V. L. POPOV

Constructive invariant theory


<http://www.numdam.org/item?id=AST_1981__87-88__303_0>
CONSTRUCTIVE INVARIANT THEORY

V.L. Popov - Moscow

1. Let $k$ be an algebraically closed field, $\text{char } k = 0$.

We denote by $V$ an $n$-dimensional coordinate linear space (of columns) over $k$, by $\text{Mat}_n$ the space of all $n \times n$-matrices with its coefficients in $k$ and by $\text{GL}_n$ the subgroup of all nondegenerate matrices in $\text{Mat}_n$. We use the notation $(a_{ij})$ for an element of $\text{Mat}_n$: this is the matrix with the coefficient $a_{ij}$ situated in its $i$-th row and $j$-th column, $1 \leq i, j \leq n$. Let us denote also by $x_i^g$, $1 \leq i \leq n$, and resp. by $x_{ij}^g$, $1 \leq i, j \leq n$, the coordinate functions on $V$, resp. $\text{Mat}_n$, with respect to the canonical basis

\[
\begin{pmatrix}
  a_1 \\
  \vdots \\
  a_n
\end{pmatrix}
\]

(i.e. $x_i^g(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}) = a_i$ and $x_{ij}^g(\begin{pmatrix} a_{pq} \end{pmatrix}) = a_{ij}$).

Let $G$ be a reductive algebraic subgroup of $\text{GL}_n$. The group $\text{GL}_n$ (and hence also $G$) acts in a natural way on $V$ (by means of a multiplication of a matrix by a column). This action defines an action of $\text{GL}_n$ on an algebra $k[V] = k[x_1, \ldots, x_n]$ of all polynomial functions on $V$. Let $k[V]^G$ be the subalgebra of $G$-invariants. This is a finitely generated graded subalgebra.

The problem of constructive invariant theory is to find explicitly a minimal (i.e. noneliminatable) system of homogeneous generators of $k[V]^G$. This means, from the theoretical point of view, that we must find such an algorithm that provides in principle a specified system by means of a finite number of effectively feasible operations (of course, from a practical point of view, a question arises immediately about the amount of all needed calculations, but it is already another side of the problem that
is connected with an improvement of the corresponding estimates or with a choice of a more effective algorithm but not with the existence of the algorithm itself). Solving this problem one assumes that G itself is "known", i.e. that one can solve in an effective way certain questions about its structure. Thus, the central concern mainly of this paper is with the case of a connected semisimple group G and we assume that the following data are known:

a) the Lie algebra Lie G of G (we consider Lie G as a linear subspace in Mat_n and it will be sufficient to know for instance the set of matrices that is a basis of this subspace),

b) a maximal torus T of G (we consider T as an image of a standard torus k^r = k^* x ... x k^* under a known homomorphism

(1) \( \phi: k^r \rightarrow GL_n, \phi((a_1, ..., a_r)) = (f_{ij}(a_1, ..., a_r)), \)

where \( f_{ij}(t_1, ..., t_r), 1 \leq i,j \leq n, \) are known rational functions of the canonical coordinate function \( t_s, 1 \leq s \leq r, \) on \( k^r, \)
i.e. \( t_s((a_1, ..., a_r)) = a_s. \)

For example, a typical situation occurs in the invariant theory when G is an image of a known standard group G' under a known homomorphism (say, G' = SL_m and G is its image under a natural representation in a space of forms of a given degree in m variables). Clearly, if one knows the Lie algebra and a maximal torus of G', then one also knows a) and b) for G itself.

Now, an algorithm for finding explicitly a minimal system of homogeneous generators of \( k[V]^G \) being given, one can in principle calculate such a constant \( M \in \mathbb{N}, \) that \( k[V]^G \) is generated by a subspace

(2) \( \bigoplus_{d=0}^{M} k[V]^G_d \)
CONSTRUCTIVE INVARIANT THEORY

(here and further $R_d$ is a space of all homogeneous elements of degree $d$ of an arbitrary $\mathbb{N}$-graded $k$-algebra $R$). On the contrary, if it is known that for a certain $M \in \mathbb{N}$ the subspace (2) generates the algebra $k[V]^G$, one can in principle find explicitly a minimal system of homogeneous generators of this algebra. Let us show how it can be done.

First of all one can explicitly describe the subspace $k[V]_d^G$ of $k[V]_d$ for any concrete $d$. It is as follows. If $G$ is finite then $k[V]_d^G$ is clearly a linear span of $\frac{1}{|G|} \sum_{g \in G} g.f$, as $f$ ranges over all monomials in $x_1, \ldots, x_n$ of degree $d$. If $G$ is connected then $k[V]_d = \{f \in k[V]_d | (\text{Lie } G)f = 0\}$ with respect to the natural action of Lie $G$ by means of differentiations of the algebra $k[V]$. Therefore, the question in this case is reduced to solving the corresponding system of linear equations. In general, the question can be reduced to the above two cases.

Let now $d_1$ be such a minimal integer, $0 < d_1 < M$, that $k[V]_{d_1}^G \neq 0$. Let us take a basis $f_1, \ldots, f_q$ of $k[V]_{d_1}^G$. Let $d_2$ be such a minimal integer, $d_1 < d_2 < M$, that $k[V]_{d_2}^G$ is not a linear span of all possible monomials in $f_1, \ldots, f_q$ that lie in $k[V]_{d_2}^G$. Let $g_1, \ldots, g_p$ be a basis of an arbitrary linear supplement to this linear span in $k[V]_{d_2}^G$. Analogously, let $d_3$ be such a minimal integer, $d_2 < d_3 < M$, that $k[V]_{d_3}^G$ is not a linear span of all possible monomials in $f_1, \ldots, f_q, g_1, \ldots, g_p$ that lie in $k[V]_{d_3}^G$, and let $h_1, \ldots, h_s$ be a basis of an arbitrary linear supplement to this linear span in $k[V]_{d_3}^G$ and so forth. This process will stop after a finite number of steps and it is not difficult to see that a finite set of polynomials $f_1, \ldots, f_q, g_1, \ldots, g_p, h_1, \ldots, h_s, \ldots$ is in fact a minimal system of homogeneous generators of the algebra $k[V]^G$ and that an arbitrary system of such type is obtained by this procedure (it also follows
from this that a minimal system of homogeneous generators of 
\( k[V]^G \) is defined, in a sense, in a unique way; specifically, 
the number of such generators is well defined and equal to 
\( \dim I_+/I_+^2 \), \( I_+ \) being the ideal in \( k[V]^G \) generated by the homogeneous 
elements of strictly positive degree).

So we see that the problem of the constructive invariant 
theory is in fact equivalent to the problem of the finding 
of a number \( M \). The problem of the case in which \( G \) is finite has 
already been solved by E. Noether, [10], [17], who proved that 
one can take \( M = |G| \) (and hence \( \dim I_+/I_+^2 < \binom{|G|+n}{n} \)). The problem 
is by no means so satisfactorily solved when \( G \) is a connected 
group. Of course, there are a lot of such concrete groups \( G \) 
when a minimal system of homogeneous generators of \( k[V]^G \) is 
explicitly described. Nevertheless, it seems that in its general 
setting the problem was considered only by Hilbert in [4] and 
(following Hilbert's idea) in [2] (in this paper \( G \) is an image 
of \( SL_m \) under a homogeneous polynomial homomorphism).

Hilbert gives two similar approaches to the problem. The first 
one reduces it to "a solution of an elementary problem from the 
arithmetic theory of algebraic functions"; more precisely, to 
the Kronecker method for the constructing of a basis of the 
ingegral closure of a finitely generated domain in its field of 
fractions. The second one is a modification of the first which 
makes it possible to avoid a direct reference to the Kronecker 
method because of some specific properties of the algebras and 
fields under consideration. Hilbert tried to avoid a reference 
to the Kronecker method because he apparently understood that 
it gives only the general strategy (reducing the problem of 
finding of the estimates of the degrees of the certain equations,
CONSTRUCTIVE INVARIANT THEORY

calculating of its discriminants etc.), but leaves the question of an explicit calculation of M somewhat vague. As a matter of fact the same is related to his second approach and, as a result, a constant M was not in fact explicitly calculated (Hilbert refers, but only in passing, to his second approach when he remarks that "a closer examination also provides an upper bound for the weights of the invariants in a complete system which depends only on n"). All these circumstances were, I believe, the reason why the authors of [2] preserving Hilbert's main idea tried to change the final part of his general strategy, replacing the appeal to a method to describe the integral quantities (in such a form or another) by a reference to the Nullstellensatz (but again the constant M was not explicitly calculated in [2]).

Several aims will be pursued in this lecture. First, it will be shown how "the vagueness" related to the Kronecker method and its modifications by means of the recent achievements of the invariant theory (the theorem of Hochster and Roberts) can be avoided. Second, it will be shown how to generalize the main idea of Hilbert's paper [4] for the case of an arbitrary connected semisimple group G. It is to be hoped that this generalization will clarify to a certain extent the somewhat unexpected (and at a first glance accidental) role which the function \( a_{ij} \mapsto \det(a_{ij}) \) plays in Hilbert's theory. In the case under consideration an explicit estimate M can be obtained. This estimate is fantastically large and its radical improvement is apparently connected with the principal change in the approach itself. To be more precise, it will be shown that the degrees of a minimal system of homogeneous generators of \( k[V]^G \) are not greater than the number
(3) \[ M = \min \{ \text{minimal positive integer divisible by each } a \in \mathbb{Z}, a \leq 2^{r+s-n(s+1)(n-1)^{s-r}r^{s+1}!} 3^{s(s-r)/2} \} \]

where \( s = \dim G, r = \rk G, m \) is the transcendence degree over \( k \) of \( k[V]^G \) and \( t \) is the maximum of \( |m^k| \) taken over all \( 1 \leq k \leq r \) and all the monomials \( t_1^{m_1} \cdots t_r^{m_r} \) that occur in the polynomials \( f_{ij}(t_1, \ldots, t_r), 1 \leq i, j \leq n, \) of (1). For instance, if \( G \) is the image of \( SL_m \) under its natural representation in a space of forms of degree \( p \) in \( m \) variables, one can take \( t = p \). The reader will see that (3) can be slightly improved by means of more thoroughness in a number of places, but this was not attempted because it does not provide a principal improvement.

Third, an approach will be discussed, as suggested in [2], and it will be shown that in reality it does not provide a solution to the problem (unfortunately in the abstract of the present lecture [1] it was pointed out that Hilbert's approach is the same as in [2], but as a matter of fact this is not the case and it would not be correct to say that Hilbert's general strategy does not lead to the solution, although it however flawed by a certain vagueness). Interestingly, the error in [2] is connected with the certain ingenious properties of \( k[V]^G \). Several intriguing problems arise in this context.

These and other questions are discussed in nn. 7,8.

The following notations are fixed throughout:

- \( k[X] \) the algebra of regular functions of an algebraic variety \( X \),
- \( k^* \) multiplicative group of \( k \),

308
\[ N \text{ additive semigroup of nonnegative integers,} \]
\[ k[b_1, \ldots, b_d], \text{ resp. } k(b_1, \ldots, b_d) \text{ the algebra, resp.} \]
\[ \text{the field, generated by } b_1, \ldots, b_d \text{ over } k, \]
\[ G \text{ a connected semisimple algebraic group (if it is not otherwise stated).} \]

2. As it was proved by Hochster and Roberts, [6], \( k[V]^G \) is a Cohen-Macaulay algebra. This is equivalent to saying that if \( \theta_1, \ldots, \theta_m \) is a homogeneous system of parameters, i.e. \( k[V]^G \) is integral over

\[ P = k[\theta_1, \ldots, \theta_m], \]

then \( k[V]^G \) is a free module over \( P \). Let \( n_1, \ldots, n_\ell \) be a homogeneous system of generators of this module,

\[ k[V]^G = Pn_1 \oplus \ldots \oplus Pn_\ell. \]

We assume that

\[ \deg \theta_i = d_i, \quad d_1 \leq \ldots \leq d_m, \]
\[ \deg n_j = e_j, \quad 0 = e_1 \leq \ldots \leq e_\ell. \]

It follows from (4), (5) and (6) that the Poincaré series of \( k[V]^G \) is

\[ F(k[V]^G, x) = \sum_{d=0}^{\infty} \dim k[V]^G_{d} x^d = \frac{\sum_{i=1}^{\ell} e_i x^{d_i}}{\sum_{j=1}^{m} (1-x^{d_j})}. \]

A classical formula of Molien-Weyl makes it possible to calculate this rational function when \( k = \mathbb{C} \). More precisely, let \( K \) be a maximal compact subgroup of \( G \) such that \( K \cap T \) is a maximal

309
torus of \( K \). Let \( \alpha_1, \ldots, \alpha_{s-r} \) be the set of the roots of \( K \) with respect to \( K \cap T \) (we consider a root as a function on \( K \cap T \)) and \( W \) is the Weyl group of \( K \). Then, \([18]\),

\[
F(k[V]^G, x) = \frac{1}{|W|} \int_{K \cap T} \frac{(1-\alpha_1(g)) \cdots (1-\alpha_{s-r}(g))}{\det(1-xg)} \, du(g), \quad (|x| < 1),
\]

where \( du(g) \) is the normalized Haar-measure. The integral on the right side of (8) reduces to integrals over the unit circumference in \( C \) and can be calculated in principle by means of residues. In the special cases (say, when \( G \) is the image of \( SL_2 \) under an irreducible representation) other formulas are also known to calculate the Poincaré series, cf. \([11]\), \([12]\).

\( G \) being a connected semisimple, it follows that \( k[V]^G \) is Gorenstein, see \([6]\). This means (and in fact is equivalent because of Stanley's theorem, \([15]\)) that \( F(k[V]^G, x) \) satisfies the following functional equation

\[
F(k[V]^G, x^{-1}) = (-1)^m q^x F(k[V]^G, x),
\]

where \( q \in \mathbb{Z} \).

Using (7) we see that (9) is equivalent to

\[
\sum_{j=1}^l e_j = xq \sum_{j=1}^l e_j
\]

and it follows from (6) that (10) is equivalent to

\[
d_1 + \ldots + d_m - e_{\ell-i+1} = q+e_i, \quad i=1, \ldots, \ell.
\]

Specifically it follows from (11) that

\[
e_\ell = d_1 + \ldots + d_m - q
\]

and

\[
e_i + e_{\ell-i+1} = e_\ell, \quad i = 1, \ldots, \ell.
\]
CONSTRUCTIVE INVARIANT THEORY

In as much as we can in principle effectively find \( F(k[V]^G, x) \),
the number \( q \) is known. We need in reality to know only \( q \), but
not \( F(k[V]^G, x) \) itself. Several facts are known \textit{a priori} about \( q \)
(for instance, always \( q \geq 0 \), [8]). We shall discuss this question
in n.7.

It follows from (2) and (3) that \( \theta_1, \ldots, \theta_m, \eta_1, \ldots, \eta_k \) is a
homogeneous system of generators of the algebra \( k[V]^G \).
We conclude now from (6) and (12) that one can take \( M \) in (2) to
be equal to

\[
\text{(14) } \quad \max(d_1 + \ldots + d_m - q, d_m)
\]

But it is not generally the case that \( d_i, 1 \leq i \leq m \), are
known. One can not derive an upper boundary for these numbers
directly from \( F(k[V]^G, x) \) (for example, one can take \( \theta_1^{s_1}, \ldots, \theta_m^{s_m} \)
instead of \( \theta_1, \ldots, \theta_m \) for arbitrary \( s_i \in \mathbb{Z}, s_i > 0, 1 \leq i \leq m \),
and this set is again a homogeneous system of parameters of
\( k[V]^G \)). So the problem arises to find an \textit{a priori} upper estimate
of numbers \( d_1, \ldots, d_m \).

If it is known for instance that

\[
\text{(15) } \quad d_m \leq D
\]

then one can take \( M \) in (2) to be equal to

\[
\text{(16) } \quad \max(mD - q, D) \leq mD
\]

(It should be noted here that \( m \) is equal to the order of the
pole of \( F(k[V]^G, x) \) at \( x = 1 \), hence one can in principle effectively
find \( m \). Another way to calculate \( m \) follows from the equality
\( m = n - \dim Gv = n - s + \dim \{ X \in \text{Lie } G | Xv = 0 \} \), where \( v \) is a point of \( V \)
in general position).
Our concern now will be to find an upper estimate of the degrees of some homogeneous systems of parameters of \( k[V]^G \). As a matter of fact this problem was solved by Hilbert in [4], when \( G \) is an image of \( SL_d \) under a homogeneous polynomial representation.

3. We shall now show how to find \( D \) in general, by developing Hilbert’s idea.

The general plan is the following. Our starting point will be the following important theorem (for the first time proved by Hilbert in [4]):

Let \( Q \) be any finitely generated graded \( k \)-subalgebra of \( k[V]^G \). Then \( k[V]^G \) is integral over \( Q \) if and only if

\[
\{ v \in V \mid f(v) = 0 \text{ for every } f \in \mathfrak{g}_i, k[V]^G \} = \{ v \in V \mid h(v) = 0 \text{ for every } h \in \mathfrak{g}_i, Q \}.
\]

Denote by \( N \) the variety of zeros in \( V \) of the homogeneous elements of \( k[V]^G \) of strictly positive degree.

It is known that

\[
(17) \quad N = \{ v \in V \mid O \in Gv \}
\]

(we use bar to denote the closure in \( V \)). The points from \( V - N \) are called semi-stable.

Let us assume for a moment that we can find such an integer \( C > 0 \) that

\[
(18) \quad \text{for every semi-stable point } v \in V, \text{ there is a homogeneous polynomial } f_v \in k[V]^G \text{ of degree } \leq C \text{ such that } f_v(v) \neq 0.
\]
Let $A$ be the $k$-subalgebra of $k[V]^G$ generated by the subspace
$C \oplus k[V]^G_d$. The variety of zeros in $V$ of the homogeneous elements
of $A$ of strictly positive degree is exactly $N$. Let $h_1, \ldots, h_q$
be a minimal homogeneous system of generators of $A$. We can in
principle effectively find such a system by means of the procedure
described in n.1. Clearly, $\deg h_i \leq C, 1 \leq i \leq q$. Let $\tilde{C}$ be the
minimal positive integer divisible by each $\deg h_i, 1 \leq i \leq q$.
We have
\begin{equation}
\tilde{C} \leq \begin{pmatrix} \text{minimal positive integer} \\
\text{divisible by each } a \in \mathbb{Z}, \end{pmatrix}.
\end{equation}
We have also
$N = \{v \in V | h_i(v) = 0, 1 \leq i \leq q\} =
\{v \in V | h_i^{\tilde{C}/\deg h_i}(v) = 0, 1 \leq i \leq q\}$. Hence $k[V]^G$ is integral
over $B = k[h_i^{\tilde{C}/\deg h_i}, \ldots, h_q^{\tilde{C}/\deg h_q}]$. It follows from the equality
$\deg h_i^{\tilde{C}/\deg h_i} = \tilde{C}, 1 \leq i \leq q$, and from the homogeneous variant
of E. Noether's normalization lemma, [19], that there exists a
homogeneous system of parameters of $B$ which are $k$-linear
combinations of $h_i^{\tilde{C}/\deg h_i}, 1 \leq i \leq q$. Clearly this will
automatically be a homogeneous system of parameters of $k[V]^G$.
This proves that one can take $D$ in (15) to be equal to $\tilde{C}$ or
(more roughly but without finding of $h_i, 1 \leq i \leq q$) to the right
side of (19).

Therefore we now have the problem of finding $C$ with the
property (18).

4. We proceed to the solution of this problem.
Further we shall identify $k^*$ with the subgroup of the scalar
matrices in $GL_n$. Let us consider the subgroup $H = k^*G$. This is an
(s+1)-dimensional connected reductive group with a onedimensional center. Let us consider also its closure \( \overline{H} \) in \( \text{Mat}_n \). The group \( H \) acts on \( \text{Mat}_n \) by means of left multiplication and \( H \) and \( \overline{H} \) are invariant under this action. Specifically, \( H \) and \( \overline{H} \) are invariant under \( k^* \) and hence are cones. \( H \) acts also on \( V \) being a subgroup of \( \text{GL}_n \).

Let \( \overline{x}_{ij} \) be the restriction of \( x_{ij} \) to \( \overline{H} \). The algebra \( k[\overline{H}] \) is generated by \( \overline{x}_{ij}, 1 \leq i,j \leq n \),

\[
(20) \quad k[\overline{H}] = k[... \overline{x}_{ij} ...].
\]

and is \( \mathbb{N} \)-graded (deg \( \overline{x}_{ij} = 1, 1 \leq i,j \leq n \)).

For a point \( v \in V \) we shall consider its orbit \( Hv \) and the closure \( \overline{Hv} \) of this orbit in \( V \). Both \( Hv \) and \( \overline{Hv} \) are cones, i.e. invariant under \( k^* \). Let \( \overline{x}_i, 1 \leq i \leq n \), be the restriction of \( x_i \) on \( \overline{Hv} \). The algebra \( k[\overline{Hv}] \) is generated by \( \overline{x}_i, 1 \leq i \leq n \),

\[
(21) \quad k[\overline{Hv}] = k[\overline{x}_1, ... \overline{x}_n].
\]

and is \( \mathbb{N} \)-graded (deg \( \overline{x}_i = 1, 1 \leq i \leq n \)). It should be noted here that the structure of \( \mathbb{N} \)-graded algebras in these cases is defined by weight decompositions of the underlying algebras with respect to the action of torus \( k^* \), i.e. a function \( f \) is homogeneous of the weight \( d \in \mathbb{N} \) iff \( f(tx) = t^d f(x) \) for each \( t \in k^* \) and \( x \).

**Proposition 1.** A point \( v \in V \) is semi-stable if and only if \( k[\overline{Hv}]^G \neq k \).

**Proof.** Let \( v \) be a semi-stable point. Then \( 0 \notin \overline{Gv} \), see (17). Hence, \( 0 \) and \( \overline{Gv} \) are disjointed closed \( G \)-invariant sets in \( \overline{Hv} \). But such sets are separated by \( G \)-invariants, [9], and therefore \( k[\overline{Hv}]^G \neq k \).
On the contrary, let $k[H_v]^G = k$. Clearly $k[H_v]^G$ is a graded subalgebra of $k[H_v]$. Let $f \in k[H_v]^G$ be an element of strictly positive degree. Being homogeneous $f$ has the properties $f(0) = 0$ and $f(tg v) = t^{\deg f(g v)} = t^{\deg f(v)}$. Therefore, $f(v) \neq 0$ because $H_v$ is dense in $H_v$. We see now that $G_v$ lies in the closed set $\{ u \in H_v | f(u) = f(v) \} \neq 0$. The proposition is proved.

Let us consider the morphism

\begin{equation}
(22) \quad \alpha : H \rightarrow H_v
\end{equation}

defined by formula

\[ \alpha(h) = hv \] (multiplication of a matrix by a column)

This morphism commutes with the action of $H$. Clearly the corresponding comorphism of the $\mathbb{N}$-graded algebras

\[ \alpha^* : k[H_v] \rightarrow k[H] \]

is a degree-preserving monomorphism. If $x_i(v) = a_i, 1 \leq i \leq n$, then

\[ \alpha^*(x_i) = a_i x_{i1} + \ldots + a_n x_{in} \]

It follows now from (21) that

\begin{equation}
(23) \quad \alpha^*(k[H_v]) \text{ is an } H\text{-invariant graded subalgebra of } k[H] \text{ generated by } n \text{ homogeneous elements } a_1 x_{i1} + \ldots + a_n x_{in}, 1 \leq i \leq n, \text{ of degree } 1
\end{equation}

We derive from Proposition 1 the following

Proposition 2. A point $v \in V$ is semi-stable if and only if

\begin{equation}
(24) \quad \alpha^*(k[H_v]) \cap k[H]^G \neq k.
\end{equation}
The advantage of this formulation is that one can say a lot about the structure and properties of $k[\bar{H}]^G$.

More precisely, let $f$ be a rational character of $H$, i.e. a homomorphism $H \to k^*$. We consider $f$ as a regular function on $H$ and a rational function on $\bar{H}$. This function is $G$-invariant because $G$ is semisimple. The set of all such characters of $H$ that are regular on $\bar{H}$ is a semigroup $S$ (with an unity) in the (multiplicative) character group of $H$. Its elements are homogeneous elements of $k[\bar{H}]^G$.

**Proposition 3.** One has:

1. $k[\bar{H}]^G$ is the vector space spanned by $S$ over $k$,
2. $\dim k[\bar{H}]_d^G \leq 1$ for each $d \in \mathbb{N}$,
3. $k[\bar{H}]^G \neq k$,
4. $S$ is a finitely generated semigroup and $f \mapsto \deg f$ is an isomorphism of $S$ with a certain subsemigroup of $\mathbb{N}$.

**Proof.** 1) Let $f$ be a nonzero homogeneous element of $k[H]^G$, $\deg f = d$. We have $f(tg) = t^d f(g) = t^d f(1_n)$ for every $t \in k^*$, $g \in G$ (here $1_n$ is the unity of the group $G$). Therefore $f(1_n) \neq 0$ because $H = k^*G$ is dense in $\bar{H}$. Multiplying $f$ by a suitable constant we can assume $f(1_n) = 1$. Hence $f(tg) = t^d$, i.e. $f \in S$.

2) Let $f$ and $h$ be nonzero homogeneous elements of $k[\bar{H}]^G$ and $\deg f = \deg h$. These elements are the semi-invariants of the torus $k^*$ of the same weight. Hence, the rational function $f/h$ is an $H$-invariant. Therefore, $f/h \in S$.

3) Clearly, the function $\det: (a_{ij}) \mapsto \det(a_{ij})$ is a nonconstant homogeneous element of $k[\bar{H}]^G$ of the degree $n$.

4) $k[\bar{H}]^G$ is finitely generated because $G$ is reductive. It follows from 1) and 2) that $S$ is finitely generated.

The algebra $k[H]$ is $\mathbb{N}$-graded and the elements of $S$ are homogeneous.
Hence we have $\deg f \in \mathbb{N}$, $f \in S$, and 4) follows.

The proposition is proved.

It should be noted here that if $H$ is known to be normal, then we can describe semigroup $S$ more precisely.

Proposition 4. If $H$ is normal then $S$ is a semigroup with one generator. This generator in its turn is a generator of the character group of $H$.

Proof. The character group of $H$ is isomorphic to $\mathbb{Z}$ because the center of $H$ is one-dimensional. Let us take one of the (two possible) generators of this group, say $\phi$, that is uniquely defined by the property: $\det = \phi^d$ for a certain $d > 0$. But $\det \in k[H]$ and therefore $\phi$ is integral over $k[H]$. Hence, $\phi \in S$ because of normality. We see now that $\phi^h \in S$, $h = 0, 1, 2, \ldots$.

We have $\phi(0) = 0$ hence $\phi^h \not\in S$ for $h < 0$.

The proposition is proved.

Remark. It is easy to understand that $\phi$ is given by the formula $\phi(tg) = t|k^* \cap G|$, $t \in k^*$, $g \in G$. Therefore $\deg \phi = |k^* \cap G|$.

Specifically, if the centre of $G$ is trivial, then $\phi(tg) = t$.

In general, we know nothing about the normality of $H$.

Therefore, we have to use in our effective constructions only the elements that we definitely know to lie in $S$ and these elements are $\det^d$, $d \in \mathbb{N}$. But they are sufficient for our purposes.

The condition (24) is equivalent to the condition

\begin{equation}
\alpha^*(k[Hv]) \cap S \neq 1.
\end{equation}

How can one know when (25) is fulfilled? The answer is given by

Proposition 5. Let $F$ be a graded $H$-invariant $k$-subalgebra of $k[H]$, $k \subseteq F$. Then the following properties are equivalent:
1) \(F \cap S \neq 1\),
2) there exists \(f \in S, f \neq 1\), that is integral over \(F\),
3) every \(h \in S\) is integral over \(F\),
4) \(k[H]^G\) is integral over \(F\).

**Proof.** 2) \(\Rightarrow\) 3). It follows from 4) of Proposition 3 that \(f^{\deg f} h = h^{\deg f} f\). Function \(f\) being integral over \(F\), hence \(f^{\deg f}\) is also integral over \(F\). Therefore, \(h^{\deg f}\) is integral over \(F\) and it follows from \(\deg f > 0\) that \(h\) itself is also.

3) \(\Leftarrow\) 4) follows from 4) of Proposition 3.

1) \(\Leftarrow\) 2) Let

\[(26) \quad f^d + f^{d-1}b_1 + \ldots + fdb_{d-1} + b_d = 0, \quad b_i \in F, 1 \leq i \leq d,\]

be an equation of integral dependence. We can assume that \(b_i, 1 \leq i \leq n\), are homogeneous because \(f\) is homogeneous.

Now, we apply Reynolds operator \(\mathcal{G}\) of averaging over \(G\) to the both sides of (26), [9]. It follows from the \(G\)-invariant of \(f\) that we shall obtain

\[(27) \quad f^d + f^{d-1}\mathcal{G}b_1 + \ldots + f\mathcal{G}b_{d-1} + \mathcal{G}b_d = 0,\]

where \(\mathcal{G}b_i \in k[H]^G, 1 \leq i \leq d\). Clearly \(F\) is invariant under \(\mathcal{G}\), therefore \(\mathcal{G}b_i \in F \cap k[H]^G, 1 \leq i \leq d\). We have also

\[(28) \quad \deg \mathcal{G}b_i = i \deg f \leq d \deg f, 1 \leq i \leq d.\]

It follows from (27), (28) and from the condition \(f \neq 1\) that there exists at least one \(i\) such that \(\mathcal{G}b_i\) is a nonconstant homogeneous \(G\)-invariant. According to 1) and 2) of Proposition 3 this element multiplied by a suitable constant from \(k\) lies in \(S\). Hence \(F \cap S \neq 1\).

The proposition is proved.
Corollary 1. If $F \cap k[\mathbb{H}]^G \neq k$ if and only if $\det$ is integral over $F$.

From (28) and the proof of Proposition 5 may be drawn the following

Corollary 2. If $f \in \mathcal{S}$, $f \neq 0$, is integral over $F$ then there exists a nonconstant homogeneous $G$-invariant element in $F$ of degree $\leq d \deg f$, where $d$ is the minimal degree of the equations of integral dependence satisfied by $f$ over $F$.

Applying to the case $F = \alpha*(k[\mathbb{H}])$ and using (25), (23) and Proposition 2 we obtain

Proposition 6. A point $v = \left( \begin{array}{c} a_1 \\ \vdots \\ a_n \end{array} \right) \in V$ is semi-stable if and only if the function $\det \in k[\mathbb{H}]$ is integral over the graded subalgebra $A_v$ of $k[\mathbb{H}]$ that is generated by the elements $a_1 x_{i1} + \ldots + a_n x_{in}$, $1 \leq i \leq n$, of degree 1. If $d_0$ is the minimal degree of the equations of integral dependence satisfied by $\det$ over $A_v$, then there exists a nonconstant homogeneous polynomial of degree $\leq d_0n$ in $k[V]^G$ which do not vanish at $v$.

Therefore we shall be able to find $C$ satisfying (18) if a number will be explicitly known that is not less than the minimal degree of the equations of integral dependence satisfied by $\det$ over $A_v$ for every semi-stable point $v$. We shall now show how to find such a number.

5. Let $v \in V$ be a semi-stable point. There exists a homogeneous system of parameters of $A_v$, say $b_1, \ldots, b_h$, such that $\deg b_i = 1$, $1 \leq i \leq h$ (because $A_v$ is generated by a system of homogeneous elements of degree 1). Function $\det$ is integral over $A_v$, hence also over $B_v = k[b_1, \ldots, b_h]$. Therefore the minimal degree of the equations of integral dependence satisfied by $\det$ over $A_v$ is not
greater than the same for $\text{det}$ over $B_v$. But $B_v$ is integrally closed because of the algebraical independence of $b_1, \ldots, b_h$. Therefore, the minimal equation of $\text{det}$ over $k(b_1, \ldots, b_h)$ has its coefficients in $B_v$. Complete the sequence $b_1, \ldots, b_h$ with $s+1-h$ elements $b_{h+1}, \ldots, b_{s+1}$, taken from among the $x_{ij}$, $1 \leq i, j \leq n$ such that $b_1, \ldots, b_{s+1}$ are algebraically independent over $k$ (it is possible because of (20)). It is easy to see that the minimal polynomial of $\text{det}$ over $k(b_1, \ldots, b_{s+1})$ is the same as over $k(b_1, \ldots, b_{s+1})$. Therefore, it will be sufficient for our purposes to find an upper boundary (that does not depend on $v$) of the degree of the minimal polynomial of $\text{det}$ over $k(b_1, \ldots, b_{s+1})$. One can do it as follows.

Let us consider for each $p \in \mathbb{N}$ the set of all monomials in $b_1, \ldots, b_{s+1}$, $\text{det}$ of degree $p$

\begin{equation}
\sum_{i_1, \ldots, i_{s+1} + ni = p} a_{i_1, \ldots, i_{s+1}} i_1^{i_1} \ldots i_{s+1}^{i_{s+1}} \text{det}^{i_{s+1}} = p.
\end{equation}

If it happens that for a certain $p = p_0$ these monomials are linearly dependent over $k$ then one can say that the degree of the minimal polynomial of $\text{det}$ over $k(b_1, \ldots, b_{s+1})$ is not greater than $p_0/n$. Indeed, if for $p = p_0$ a nontrivial linear combination

\begin{equation}
\sum_{i_1, \ldots, i_{s+1} + ni = p} a_{i_1, \ldots, i_{s+1}} i_1^{i_1} \ldots i_{s+1}^{i_{s+1}} \text{det}^{i_{s+1}} = 0,
\end{equation}

where $a_{i_1, \ldots, i_{s+1}} \in k$, is equal to zero, then there exists at least one nonzero $a_{i_1, \ldots, i_{s+1}}$ with $i \neq 0$ (because $b_1, \ldots, b_{s+1}$ are algebraically independent). It follows from (29) that $i \leq p_0/n$ for every $a_{i_1, \ldots, i_{s+1}}$. Therefore it follows from (30) that $\text{det}$ is a root of an equation of degree $\leq p_0/n$ with its coefficients in $k(b_1, \ldots, b_{s+1})$.

So we now have the problem of finding $p_0$. Technically it will be more convenient for us to consider only those of (29) for which
CONSTRUCTIVE INVARIANT THEORY

(31) \( p = nc \) and \( i_1 = nj_1, \ldots, i_{s+1} = nj_{s+1} \)

where \( c, j_1, \ldots, j_{s+1} \) are integers. We shall find such \( c = c_0 \) that the monomials (29) with property (31) are linearly dependent over \( k \). Hence the degree of the minimal polynomial of \( \det \) over \( k(b_1, \ldots, b_{s+1}) \) will not be greater than \( c_0 \).

6. Let \( N^+ \) and \( N^- \) be the pair of "opposite" maximal nilpotent subalgebras of \( \text{Lie G} \) that correspond to a choice of positive and negative roots with respect to \( T \). Let \( Y_1, \ldots, Y_d \) and \( Z_1, \ldots, Z_d \) be the bases of the linear spaces \( N^+ \) and \( N^- \), \( d = (s-r)/2 \), and \( y_1, \ldots, y_d \) and \( z_1, \ldots, z_d \) the coordinate functions on these spaces with respect to these bases.

Let us consider the variety \( N^+ \times k^N \times N^- \). One can identify in a natural way the functions \( y_1, \ldots, y_d, z_1, \ldots, z_d, t_1, t_1^{-1}, \ldots, t_r, t_r^{-1} \) with the regular functions on this variety. Clearly \( k[N^+ \times k^N \times N^-] \) is generated by these functions.

For an arbitrary nilpotent matrix \( X \in \text{Mat}_n \) its exponential \( \exp X \) is the matrix

(32) \[ 1_n + \frac{1}{1!} X + \frac{1}{2!} X^2 + \ldots + \frac{1}{(n-1)!} X^{n-1}, \]

because \( X^p = 0 \) when \( p \gg n \).

It is well known, [7], that the morphism

\[ \beta: N^+ \times k^N \times N^- \rightarrow \overline{H} \]

given by the formula (cf. (1))

\[ \beta(X^+, (a_1, \ldots, a_r), X^-) = \exp X^+ (f_{ij}(a_1, \ldots, a_r)) \exp X^- \]

is an isomorphism of \( N^+ \times k^N \times N^- \) with an open set of \( G \) ("big cell").
Consider now the following matrices (with its coefficients in $k[N^+ \times k^r \times N^-]$)

\[(33)\quad Y = \sum_{i=1}^{d} y_i y_i \quad \text{and} \quad Z = \sum_{i=1}^{d} z_i z_i\]

Let $\exp Y$ and $\exp Z$ be the results of the substitution of $Y$ and resp. $Z$ instead of $X$ in (32). Then

$$\beta^*(\overline{x}_{ij}) \text{ is the coefficient of the matrix } \exp Y (f_{pq}(t_1, \ldots, t_r)) \exp Z$$

$$\text{situated in its } i\text{-th row and } j\text{-th column}$$

It follows now from (34), (33), (32) and the definition of the number $t$ (cf. (1) and (3)) that

$$\beta^*(\overline{x}_{ij}) \text{ is a } k\text{-linear combination of the monomials}$$

$$y_1^{r_1} \ldots y_d^{r_d} z_1^{q_1} \ldots z_d^{q_d} t_1^{m_1} \ldots t_r^{m_r}$$

where $r_i, q_i \in \mathbb{N}, 1 \leq i \leq d, m_j \in \mathbb{Z}, 1 \leq j \leq r$, and

$$0 \leq r_1 + \ldots + r_d \leq n-1,$$

$$0 \leq q_1 + \ldots + q_d \leq n-1,$$

$$\max_{1 \leq i \leq r} |m_i| \leq t.$$\[(35)\]

Now we note that the function (30) is homogeneous and hence is equal to zero if and only if its restriction to $G$ vanishes. In its turn it happens if and only if the image of this restriction under the comorphism $\beta^*$, i.e. the function

$$\beta^*(b_1^{i_1} \ldots b_s^{i_s+1} \det^i),$$

vanishes.

The function $b_1^{i_1} \ldots b_s^{i_s+1} \det^i, i_1 + \ldots + i_s + 1 + ni = p$, is homogeneous of degree $p$ , therefore it follows form (35) that
the function (36) is a linear combination of the monomials

\[
\frac{r_1}{y_1} \cdots \frac{r_d}{y_d} \frac{q_1}{z_1} \cdots \frac{q_d}{z_d} \frac{m_1}{t_1} \cdots \frac{m_r}{t_r}
\]

(37)

where \( r_i, q_i \in \mathbb{N} \), \( 1 \leq i \leq d \), \( m_j \in \mathbb{Z} \), \( 1 \leq j \leq r \), and

\[
0 \leq r_1 + \ldots + r_d \leq p(n-1),
\]

\[
0 \leq q_1 + \ldots + q_d \leq p(n-1),
\]

\[
\max_{1 \leq i \leq r} |m_i| \leq pt
\]

and the coefficients of this linear combination are the \( k \)-linear combinations of the element \( a_{i_1} \ldots i_{s+1} \),

\[
i_1 + \ldots + i_{s+1} \equiv p.
\]

We need to remember here that if \( \delta_1, \ldots, \delta_h \) are the variables then

the total number of the monomials \( \delta_1^{s_1} \cdots \delta_h^{s_h} \), \( s_i \in \mathbb{N} \),

(38)

\[1 \leq i \leq h, \text{ is equal to } \binom{k+h-1}{k} \text{ if } s_1 + \ldots + s_h = k \text{ and}
\]

\[\text{equal to } \binom{k+h}{k} \text{ if } s_1 + \ldots + s_h < k.\]

It easily follows from (38) that the total number of the monomials in \( y_1, \ldots, y_d, z_1, \ldots, z_d, t_1, \ldots, t_r \) that are described in (37) is not greater than

\[
\left( \frac{d+p(n-1)}{d} \right)^2 (2pt+1)^r.
\]

On the other hand assume now that the conditions (31) are fulfilled. It follows then from (38) that for a given \( c \) the total number of the coefficients \( a_{i_1} \ldots i_{s+1} \) in (30) is equal to

\[
\binom{s+c+1}{c}.
\]
In view of (37) we see that if for a certain c one has an inequality

\[
\left( \frac{d+cn(n-1)}{d} \right)^2 (2cnt+1)^r < \binom{s+c+1}{c}
\]

then the monomials (29) (with the conditions (31) to be fulfilled) are linearly dependent over k. Let us show that (39) is fulfilled for

\[
c = \frac{\frac{2}{3}s^+n^s(n-1)^{s-r}r^{(s+1)!}}{3^s(\frac{s-r}{2})!}
\]

Indeed, we have \( d = \frac{s-r}{2} \leq n(n-1)/2 \) and

\[
\left( \frac{d+cn(n-1)}{d} \right)^2 (2cnt+1)^r \leq \frac{(cn(n-1)+d)^2}{(d!)^2} (2cnt+1)^r = \frac{(c + \frac{1}{n})^r(2nt)^r}{(\frac{s-r}{2})^2} \leq (c + \frac{1}{n})^r \leq \frac{n^s(n-1)^{s-r}r^{(s+1)!}}{3^s(\frac{s-r}{2})!}.
\]

Also \( \frac{(s+c+1)}{c} > \frac{c^{s+1}}{(s+1)!} \). Hence (39) is definitely fulfilled if

\[
(c+\frac{1}{n})^s \frac{n^s(n-1)^{s-r}r^r}{\left(\frac{s-r}{2}\right)!} \leq \frac{c^{s+1}}{(s+1)!}
\]

or equivalently if

\[
\frac{n^s(n-1)^{s-r}r^r(s+1)!}{\left(\frac{s-r}{2}\right)!} \leq c\left(1 + \frac{1}{2c}\right)^s.
\]

This inequality in its turn is fulfilled if c is given by the formula (40) because \( (1 + \frac{1}{2c}) > \frac{3}{7} \).
CONSTRUCTIVE INVARIANT THEORY

Summing up all the results of nn. 1-6 we obtain the following

Theorem. Let $G \subset GL_n(V)$ be a connected semisimple algebraic group, $s = \dim G$, $r = \text{rk } G$. Let $m$ be the transcendence degree of $k[V]^G$ over $k$ and $t$ be a constant defined in (3). Then the degrees of the elements of a minimal homogeneous system of generators of the algebra $k[V]^G$ are not greater than the number

$$0 < a \leq \frac{2^{r+s}n^{s+1}(n-1)^{s-r}t^{r(s+1)!}}{3^s(s-r)!^2}$$

minimal positive integer divisible by each $a \in \mathbb{Z}$.

7. This section contains several remarks about the number $q$ in (9).

We know that $F(k[V]^G, x)$ has a pole of order $m$ at $x = 1$. Therefore the Laurent expansion about $x = 1$ begins

$$F(k[V]^G, x) = \frac{\gamma}{(1-x)^m} + \frac{\tau}{(1-x)^{m-1}} + \ldots .$$

It follows from (7) and (41) that

$$\gamma = \lim_{x \to 1} (1-x)^m \left( \sum_{i=1}^{\ell} x^i \right) \left( \prod_{j=1}^{m} d_j \right) = \frac{\ell}{m} \frac{\prod_{j=1}^{d_j}}{\prod_{j=1}^{d_j}} .$$
\[
\tau = - \lim_{x \to 1} \frac{\sum_{i=1}^{k} e_i}{x} = \lim_{x \to 1} \frac{\sum_{i=1}^{k} e_i}{x} = - \sum_{j=1}^{m} \frac{d}{dx} \left(1-x^m\right)
\]

\[
\tau = - \lim_{x \to 1} \frac{\sum_{i=1}^{k} e_i}{x} = \lim_{x \to 1} \frac{\sum_{i=1}^{k} e_i}{x} = - \sum_{j=1}^{m} \frac{d}{dx} \left(1-x^m\right)
\]

\[
\tau = - \lim_{x \to 1} \frac{\sum_{i=1}^{k} e_i}{x} = \lim_{x \to 1} \frac{\sum_{i=1}^{k} e_i}{x} = - \sum_{j=1}^{m} \frac{d}{dx} \left(1-x^m\right)
\]

\[
\tau = - \lim_{x \to 1} \frac{\sum_{i=1}^{k} e_i}{x} = \lim_{x \to 1} \frac{\sum_{i=1}^{k} e_i}{x} = - \sum_{j=1}^{m} \frac{d}{dx} \left(1-x^m\right)
\]

Therefore

\[
\frac{2\tau}{Y} = \sum_{j=1}^{m} (d_j - 1) - \frac{2}{k} \sum_{i=1}^{k} e_i.
\]

Adding up the equalities (11) over all \(i=1, \ldots, k\) we shall obtain

\[
\frac{m}{\sum_{j=1}^{m} d_j} - q = \frac{2}{k} \sum_{i=1}^{k} e_i.
\]

Now it follows from (45) and (44) that

\[
\frac{2\tau}{Y} = q - m
\]

or in another form

\[
q = \frac{2\tau}{Y} + \dim V - (\dim G_v, v \in V \text{ is a point in general position}).
\]

So we have

1) \(\frac{2\tau}{Y}\) is always an integer,

2) \(q = \dim V - \frac{2\tau}{Y}\) (\(\dim G_v, v \in V \text{ is a point in general position}\)).
As a matter of fact to derive the conclusions we used only that $k[V]^G$ is Gorenstein (but not that $G$ is a connected semisimple group). Specifically, these conclusions are also valid for those finite $G$ with a property that $k[V]^G$ is Gorenstein (e.g. if $G \subseteq \text{SL}_n$, cf. [13]). It is remarkable that one can describe $\gamma$ and $\tau$ for an arbitrary finite group $G$ completely in terms of the internal properties of $G$ itself, [13]:

$$
\gamma = \frac{1}{|G|},
$$

$$
\tau = \frac{\text{the number of pseudo-reflections in } G}{2|G|}.
$$

Therefore in this case

$$
\frac{2\tau}{\gamma} = \text{the number of pseudo-reflections in } G.
$$

If $G$ is finite and $k[V]^G$ is Gorenstein then it follows from (46) that

$$
q = \dim V + (\text{the number of pseudo-reflections in } G).
$$

If for instance $G \subseteq \text{SL}_n$ then $q = \dim V$ (it should be noted also conversely that if $k[V]^G$ is Gorenstein and $q = \dim V$ then $G \subseteq \text{SL}_n$, cf. [13]).

It seems to me to be very interesting to establish whether there exists an interpretation of the numbers $\gamma, \tau$ and $\frac{2\tau}{\gamma}$ completely in terms of the internal properties of $G$ itself, that is analogous to (47), (48), when $G$ is a connected semisimple group.

It is proved in [14] that if $G$ is a connected semisimple and the trivial character of $T$ is "critical" then

$$
q = \dim V, \text{ hence } \frac{2\tau}{\gamma} = (\dim Gv, v \in V \text{ is a point in general position}).
$$
If for instance $G$ is an image of $\text{SL}_2$ under its natural representation in the space of binary forms of degree $n-1$, then the trivial character is critical and (47) is fulfilled when $n \geq 4$, [14] (and (47) is not fulfilled when $n = 2, 3$).

8. We shall discuss in this last section an approach to the solution of the problem of constructive invariant theory suggested in [2].

The general strategy in [2] is the same as in n.3 - it provides an effective way to calculate the constant $C$ satisfying the property (18). (It should be incidentally noted that the reasoning on page 67 in [2] is not correct. That is to say, the ring $B'$ depends on the point $x_0$, therefore the minimal equations of $\det(Y_{ij})$ over the fields of fractions of the rings $B'$ constructed for the rings $B'$ constructed for $x_0$ and $s.x_0$ are a priori different. Hence, the equality $Q_k((Y_{ij}).(s.x_0)) = Q_k((Y_{ij}).x_0)$ remains unsubstantiated. As a matter of fact, the assertion itself is correct but one has to change the proof using Reynolds operator $\Psi$ as it was done above, n.4, formula (27)).

After finding the constant $C$, the authors consider an ideal $J$ in $k[V]$ generated by all polynomials $f_v$, $v \in V-N$, see (18), and then notice: "the Nullstellensatz shows that some power of every invariant is in $J$. As we may (at least theoretically) pick a finite system of generators of $J$ of degree $\leq M'$ ($= C$) we are then reduced to forming a system of generators of the "root" of $J$; Hilbert's own proof of his Nullstellensatz shows how this (again theoretically) may be done explicitly". But in reality this assertion leads to the solution only if $\forall J$ coincides with the ideal $I$ in $k[V]$ generated by all $G$-invariant polynomials of strictly positive degree (it is easy to understand that a set of invariants,
that is a homogeneous system of generators of \( I \), is also a system of generators of \( k[V]^G \). However, in general we have only the equality
\[
\sqrt{J} = \sqrt{I}.
\]
Therefore \( \sqrt{J} = I \) if and only if \( I \) is the radical ideal, i.e. \( \sqrt{I} = I \). There seems to be an impression that in [2] the equality \( \sqrt{I} = I \) is considered to be self-evident. However, in general this equality does not take place. Examples are given below, but here we say only that when \( \sqrt{I} \neq I \) we can say nothing in general about the basis of \( I \), knowing the basis of \( \sqrt{I} \) (hence the approach suggested in [2] does not lead to the solution).

Now, for the examples. Firstly, it is evident that if \( G \) is finite then \( \sqrt{I} \) always coincides with the ideal in \( k[x_1, \ldots, x_n] \) generated by \( x_1, \ldots, x_n \). Hence \( \sqrt{I} \neq I \) if \( G \) is not trivial. It is more interesting (and more difficult) to construct such an example when \( G \) is a connected semisimple group. One can find in [3], pp. 159-160, an example when \( G \) is isomorphic to \( SO(2k+1) \). But it is only the classical case of homogeneous polynomial representations of \( SL_d \) under consideration in [2]. Therefore it will be more instructive to have an example valid for this case. We shall show now that if \( G \) is an image of \( SL_2 \) under its natural representation in the space of binary forms of degree 6, then \( \sqrt{I} \neq I \).

Denote by \( R_d \) the unique (up to isomorphism) irreducible \( SL_2 \)-module of degree \( d+1 \). It is known that the multiplicity \( c(d,e) \) of \( R_d \) in \( k[V]^e \) is equal to the dimension of the space of covariants of binary form of degree \( e \) that are homogeneous of degree 6 in the coefficients and order \( d \) in the variables (i.e. \( c(d,e) = m(e, 6,d) \) in the notations of [11]). Calculating these
numbers by means of one known method or another (I used Sylvester's tables of Poincaré series for the covariants, [16]) one obtains the following table

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>8</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>c(d,e)</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
</tbody>
</table>

It is known that $k[V]^G$ has a minimal homogeneous system of generators $f_2, f_4, f_6, f_{10}, f_{15}$, $\deg f_i = i$, with $f_2, f_4, f_6, f_{10}$ algebraically independent and $f_{15}^2 \in k[f_2, f_4, f_6, f_{10}]$, see [11].

Clearly $I_5 = k[V]_3f_2 \oplus k[V]_1f_4$. It follows from the table above that the multiplicity of $R_2$ in $I_5$ is equal to 1. We can conclude now from $c(2,5) = 2$ that there exists a submodule $R_2$ in $k[V]_5$ that does not lie in $I_5$. We also have

$I_{10} = k[V]_8f_2 + k[V]_6f_4 + k[V]_4f_6 + k[V]_0f_{10}$. The polynomials $f_2, f_4, f_6$ clearly are irreducible, hence

$k[V]_8f_2 \cap k[V]_6f_4 \cap k[V]_4f_6 = 0$.

But $k[V]_8f_2 + k[V]_6f_4 \cong (k[V]_8f_2 \oplus k[V]_6f_4)/(k[V]_8f_2 \cap k[V]_6f_4)$ and it is easy to understand that $k[V]_8f_2 \cap k[V]_6f_4 = k[V]_4f_2f_4$.

It follows from here and from the table above that the multiplicity of $R_4$ in $I_{10}$ is equal to $c(4,8) + c(4,6) - c(4,4) + c(4,4) = 7 + 4 = 11 = c(4,10)$. Therefore, every irreducible submodule $R_4$ in $k[V]_{10}$ lies in fact in $I_{10}$. Let us now take a submodule $R_2$ in $k[V]_5$ that does not lie in $I_5$ and let $f$ be an element of this submodule that is a highest vector (with respect to some fixed maximal torus and Borel subgroup $B$ of $SL_2$). So $f$ is a $B$-semi-invariant of the weight 2. But $f^2 \in k[V]_{10}$ is evidently a $B$-semi-invariant of the weight 4. Therefore $f^2$ is a highest vector of a module $R_4 \subset k[V]_{10}$. It follows from the above that $f^2 \in I_{10}$.

We now see that $f \in k[V], f \notin I$, but $f^2 \in I$, i.e. $\sqrt{I} \neq I$. 330
It will be interesting to clarify whether or not $I$ is radical for the other irreducible representations of $SL_2$ (it is easy to see that $I$ is radical for the representations of dimensions $2, 3, 4, 5$; apparently it is not the case for the dimensions $\geq 8$). The property for $I$ to be radical seems to be very ingenious and to reflect important properties of $G$-module $k[V]$ (for example one can prove that if $\sqrt{I} = I$ and there exists a dense orbit in $N$, then $k[V]$ is a free $k[V]^G$-module). It would also be interesting to classify the connected semisimple groups for those $\sqrt{I} = I$.

The fact that $\sqrt{I} \neq I$ leads in general to a number of questions about the structure of $I$ itself. There is as yet little known in this direction. We want to conclude by formulation a conjecture about the structure of the reduced primary decomposition of $I$.

Let $X(T)$ be the character group of $T$ (written additively). We consider $X(T)$ as a lattice in $X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$. Let $\Delta$ be the set of the weights of $T$ in $V$. Denote by $V_\lambda$ the weight space in $V$ of the weight $\lambda \in \Delta$. Consider all the maximal subsets $\Delta(\mu)$ of $\Delta$ that lie in an open halfspace of $X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$ (depending on $\Delta(\mu)$) and for each $\Delta(\mu)$ consider the following subspace in $V$

$$N_T(\mu) = \bigoplus_{\lambda \in \Delta(\mu)} V_\lambda.$$ 

Let $k[V]^T$ be the subalgebra of $T$-invariants in $k[V]$, $I_T$ the ideal in $k[V]$ generated by all homogeneous elements of $k[V]^T$ of strictly positive degree and $N_T$ the variety of zeros of $I_T$ in $V$. It follows from the Hilbert-Mumford theorem, [9], that

$$N_T = \bigcup_{\mu} N_T(\mu),$$

$$N = GN_T = \bigcup_{\mu} GN_T(\mu).$$
It may happen in general that $\text{GN}_T^{(\mu)} \subset \text{GN}_T^{(\nu)}$.

Conjectures (Vinberg).

1). There is no imbedded primes belonging to a reduced primary decomposition of $I_T$,

2). The varieties defined by imbedded primes belonging to a reduced primary decomposition of $I$ are exactly those $\text{GN}_T^{(\mu)}$ for which there exists such $\nu$ that $\text{GN}_T^{(\mu)} \subset \text{GN}_T^{(\nu)}$. 
REFERENCES


V.L. Popov
ul. Musy Džalilja, d. 17, k. 2, kv. 246
Moscow M-580
115580 USSR