^3)^2,B,Lvars);
```

$$2\,p2^6 - 4\,y^2\,p2^3 - 24\,p2^4\,p4 + 2\,p2^4 + 16\,y^2\,p2\,p4 + 96\,p2^2\,p4^2 - 8\,p2^2\,p4 - 128\,p4^3 + p2^2 - 2\,p4$$

```
> PolInvReduce((x-y)^3,B,Lvars);
```

$$2\,y^2\,x + 2\,y^3 + x\,p2 - 3\,y\,p2$$

```
> PolInvReduce(x^7*y^3-x^3*y^7,B,Lvars);
```

$$p2\ q4\ p4$$

That the Hilbert series with the degrees given as below takes the simple form 1/(1-s)^2 corresponds to the fact that the ring for which B is an involutive basis is isomorphic to the polynomial ring in x and y.

```
> h:=PolHilbertSeriesNeu([x=1,y=1,q4=4,p2=2,p4=4], s);
```

$$\begin{aligned}
h := &\frac{1}{(1-s)^2\,(1-s^4)^2\,(1-s^2)} - \frac{s^8}{(1-s^4)^2\,(1-s^2)} - \frac{s^9}{(1-s^4)^2\,(1-s^2)} - \frac{s^{10}}{(1-s^4)^2\,(1-s^2)}\\
&- \frac{s^{11}}{(1-s^4)^2\,(1-s^2)} - 2\,\frac{s^4}{(1-s)\,(1-s^4)^2\,(1-s^2)} - \frac{s^9}{(1-s^4)\,(1-s^2)}\\
&- \frac{s^5}{(1-s^4)^2\,(1-s^2)} - \frac{s^6}{(1-s^2)\,(1-s^4)} - \frac{s^6}{(1-s^2)\,(1-s^4)^2} - \frac{s^7}{1-s^4}\\
&- \frac{s^5}{(1-s^4)\,(1-s^2)} - \frac{s^7}{(1-s^4)^2\,(1-s^2)} - \frac{s^2}{(1-s)^2\,(1-s^4)^2\,(1-s^2)}
\end{aligned}$$

```
> simplify(h);
```

$$\frac{1}{(-1+s)^2}$$

Finally the commad NotHas extracts from B all relations not involving x or y, thus yielding a presentation for I(G) on the generators p2,p4,q4.

```
> R:=NotHas(B,[x,y]);
```

$$R := [q4^2 - p2^2\, p4 + 4\, p4^2]$$

5 Some refined techniques

One problem that was not solved satisfactorily in Section 3 was how to prove that one had generators for the ring of invariants in order to conclude from the equality of the HILBERT series and the MOLIEN series that one had a presentation of the ring of invariants. We give some hints in this section, how to use the JANET algorithm directly on the invariants towards this aim. At the same time, this technique can used to obtain a standard expression of any given invariant in terms of the generators. The theoretical concept used in this section is the fact that the ring $I(G)$ of invariants of a finite complex matrix group $G \leq \mathrm{GL}(n, \mathbb{C})$ is COHEN-MACAULY, cf. [Ben 93] pg. 50. This implies that there exist n homogeneous invariants, $f_1, \ldots, f_n \in I(G)$, which form a system of parameters, i. e., which are algebraically independent and have the property that $I(G)$ is a free $\mathbb{C}[f_1, \ldots, f_n]$-module of finite rank.

Proposition 5.1 *Let $f_1, \ldots, f_n \in I(G)$ be homogeneous. The following three statements are equivalent.*
1) $f_1, \ldots, f_n$ form a set of parameters for $I(G)$.
2) $f_1, \ldots, f_n$ form a set of parameters for $\mathbb{C}[x_1, \ldots, x_n]$.
3) $\mathbb{C}[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$ is a finite dimensional $\mathbb{C}$ algebra.
Moreover, if the cosets of $b_1, \ldots, b_t \in \mathbb{C}[x_1, \ldots, x_n]$ form a $\mathbb{C}$-basis for $\mathbb{C}[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$, then $I(G)$ is generated by the f_i and the $\pi(b_j)$ with π as defined at the end of Section 2.

Proof: Obviously all three conditions imply that $f_1, \ldots, f_n$ are algebraically independent so that we only have to deal with the other issues. The implication o 2) implies 1) can be taken from the poof of Theorem 4.3.6 in [Ben 93] , where the COHEN-MACAULY property of the ring of invariants is proved. The reversed implication follows form Theorem 4.3.5 in [Ben 93]. That 2) implies 3) is obvious. We shall see how the JANET algorithm can be modified to obtain a constructive proof of the implication 3) to 2), which at the same time yields an algorithm to construct a $\mathbb{C}[f_1, \ldots, f_n]$-basis of $\mathbb{C}[x_1, \ldots, x_n]$ or with some more effort of $I(G)$ and how to express any given element of $\mathbb{C}[x_1, \ldots, x_n]$ resp. $I(G)$ in this basis. In fact, we shall formulate this part of the proof as an algorithm, which is slightly more general than the situation considered here. q. e. d.

Algorithm 5.2 *Input: Algebraically independent elements $f_1, \ldots, f_n \in \mathbb{C}[x_1, \ldots, x_n]$ such that*

$$\mathbb{C}[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$$

is finite dimensional.
Output: A $\mathbb{C}[f_1, \ldots, f_n]$-basis $(b_1, \ldots b_s)$ of $\mathbb{C}[x_1, \ldots, x_n]$ and a procedure to express any given element of $\mathbb{C}[x_1, \ldots, x_n]$ in this basis.
Algorithm: Perform the usual JANET*-algorithm on $f_1, \ldots, f_n$ with the usual degree lexicographical ordering with the following variation: Instead of starting with $f_1, \ldots, f_n$, introduce a symbol a_i for each f_i, start out with the pairs $(f_i; a_i)$, and perform all the operations in both components, e. g. multiplication with x_j, addition and subtraction. The operations are done according to the usual rules coming from the first components, so that one ends up with $(r_j; \sum r_{ji} a_i)$, where the $r_j \in \mathbb{C}[x_1, \ldots, x_n]$ form a* JANET*-basis for the ideal generated by $f_1, \ldots, f_n$ and the r_{ji} lie in $\mathbb{C}[x_1, \ldots, x_n]$.*
The $\mathbb{C}[f_1, \ldots, f_n]$-basis of $\mathbb{C}[x_1, \ldots, x_n]$ is given by all monomials in $\mathbb{C}[x_1, \ldots, x_n]$, which do not occur as a leading monomial of some polynomial of $(f_1, \ldots, f_n)$, i. e. which are not multiples of the leading monomials of the r_j in the JANET *basis.*
Procedure to express a given element h of $\mathbb{C}[x_1, \ldots, x_n]$ in the above basis: Perform involutive division on h with the $r_j - \sum r_{ji} a_i$ (instead of the usual r_j). In this process one builds up linear combinations of monomials of the a_i, the coefficients of which are polynomials in $x_1, \ldots, s_n$. These coefficients are processed according to the JANET*-rules, until the process terminates, i. e. only monomials of the constructed basis occur. Now one rewrites the expression as a sum of the basis elements with polynomials in the a_i as coefficients.*

Proof: That the algorithm terminates is clear from JANET's algorithm. That the procedure terminates is also clear for the same reason. The procedure shows that the momomials representing a $\mathbb{C}$-basis of $\mathbb{C}[x_1,\ldots,x_n]/(f_1,\ldots,f_n)$ form a generating set for $\mathbb{C}[x_1,\ldots,x_n]$ as $\mathbb{C}[f_1,\ldots,f_n]$-module. Tensoring with the $\mathbb{C}[f_1,\ldots,f_n]$-module $\mathbb{C}$, where all f_i act on $\mathbb{C}$ as multiplication by 0, shows that the rank of $\mathbb{C}[x_1,\ldots,x_n]$ as $\mathbb{C}[f_1,\ldots,f_n]$-module is equal to the number of these monomials. It follows they even form a set of free generators, since the matrices over $\mathbb{C}[f_1,\ldots,f_n]$ expressing one by the others are quadratic and therefore inverse to each other. q. e. d.

It is clear that the modified JANET algorithm 5.2 does everything one can hope for from the side of commutative algebra: It decides whether given homogeneous invariants $f_1,\ldots,f_n$ form parameters for the invariant ring, by checking the finite dimensionality of $\mathbb{C}[x_1,\ldots,x_n]/(f_1,\ldots,f_n)$. Once this is established, it expresses each new invariant in the normal form by the procedure of the algorithm and thereby enables one to quickly find the free generators b_i of $I(G)$ as $\mathbb{C}[x_1,\ldots,x_n]$-module. So one has

$$I(G) = \bigoplus_i \mathbb{C}[f_1,\ldots,f_n]b_i.$$

And finally once the b_i are given in the normalform, it can also by a slight extension of involutive division express each given invariant as a linear combination of the b_i with coefficients in $\mathbb{C}[f_1,\ldots,f_n]$. Finally, it therefore is also able to quickly derive a presentation of $I(G)$, simply by expressing the products b_ib_j in this normal form.

References

[Ben 93] D. J. Benson, Polynomial Invariants of Finite Groups. LMS Lecture Notes 190, Cambridge Univ. Press 1993.

[GeB 98a] V. P. Gerdt, Y. A. Blinkov, Involutive bases of polynomial ideals. Mathem. and Computers in Simulation 45 (1998), 519-541.

[GeB 98b] V. P. Gerdt, Y. A. Blinkov, Minimal involutive bases. Mathem. and Computers in Simulation 45 (1998), 543-560.

[Kem 98] G. Kemper, Computational Invariant Theory. The Curves Seminar at Queen's, Volume XII, in: Queen's Papers in Pure and Applied Math. 114 (1998), 3-26.

[Kem 99] G. Kemper, HILBERT Series and degree bounds in invariant theory. in: B. Heinrich Matzat, Gert-Martin Greuel, Gerhard Hiss, eds, Algorithmic Algebra and Number Theory, Springer-Verlag, Heidelberg, 1999.

[Pom 94] J.- F. Pommaret, Partial Differential Equations and Group Theory. Kluver Academic Publishers 1994.

[Sta 79] R. P. Stanley, Invariants of finite groups. AMS Bulletin vol. 1, No. 3 (1979), 475-511.

[Stu 93] B. Sturmfels, Algorithms in Invariant Theory. Springer 1993.

Author's address:
RWTH Aachen, Lehrstuhl B für Mathematik
Templergraben 64
52062 Aachen, Germany
e-mail: plesken@willi.math.rwth-aachen.de