CONSTRUCTIVE INVARIANT THEORY

HARM DERKSEN*

Contents

In these lecture notes, we will discuss the constructive aspects of modern invariant theory. A detailed discussion on the computational aspect of invariant theory can be found in the books [38, 9]. The invariant theory of the nineteenth century was very constructive in nature. Many invariant rings for classical groups (and SL_2 in particular) were explicitly computed. However, we will not discuss this classical approach here, but we will refer to [32, 25] instead. Our starting point will be a general theory of invariant rings. The foundations of this theory were built by Hilbert. For more on invariant theory, see for example [23, 35, 24].

1. Hilbert's first approach

Among the most important papers in invariant theory are Hilbert's papers of **1890** and **1893** (see [15, 16]). Both papers had an enormous influence, not only on invariant theory but also on commutative algebra and algebraic geometry. Much of the lectures

*The author was partially supported by NSF, grant DMS 0102193.

will be centered around these two papers, and their place within modern invariant theory.

1.1. **Hilbert's Basissatz.**

Theorem 1.1 (cf. [15]). *If K is a field, then the polynomial ring $K[x_1, x_2, \dots, x_n]$ is Noetherian, i.e., every ideal of $K[x_1, \dots, x_n]$ is finitely generated.*

The statement in this theorem is not constructive, because it does not tell us how to find the generators of an ideal. Today exploiting new and important methods using Gröbner Bases we see that many problems concerning ideals have constructive solutions. There are many books on Gröbner bases methods (for example [1, 3, 6, 27, 39]), so we will keep the discussion here to a minimum.

Definition 1.2. An *admissible monomial ordering* is an ordering "$<$" on the monomials with the properties:

(1) $<$ is a total ordering.
(2) $1 < m$ for every monomial m not equal to 1,
(3) If $m_1 < m_2$ then $mm_1 < mm_2$ for all monomials m_1, m_2, m.

Proposition 1.3. *If "$<$" is an admissible ordering, then it is a well-ordering: Every nonempty set of monomials has a smallest element.*

Exercise 1.4. *Use Hilbert Basissatz (Theorem 1.1) to prove Proposition 1.3.*

An important ordering is the *lexicographic ordering* defined by:

$$x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} < x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n} \Leftrightarrow \text{there is a } k \text{ such that } a_i = b_i \text{ for } i < k \text{ and } a_k = b_k.$$

Other monomial orderings such as the reverse lexicographic total degree ordering may be more efficient in practice, but we will not discuss them here.

Fix an admissible ordering $<$. If f is a polynomial in $K[x_1, \dots, x_n]$, then the *leading monomial* $\mathrm{lm}(f)$ is the largest monomial appearing in f. If c is the coefficient of $\mathrm{lm}(f)$ in f, then $\mathrm{lc}(f) := c$ is called the *leading coefficient* and $\mathrm{lt}(f) := c\,\mathrm{lm}(f)$ is called the *leading term* of f. If I is an ideal, then let $\mathrm{lm}(I)$ be the (monomial) ideal generated by all $\mathrm{lm}(f)$, $f \in I$.

Definition 1.5. A subset $\mathcal{G} = \{f_1, f_2, \dots, f_r\}$ of I is called a Gröbner basis (with respect to the ordering $<$) if $\mathrm{lm}(I)$ is generated by $\{\mathrm{lm}(f_1), \dots, \mathrm{lm}(f_r)\}$.

It is clear that every ideal has a finite Gröbner basis, since $\mathrm{lm}(I)$ is a finitely generated ideal by Theorem 1.1.

Proposition 1.6. *If $\mathcal{G}$ is a Gröbner basis of I, then $\mathcal{G}$ generates I as an ideal.*

Proof. Supppose that $h \in I$ is nonzero. Since $\mathrm{lm}(h) \in I$ and $\mathcal{G}$ is a Gröbner basis, we get that $\mathrm{lm}(h)$ is divisible by $\mathrm{lm}(f_{i_0})$ for some i_0. Define

$$h_1 = h - a_0 f_{i_0}$$

where $a_0 = \operatorname{lt}(h_0)/\operatorname{lt}(f_{i_0})$. Note that $\operatorname{lm}(h_1) < \operatorname{lm}(h)$. By repeating this process we have

$$h_{j+1} = h_j - a_i f_{i_j}$$

with $\operatorname{lm}(h_{j+1}) < \operatorname{lm}(h_j)$ for all j. We must have $h_k = 0$ for some k. Otherwise

$$\{\operatorname{lm}(h_0), \operatorname{lm}(h_1), \dots\}$$

is strictly decreasing and this set would not have a smallest element, contradicting Proposition 1.3. From this it follows that $h \in (f_1, f_2, \dots, f_r)$. The proof gives an algorithm for writing h as a combination of $f_1, \dots, f_r$. □

If an ideal is given by a finite set of generators, then the so-called *Buchberger algorithm* can find a Gröbner basis for it. Although the general complexity of the Buchberger algorithm is very bad, one is still able to compute a Gröbner basis in many interesting examples.

The following Exercise shows that the lexicographic ordering is useful for the *elimination of variables* $x_1, \dots, x_k$ in an ideal I of $K[x_1, \dots, x_n]$.

Exercise 1.7. *If $\mathcal{G}$ is a Gröbner basis with respect to the lexicographic ordering, then $\mathcal{G} \cap K[x_{k+1}, x_{k+2}, \dots, x_n]$ is a Gröbner basis of $I \cap K[x_{k+1}, x_{k+2}, \dots, x_n]$.*

1.2. **Algebraic groups.** For convenience, we will work over an algebraically closed field. Radical ideals of the polynomial ring correspond to Zariski closed subsets of the affine space. Note that such a correspondance is based on Hilbert's Nullstellensatz which was proven in the **1893** paper (see [16]).

Definition 1.8. A linear algebraic group is an affine variety G with a fixed element $e \in G$, and morphisms $m : G \times G \to G$ (multiplication) and $i : G \to G$ (inverse) such that G satisfies the usual group axioms.

A homomorphism of algebraic groups $\phi : H \to G$ is a morphism of affine algebraic varieties which is also a homomorphism of groups. Such a homomorphism is called an isomorphism if ϕ is an isomorphism of affine algebraic varieties.

Often a linear algebraic group is defined as a Zariski closed subgroup of GL_n for some n. One can show that our definition is equivalent to this. Exercise 1.9 below shows that a Zariski closed subgroup of GL_n is a linear algebraic group according to our definition. Remark 1.23 shows that any group that is a linear algebraic group according to our definition is indeed isomorphic to a Zariski closed subgroup of GL_n for some n.

Finite groups, the orthogonal group O_n, the special linear group SL_n are examples of algebraic groups.

Exercise 1.9. *We can identify GL_n with the Zariski closed subset of $\mathrm{M}_n(K) \times K$ defined by*

$$\{(A, b) \mid \det(A)b = 1\}$$

(here $\mathrm{M}_n(K)$ *is the set of* $n \times n$ *matrices with entries in* K*). Using this identification, show that* GL_n *is a linear algebraic group. (What are* e*,* m *and* i*?) Also prove that every Zariski closed subgroup of* GL_n *is a linear algebraic group.*

In particular the multiplicative group $K^\star = \mathrm{GL}_1$ is an algebraic group. The r-dimensional torus is defined as $(K^\star)^r$ and this group is of course an algebraic group as well.

Definition 1.10. A *rational action* of G on an affine variety X is a morphism

$$\mu : G \times X \to X$$

which satisfies the usual axioms of an action of a group on a set. Instead of $\mu(g,x)$ we will write $g \cdot x$. If X is a vector space and G acts by linear transformations, then X is called a *representation space*. An affine variety with a rational action of G is called an *affine* G*-variety*.

If G acts rationally on an affine variety X, then G also acts on the coordinate ring $K[X]$ as follows. If $f \in K[X]$ and $g \in G$, then $g \cdot f$ is defined by

$$(g \cdot f)(x) := f(g^{-1} \cdot x), \quad x \in X.$$

(Note that we have to put in the inverse to make it an action.) Now the *invariant ring* is defined by

$$K[X]^G = \{f \in K[X] \mid g \cdot f = f \text{ for every } g \in G\}.$$

Example 1.11. Suppose that $G = S_n$, the symmetric group, and V is a K-vector space with a basis $v_1, v_2, \ldots, v_n$. We can let G act on V by:

$$\sigma \cdot v_i = v_{\sigma(i)}.$$

Let $x_1, x_2, \ldots, x_n$ be the coordinate functions which are dual to $v_1, \ldots, v_n$. The coordinate ring of V is $K[x_1, x_2, \ldots, x_n]$. It is well-known that the invariant ring is equal to

$$K[V]^G = K[e_1, e_2, \ldots, e_n]$$

where e_k is the *k-th elementary symmetric function* defined by

$$e_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Example 1.12. Let us assume that $\operatorname{char} K = 0$. Suppose $G = \mathrm{SL}_2$. Define V_d, the *binary forms of degree* d by

$$V_d = \{a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d \mid a_0, a_1, \ldots, a_d \in K\}$$

Now V_d is a representation of SL_2 where SL_2 acts by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(X,Y) = f(aX + cY, bX + dY).$$

Let t_i be the linear function on V_d that maps a polynomial $a_0X^d+a_1X^{d-1}Y+\cdots+a_dY^d$ to the coefficient a_i. We can identify $K[V_d]$ with $K[t_0,t_1,\dots,t_d]$. Gordan proved (before Hilbert's general Finiteness Theorem) that $K[V_d]^{\mathrm{SL}_2}$ is always finitely generated (see [14]). For $d=2$ we have

$$K[V_2]^{\mathrm{SL}_2}=K[t_1^2-4t_0t_2].$$

The term $t_1^2-4t_0t_2$ may be recognized as the discriminant of a quadratic equation.

Example 1.13. Let $K^\star$ be the multiplicative group. We let $K^\star$ act on $V=K^3$ by

$$\lambda\cdot(x_1,x_2,x_3)=(\lambda^{-2}x_1,\lambda x_2,\lambda^3x_3)$$

One can check that the invariant ring is equal to

$$K[x_1,x_2,x_3]^{K^\star}=K[x_1x_2^2,x_1^2x_2x_3,x_1^3x_3^2].$$

1.3. **Hilbert's Finiteness Theorem.** Nagata showed in [30] that invariant rings are not always finitely generated (answering Hilbert's fourteenth problem, [17]). Nevertheless, invariant rings are finitely generated for a large class of groups, so-called *linearly reductive groups*.

Besides the notion of linear reductivity, there are also other notions like *group-theoretical reductivity* and *geometric reductivity* (these two notions actually coincide). Many results such as finite generation of invariant rings and geometric properties of invariant rings also hold for these more general notions of reductivity, but usually the proofs are more complicated. In characteristic 0, all notions of reductivity coincide. We will stick to linear reductivity and not further discuss the other notions of reductivity.

Definition 1.14. A Reynolds operator for a linear algebraic group G is a K-linear map $\mathcal{R}:K[G]\to K$ such that $\mathcal{R}(1)=1$ and $\mathcal{R}(g\cdot f)=\mathcal{R}(f)$ for all $g\in G$ and $f\in K[X]$ (G acts on itself rationally by left multiplication, so G also acts on $K[G]$). An algebraic group with a Reynolds operator is called *linearly reductive*.

Often an algebraic group is called linearly reductive if every representation is a direct sum of irreducible representations (i.e., representations without non-trivial proper subspaces which are stable under the action). It can be shown that this definition is equivalent to our definition.

Example 1.15. A finite group G is linearly reductive as long as the characteristic of the base field K does not divide the group order G. Let us define $\mathcal{R}$ as the averaging over the group

$$\mathcal{R}(f)=\frac{1}{|G|}\sum_{g\in G}g\cdot f.$$

It is straightforward to check that $\mathcal{R}$ satisfies the conditions for a Reynolds operator (see Definition 1.14).

Example 1.16. The group $K^\star$ is linearly reductive. Indeed, the coordinate ring of $K^\star$ can be identified with the ring of Laurent polynomials

$$K[x, x^{-1}]$$

For any $f \in K[x, x^{-1}]$, we define $\mathcal{R}(f)$ as the constant coefficient.

Exercise 1.17. *Check that $\mathcal{R}$ in the previous example is indeed a Reynolds operator.*

Example 1.18. For classical groups over $\mathbb{C}$, the Reynolds operator is averaging over a maximal compact subgroup. For example, $\mathrm{GL}_n(\mathbb{C})$ has the subgroup $\mathrm{U}_n(\mathbb{C})$. It is known that the unitary group is Zariski-dense in $\mathrm{GL}_n(\mathbb{C})$. Then we can define

$$\mathcal{R}(f) = \int_{U_n(\mathbb{C})} f \, d\mu$$

where $d\mu$ is a so-called Haar-measure (a measure that is invariant under the group action which we will normalize such that $\int d\mu = 1$). It is clear that $\mathcal{R}(1) = 1$ and that $\mathcal{R}(g \cdot f) = \mathcal{R}(f)$ for $g \in U_n(\mathbb{C})$. Using the fact that $U_n(\mathbb{C})$ lies Zariski dense in $\mathrm{GL}_n(\mathbb{C})$ one gets that $\mathcal{R}(g \cdot f) = \mathcal{R}(f)$ for all $g \in \mathrm{GL}_n(\mathbb{C})$.

A more algebraic definition of the Reynolds operator for GL_n and SL_n is in terms of the so-called omega process. This method was already known in the 19th century, but we will not discuss it here (see [38, 4.3]).

If G is a linearly reductive group acting rationally on an affine variety X, then the Reynolds operator also "acts" on the coordinate ring of X. Indeed, the action $\mu : G \times X \to X$ corresponds to a ring homomorphism

$$\mu^\star : K[X] \to K[G] \otimes K[X].$$

If we compose this with

$$\mathcal{R} \otimes \mathrm{id} : K[G] \otimes K[X] \to K \otimes K[X] \cong K[X]$$

where id is the identity, we get a linear map $(\mathcal{R} \otimes \mathrm{id}) \circ \mu^\star$ which we will denote by $\mathcal{R}_X$ (or simply again by $\mathcal{R}$ if there is no confusion).

Exercise 1.19. *Suppose that G is a linearly reductive group acting rationally on an affine variety X. Prove that:*

(a) *$\mathcal{R}_X$ is a $K[X]^G$-module homomorphism, i.e.,*

$$\mathcal{R}_X(\sum_i a_i f_i) = \sum_i \mathcal{R}_X(a_i) f_i$$

if $a_i \in K[X]$ and $f_i \in K[X]^G$ for all i,

(b) *$\mathcal{R}_X(f) = f$ for all $f \in K[X]^G$,*

(c) *if $V \subseteq K[X]$ is a G-stable subspace, then $\mathcal{R}_X(V) = V^G$.*

Exercise 1.20. *Suppose that X and Y are affine G-varieties and suppose that*

$$\psi : X \to Y$$

is a G-equivariant morphism. This means that $\psi(g \cdot x) = g \cdot \psi(x)$ for all $x \in X$ and all $g \in G$. The morphism ψ corresponds to a ring homomorphism $\psi^\star : K[Y] \to K[X]$.

(a) *Let $\mathcal{R}_X : K[X] \to K[X]^G$ and $\mathcal{R}_Y : K[Y] \to K[Y]^G$ be the Reynolds operators. Show that the diagram*

$$\begin{tikzcd} K[Y] \arrow[r, "\psi^\star"] \arrow[d, "\mathcal{R}_Y"'] & K[X] \arrow[d, "\mathcal{R}_X"] \\ K[Y]^G \arrow[r, "\psi^\star"'] & K[X]^G \end{tikzcd}$$

commutes, i.e., $\psi^\star \circ \mathcal{R}_Y = \mathcal{R}_X \circ \psi^\star$.

(b) *Suppose that $\psi : X \to Y$ is a closed immersion (i.e., $\psi^\star$ is surjective). Use (a) to prove that the restriction of $\psi^\star$ to $K[Y]^G$ gives a surjective ring homomorphism $K[Y]^G \to K[X]^G$. In particular, if $K[Y]^G$ is finitely generated, then so is $K[X]^G$.*

We will now prove Hilbert's Finiteness Theorem (stated in a slightly more general way).

Theorem 1.21. *Suppose that V is a representation of a linearly reductive group G. Then $K[V]^G$ is finitely generated.*

Proof. Define I as the ideal in $K[V]$ generated by all homogeneous invariants of positive degree. By Hilbert's Basissatz, I has finitely many generators. Each of these generators is lies in an ideal generated by *finitely many* homogeneous invariants of positive degree. It follows that I can be generated by finitely many homogeneous invariants, say $f_1, \dots, f_r$. We claim that $K[V]^G = K[f_1, \dots, f_r]$. Suppose that $h \in K[V]^G$ is homogeneous of degree d. We will prove by induction on d that $h \in K[f_1, \dots, f_r]$. The case $d = 0$ is trivial. If $d > 0$ then we can write

$$h = \sum_{i=1}^{r} a_i f_i \tag{1}$$

with $a_1, a_2, \dots, a_r \in K[V]$. We may assume that a_i is homogeneous of degree $d - \deg(f_i)$ for all i. We apply the Reynolds operator to (1) to obtain

$$h = \mathcal{R}(h) = \sum_{i=1}^{r} \mathcal{R}(a_i) f_i.$$

Now $\mathcal{R}(a_i)$ is a homogeneous invariant of degree $d - \deg(f_i) < d$ for all i (since $\mathcal{R}$ preserves degree by Exercise 1.19). By induction we have $\mathcal{R}(a_1), \dots, \mathcal{R}(a_r) \in K[V]^G$, hence $h \in K[V]^G$. □

Lemma 1.22. *If X is an affine G variety, then there exists a representation Y of G and a G-equivariant closed embedding $\psi : X \to Y$.*

Proof. Let $W \subset K[X]$ be a finite dimensional subspace such that W generates $K[X]$. Let Z be the span of all $g \cdot w$ with $g \in G$ and $w \in W$. It is clear that Z is G-stable and that Z generates $K[X]$. We claim that Z is still finite dimensional. Let $\mu^\star : K[X] \to K[G] \otimes K[X]$ be the homomorphism corresponding to the regular action $\mu : G \times X \to X$. We can find finite dimensional subspaces $A \subseteq K[G]$ and $B \subseteq K[X]$ such that $\psi^\star(W) \subseteq A \otimes B$. In particular, we have for fixed $g \in G$ and $w \in W$ that $(g \cdot f)(x) = \mu^\star(f)(g, x)$ (seen as a function on x only) lies in B. Since B is finite dimensional we get that Z is finite dimensional. The action of G on Z is again rational and linear, so Z is a representation.

We can view Z as the linear functions in the coordinate ring $K[Z^\star]$ of $Z^\star$. The inclusion $Z \to K[X]$ extends to a ring homomorphism $K[Z^\star] \to K[X]$ which respects the action of G. This homomorphism is surjective since Z generates $K[X]$. The homomorphism corresponds to a G-equivariant closed embedding of affine G-varieties $X \to Z^\star$. We can take $Y = Z^\star$. □

Remark 1.23. We can view G as a G-variety by letting G act on itself by left multiplication. By Lemma 1.22 there exists a G-equivariant embedding $\psi : G \to Y$ where Y is a representation of G. Now ψ induces a morphism $\phi : G \to \operatorname{End}(Y)$. It is not hard to show that $\phi(G)$ is Zariski closed and that ϕ induces an isomorphism between G and $\psi(G)$. In particular G can be identified with a closed subgroup of GL_n where $n = \dim Y$.

Corollary 1.24. *If X is an affine G-variety, and G is a linearly reductive group, then $K[X]^G$ is finitely generated.*

Proof. Let $\psi : X \to Y$ be a closed G-equivariant embedding where Y is a representation as in Lemma 1.22. We know that $K[Y]^G$ is finitely generated by Theorem 1.21. Hence $K[X]^G$ is finitely generated by Exercise 1.20. □

1.4. **An algorithm for computing generating invariants.** The **1890** proof of Hilbert's Finiteness Theorem is not constructive, and it was criticized for this. Nevertheless it was shown in [7] that it is possible to make an algorithm for computing generating invariants based on this proof.

Proposition 1.25. *Suppose that V is a representation of a linearly reductive group. Let again I be the ideal of $K[V]$ which is generated by all homogeneous invariants of positive degree. If $I = (f_1, f_2, \dots, f_r)$, then $K[V]^G = K[\mathcal{R}(f_1), \dots, \mathcal{R}(f_r)]$.*

Proof. Let $\mathfrak{m}$ be the maximal homogeneous ideal of $K[V]$. Since I and $\mathfrak{m}I$ are ideals which are stable under the action of G, we have $\mathcal{R}(I) \subseteq I$ and $\mathcal{R}(\mathfrak{m}I) \subseteq \mathfrak{m}I$. Now $\mathcal{R}$ induces a map

$$I/\mathfrak{m}I \to I/\mathfrak{m}I$$

which is just the identity, because I is generated by invariants. In particular this means that $I/\mathfrak{m}I$ is generated by the images of $\mathcal{R}(f_1),\dots,\mathcal{R}(f_r)$. By the homogeneous Nakayama lemma (see Exercise 1.26 below) it follows that $I=(\mathcal{R}(f_1),\dots,\mathcal{R}(f_r))$ and by the proof of Hilbert's Finiteness Theorem it follows now that $K[V]^G=K[\mathcal{R}(f_1),\dots,\mathcal{R}(f_r)]$. □

Exercise 1.26. *Prove the homogeneous Nakayama lemma: Suppose that $R=\bigoplus_{d=0}^{\infty}R_d$ is a finitely generated graded algebra over $R_0=K$ and suppose that M is a finitely generated graded R-module. (For example, $R=K[V]$ and $M=I\subset R$ is a homogeneous ideal.) Let $\mathfrak{m}=\bigoplus_{d=1}^{\infty}R_d$ be the maximal homogeneous ideal. Suppose that the images of some homogeneous elements $f_1,\dots,f_r\in M$ span the vector space $M/\mathfrak{m}M$. Then M is generated by $f_1,f_2,\dots,f_r$. (Hint: Let N be the submodule generated by $f_1,\dots,f_r$ and suppose that $M\neq N$. Let g be an element of $M\setminus N$ of minimal degree and deduce a contradiction.)*

Let $B\subseteq V\times V$ be the Zariski closure of the subset $\{(v,g\cdot v)\mid v\in V,g\in G\}$ and let $\mathfrak{b}$ be the vanishing ideal of B. The set B is sometimes called the *graph of the action.* The graph of an action is useful for studying invariant rings (see [35, 2.3],[24, pp. 20–24] and [29]). Once we have generators for the ideal, one can easily compute the Hilbert ideal I from Proposition 1.25 as we will explain below. We can identify the coordinate ring $K[V\times V]$ with the polynomial ring in two variables, $K[x_1,\dots,x_n,y_1,\dots,y_n]$. We will sometimes use the abbreviations $x=(x_1,x_2,\dots,x_n)$ and $y=(y_1,y_2,\dots,y_n)$.

Theorem 1.27. *We have*

$$(\mathfrak{b}+(y_1,\dots,y_n))\cap K[x_1,\dots,x_n]=I$$

In particular, if $\mathfrak{b}=(f_1(x,y),f_2(x,y),\dots,f_r(x,y))$, then

$$I=(f_1(x,0),f_2(x,0),\dots,f_r(x,0)).$$

Proof. If f is a homogeneous invariant of positive degree, then $f(x)-f(y)\in\mathfrak{b}$ since it vanishes on B. This proves "$\supseteq$".

We will now prove the other inclusion, "$\subseteq$". Suppose that $h(x,y)\in\mathfrak{b}+(y_1,y_2,\dots,y_n)$. We can write

$$h(x)=b+\sum_i a_i(x)f_i(y) \tag{2}$$

with $b\in\mathfrak{b}$ and f_i homogeneous of positive degree for all i. We view $V\times V$ as a representation of G where G acts trivially on the first factor and nontrivially on the second. To this action we associate a Reynolds operator

$$\mathcal{R}:K[V\times V]\to K[V\times V]^G=K[y_1,\dots,y_n]^G[x_1,\dots,x_n].$$

We apply $\mathcal{R}$ to (2) to obtain

$$h(x)=\mathcal{R}(b)+\sum_i a_i(x)\mathcal{R}(f_i(y))$$

Now we will substitute $y = x$. Note that $\mathcal{R}(b) \in \mathfrak{b}$ since $\mathfrak{b}$ is G-stable (see Exercise 1.19). Now $\mathcal{R}(b)$ will vanish on the diagonal of $V \times V$, which means that $\mathcal{R}(b)$ becomes 0 after the substitution $y = x$. We get

$$h(x) = \sum_i a_i(x)\mathcal{R}(f_i(x))$$

Now $\mathcal{R}(f_i(x))$ is a homogeneous invariant of positive degree for all i, so we have shown that $h(x) \in I$. □

The ideal $\mathfrak{b}$ can be obtained in a constructive way. First, since G is a linear algebraic group, we may view G as a Zariski closed subset of K^s for some s, so the coordinate ring of G is $K[z_1, z_2, \dots, z_s]/I_G$ where $I_G = (h_1(z), \dots, h_t(z))$ is the vanishing ideal of G. The representation of G on V is a homomorphism $G \to \mathrm{GL}(V)$ given by the $n \times n$ matrix

$$\begin{pmatrix} a_{1,1}(z) & a_{1,2}(z) & \cdots & a_{1,n}(z) \\ a_{2,1}(z) & a_{2,2}(z) & & a_{2,n}(z) \\ \vdots & & \ddots & \vdots \\ a_{n,1}(z) & a_{n,2}(z) & \cdots & a_{n,n}(z) \end{pmatrix}$$

where $a_{i,j}(z) \in K[z_1, \dots, z_s]$.

Let us define

$$\Gamma \subseteq G \times V \times V \subseteq K^s \times V \times V$$

by

$$\Gamma = \{(g, v, g \cdot v) \mid g \in G, v \in V\}$$

The vanishing ideal

$$I_\Gamma \subseteq K[z_1, \dots, z_s, x_1, \dots, x_n, y_1, \dots, y_n]$$

of Γ is given by

$$I_\Gamma = \Big(h_1(z), \dots, h_t(z), \Big\{y_i - \sum_{j=1}^n a_{i,j}(z)x_i \Big| i = 1, 2, \dots, n\Big\}\Big).$$

Note that

$$K[z_1, \dots, z_s, x_1, \dots, x_n, y_1, \dots, y_n]/I_\Gamma \cong$$
$$\cong K[z_1, \dots, z_s, x_1, \dots, x_n]/(h_1(z), \dots, h_t(z)) \cong K[G] \otimes K[V]$$

is a reduced ring an that I_Γ is therefore a radical ideal. Now B is the Zariski closure of the projection of Γ onto $V \times V$. It follows from this that

$$\mathfrak{b} = I_\Gamma \cap K[x_1, \dots, x_n, y_1, \dots, y_n].$$

Using Buchberger's algorithm, one can find a Gröbner basis of the ideal I_Γ with respect to the lexicographic ordering. In this way one also obtains a Gröbner basis of $\mathfrak{b}$ (see Exercise1.7) so in particular one has a set of generators of $\mathfrak{b}$ (see Proposition 1.6).

Example 1.28. For illustration, we give an easy example. Let G be the cyclic group of order 2 generated by σ. As an algebraic variety G is just a set of two points, so we can identify G with $\{\pm 1\} \subset K$. Now the coordinate ring of G is equal to $K[z]/(z^2-1)$.

Consider now the representation of G in K^2, defined by

$$\sigma \cdot (x_1, x_2) = (x_2, x_1).$$

This representation is given by the matrix

$$\begin{pmatrix} \frac{z+1}{2} & \frac{1-z}{2} \\ \frac{1-z}{2} & \frac{z+1}{2} \end{pmatrix}.$$

Indeed for $z = 1$ we get the identity matrix and for $z = -1$ we get

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

which represents the action of σ. We form the ideal

$$I_\Gamma = \Big(z^2 - 1, y_1 - \frac{z+1}{2}x_1 - \frac{1-z}{2}x_2, y_2 - \frac{1-z}{2}x_1 - \frac{z+1}{2}x_2\Big).$$

We use the Buchberger algorithm with the pure lexicographic ordering such that

$$z > x_1 > x_2 > y_1 > y_2$$

in the ring $K[z, x_1, x_2, y_1, y_2]$ and we obtain a Gröbner basis

$$\{z^2-1, x_2z-y_2z+x_2-y_2, y_1z-y_2z+2x_2-y_1-y_2, x_1+x_2-y_1-y_2, x_2^2-x_2y_2-x_2y_1+y_1y_2\}.$$

We only take the elements in this Gröbner basis which lie in $K[x_1, x_2, y_1, y_2]$. This gives us a Gröbner basis of $\mathfrak{b}$:

$$\{x_1 + x_2 - y_1 - y_2, x_2^2 - x_2y_2 - x_2y_1 + y_1y_2\}.$$

Now we substitute $y_1 = y_2 = 0$ and we obtain generators of Hilbert's ideal

$$I = (x_1 + x_2, x_2^2).$$

To find generators of $K[x_1, x_2]^G$ we have to apply the Reynolds operator to these to elements. For finite groups, the Reynolds operator is just averaging over the group (see Example 1.15). We obtain $\mathcal{R}(x_1+x_2) = x_1+x_2$ because x_1+x_2 was already invariant. Also we have that $\mathcal{R}(x_2^2) = (x_2^2 + x_1^2)/2$. We obtain

$$K[x_1, x_2]^G = K\Big[x_1 + x_2, \frac{x_1^2 + x_2^2}{2}\Big].$$

Clearly we run into trouble if K has characteristic 2, but then G is no longer linearly reductive.

2. Hilbert's second approach

Hilbert's first proof of 1890 was being criticized for not being constructive (although as we have just seen, it can be made constructive). In 1893 Hilbert gave a second, more constructive, proof (see [16]). This new proof is more geometric in nature. The correspondence between (radical) ideals and algebraic sets is of fundamental importance to algebraic geometry. This correspondance is based on Hilbert's *Nullstellensatz* which was proven in his invariant theory paper of 1893. (We actually already used algebraic geometry and therefore implicitly the Nullstellensatz throughout the previous section.) We again will assume that K is algebraically closed. The reader is assumed to be familiar with Hilbert's Nullstellensatz, the correspondance between affine algebraic varieties and finitely generated rings over the field K, and with the correspondance between radical ideals and Zariski closed subsets of affine varieties. We will stick to the following notation. If $J \subseteq K[X]$ is an ideal, then we call

$$\mathcal{Z}(J) = \{\alpha \in X \mid f(\alpha) = 0 \text{ for all } f \in J\}$$

the *zero set of* J. If $S \subseteq X$ is a subset, then the vanishing ideal of S is

$$\mathcal{I}(S) = \{f \in K[X] \mid f(s) = 0 \text{ for all } s \in S\}.$$

This section will be in the spirit of Hilbert's paper of 1893.

2.1. **Geometry of Invariant Rings.**

Suppose that G is a linearly reductive group, and that X is an affine G-variety. The invariant ring $K[X]^G$ is finitely generated, and corresponds to an affine variety which will be denoted by $X/\!\!/G$. The inclusion $K[X]^G \subseteq K[X]$ induces a dominant morphism $\pi : X \to X/\!\!/G$. This map π we will call *categorical quotient* (since it has certain universal properties in the category of affine varieties). Sometimes the affine variety $X/\!\!/G$ itself is called the categorical quotient. We will study some of the nice geometric properties of this quotient map.

If $J = \mathcal{I}(Y) \subseteq K[X]^G$ is the vanishing ideal of a Zariski closed subset $Y \subseteq X/\!\!/G$, then $\sqrt{K[X]J}$ is the vanishing ideal of $\pi^{-1}(Y) \subseteq X$. If $J = \mathcal{I}(Y) \subseteq K[X]$ is the vanishing ideal of $Y \subseteq X$, then $J^G = J \cap K[X]^G$ is the vanishing ideal of $\overline{\pi(Y)}$, the Zariski closure of $\pi(Y) \subseteq X/\!\!/G$.

Exercise 2.1. *Prove that for a linearly reductive group and an affine G-variety X the categorical quotient $\pi : X \to X/\!\!/G$ has the following universal property. If $\psi : X \to Y$ is a morphism of affine varieties which is constant on orbits, then there exists a unique morphism of affine varieties $\varphi : X/\!\!/G \to Y$ such that $\varphi \circ \pi = \psi$.*

Proposition 2.2. *The categorical quotient $\pi : X \to X/\!\!/G$ has the following properties:*

(a) *$\pi : X \to X/\!\!/G$ is surjective.*

(b) *If $Y_1, Y_2 \subseteq X$ are G-stable and Zariski closed, then*

$$\overline{\pi(Y_1)} \cap \overline{\pi(Y_2)} = \overline{\pi(Y_1 \cap Y_2)}.$$

(c) *If $Y \subseteq X$ is G-stable and Zariski closed, then $\pi(Y)$ is Zariski closed.*

(d) *The topology of $X/\!\!/G$ is the quotient topology.*

(e) *For every $x \in X/\!\!/G$, $\pi^{-1}(x)$ contains exactly one closed orbit. Every orbit closure in $\pi^{-1}(x)$ contains the closed orbit.*

Proof. (a) Let $x \in X/\!\!/G$ and let $\mathfrak{m}_x = \mathcal{I}(\{x\}) \subset K[X]^G$ be the corresponding maximal ideal. The vanishing ideal of $\pi^{-1}(x)$ is $\sqrt{K[X]\mathfrak{m}_x}$. If $\pi^{-1}(x) = \emptyset$, then $1 \in K[X]\mathfrak{m}_x$, say

$$1 = \sum_{i=1}^{r} a_i f_i \tag{3}$$

with $a_1, \dots, a_r \in K[X]$ and $f_1, \dots, f_r \in \mathfrak{m}_x \subset K[X]^G$ by Hilbert's Nullstellensatz. We apply the Reynolds operator $\mathcal{R}_X : K[X] \to K[X]^G$ to (3):

$$1 = \mathcal{R}_X(1) = \sum_{i=1}^{r} \mathcal{R}_X(a_i) f_i$$

The righthandside clearly lies in $\mathfrak{m}_x$ since $\mathcal{R}_X(a_i) \in K[X]^G$ for all i. We see that $1 \in \mathfrak{m}_x$ which gives a contradiction to our assumption that $\mathfrak{m}_x$ is a maximal ideal.

(b) Suppose that $I_1 = \mathcal{I}(Y_1), I_2 = \mathcal{I}(Y_2) \subset K[X]$ are the vanishing ideals of Y_1 and Y_2 respectively. We have

$$(I_1 + I_2)^G = \mathcal{R}_X(I_1 + I_2) = \mathcal{R}_X(I_1) + \mathcal{R}_X(I_2) = I_1^G + I_2^G.$$

Now the zero set of $(I_1 + I_2)^G$ is $\overline{\pi(Y_1 \cap Y_2)}$ and the zero set of $I_1^G + I_2^G$ is $\overline{\pi(Y_1)} \cap \overline{\pi(Y_2)}$.

(c) Suppose that $x \in \overline{\pi(Y)} \setminus \pi(Y)$. Now $\pi^{-1}(x)$ and Y are G-stable and Zariski closed. By (b) we have

$$x \in \overline{\pi(\pi^{-1}(x))} \cap \overline{\pi(Y)} = \overline{\pi(\pi^{-1}(x) \cap Y)} = \emptyset$$

and we get a contradiction.

(d) This is clear, since $Y \subset X/\!\!/G$ is Zariski closed if and only if $\pi^{-1}(Y)$ is Zariski closed by (c).

(e) If $\pi^{-1}(x)$ contains at least 2 distinct closed orbits say $G \cdot y_1$ and $G \cdot y_2$, then

$$x \in \pi(G \cdot y_1) \cap \pi(G \cdot y_2) = \pi((G \cdot y_1) \cap (G \cdot y_2)) = \emptyset$$

by (b) and (c) which is a contradiction. Therefore $\pi^{-1}(x)$ has at most 1 closed orbit.

Now we will show that $\pi^{-1}(x)$ has at least one closed orbit. First we note that orbits are always locally closed, i.e., if $x \in X$, then the orbit $G \cdot x$ is a Zariski open subset of its closure $\overline{G \cdot x}$. To see this, we remark that as the image of a morphism, $G \cdot x$ is constructible. Therefore, $G \cdot x$ contains an nonempty open subset U of $\overline{G \cdot x}$. It is clear that $G \cdot x = G \cdot U$. But $G \cdot U \subseteq \overline{G \cdot x}$ is open since it is a union of open subsets.

Choose $y_1 \in \pi^{-1}(x)$. We define $y_2, y_3, \dots, \in \pi^{-1}(x)$ by induction as follows. For every i, choose $y_{i+1} \in \overline{G \cdot y_i} \setminus G \cdot y_i$. If for some i, $G \cdot y_i$ is closed, then we have proven that $\pi^{-1}(x)$ has a closed orbit (and $\overline{G\cdot y_1}$ contains that closed orbit $G\cdot y_i$). Otherwise, we get an infinite sequence

$$\overline{G\cdot y_1}\supseteq\overline{G\cdot y_2}\supseteq\cdots. \tag{4}$$

Also observe that $\overline{G\cdot y_{i+1}}$ is contained in $\overline{G\cdot y_i}\setminus G\cdot y_i$ because $G\cdot y_i$ is open in $\overline{G\cdot y_i}$. In particular, (4) is a strictly descreasing sequence of Zariski closed sets, which contradicts the Noetherian property. □

Example 2.3. Let $G=\mathbb{C}^\star$ be the multiplicative group acting on $V:=\mathbb{C}^3$ as follows:

$$\lambda,(x_1,x_2,x_3)=(\lambda^{-2}x_1,\lambda x_2,\lambda^3x_3).$$

The invariant ring $K[V]^{\mathbb{C}^\star}$ is generated by $x_1x_2^2$ $x_1^2x_2x_3$ and $x_1^3x_3^2$. We have

$$K[V]^{\mathbb{C}^\star}=K[x_1x_2^2,x_1^2x_2x_3,x_1^3x_3^2]\cong K[y_1,y_2,y_3]/(y_2^2-y_1y_3).$$

We consider the quotient map

$$\pi:\mathbb{C}^3\to\mathbb{C}^3/\!\!/\mathbb{C}^\star\cong\{(y_1,y_2,y_3)\in\mathbb{C}^3\mid y_2^2-y_1y_3=0\}.$$

We get

$$\pi^{-1}(0)=\{(x_1,x_2,x_3)\in\mathbb{C}^3\mid x_1x_2^2=x_1^2x_2x_3=x_1^3x_3^2=0\}=$$
$$=\{(x_1,x_2,x_3)\in\mathbb{C}^3\mid x_1=0\text{ or }x_2=x_3=0\}.$$

If $x_1\neq0$ then the orbit of $(x_1,0,0)$ is not closed (take the limit $\lambda\to\infty$ and one sees that $(0,0,0)$ lies in the orbit closure). If $x_2\neq0$ or $x_3\neq0$, then the orbit of $(0,x_2,x_3)$ is not closed (take the limit $\lambda\to0$ and one sees again that $(0,0,0)$ lies in the orbit closure). The only closed orbit in $\pi^{-1}(0)$ is $\{0\}$. For any nonzero $y\in\mathbb{C}^3/\!\!/C^\star$, one can check that the fiber $\pi^{-1}(y)$ is connected and one dimensional. Since $\pi^{-1}(y)$ does not contain any zero dimensional orbits, $\pi^{-1}(y)$ consists of a single orbit.

Exercise 2.4. *A quotient $\pi:X\to X/\!\!/G$ is called geometric, if the fibers of π are exactly the orbits in X. Suppose that G is a linearly reductive group and X is an affine G-variety. Show that the categorical quotient $\pi:X\to X/\!\!/G$ is geometric if and only if all orbits in X are Zariski closed.*

Exercise 2.5. *Consider the group $\mathrm{GL}_n(\mathbb{C})$ acting on the $n\times n$ matrices $\mathrm{M}_n(\mathbb{C})$ by conjugation. The categorial quotient $\pi:\mathrm{M}_n(\mathbb{C})\to\mathbb{C}^n$ is equal to*

$$A\mapsto(s_1(A),s_2(A),\ldots,s_n(A))$$

where $s_i(A)$ is defined by

$$\det(\lambda I+A)=\lambda^n+s_1(A)\lambda^{n-1}+\cdots+s_n(A).$$

Using the Jordan normal form, describe the orbits in the fibers of this quotient map. Identify the closed orbit in each fiber.

2.2. **Hilbert's Nullcone.** Suppose now that V is a representation of a linearly reductive group G. Let $I \subseteq K[V] \cong K[x_1, \dots, x_n]$ be again the ideal generated by all homogeneous invariants of positive degree. We define

$$\mathcal{N} = \mathcal{Z}(I).$$

Geometrically, $\mathcal{N}$ is equal to $\pi^{-1}(\pi(0))$ where $\pi : V \to V/\!\!/G$ is the categorical quotient. The only closed orbit in $\pi^{-1}(\pi(0))$ must be the orbit $\{0\}$. By Proposition 2.2 it follows that

$$\mathcal{N} = \pi^{-1}(\pi(0)) = \{v \in V \mid 0 \in \overline{G \cdot v}\}.$$

This set $\mathcal{N}$ is often called *Hilbert's nullcone.*

Definition 2.6. A *1-Parameter SubGroup (1-PSG)* $\lambda : K^\star \to G$ is a morphism which is also a homomorphism of groups.

One parameter subgroups give an easy way to describe Hilbert's Nullcone because of the following result.

Theorem 2.7 (Hilbert-Mumford criterion)**.** *Suppose that $v \in V$, then*

$$v \in \mathcal{N} \Leftrightarrow \textit{there exists a } 1\textit{-PSG such that } \lim_{t\to 0} \lambda(t) \cdot v = 0.$$

The limit $\lim_{t\to 0} \lambda(t) \cdot v$ may not make any immediate sense because we are working over an arbitrary algebraically closed field K, not necessarily $\mathbb{C}$. However, note that $\lambda(t) \cdot v$ can be seen as a vector of Laurent polynomials. For a Laurent polynomial $p(t) \in K[t, t^{-1}]$ we say that $\lim_{t\to 0} p(t)$ exists if $p(t)$ is actually a polynomial. In that case we define $\lim_{t\to 0} p(t) = p(0)$.

Example 2.8. Suppose that $G = \mathrm{SL}_2$ and

$$V_d = \{a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d \mid a_0, \dots, a_d \in K\}$$

is again the binary forms of degree d. We can define a 1-PSG $\lambda : K^\star \to G$ by

$$\lambda(t) = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$$

If

$$f(X,Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d$$

then

$$\lambda(t) \cdot f(X,Y) = a_0X^dt^d + a_1X^{d-1}Yt^{d-2} + \cdots + a_dY^dt^{-d}.$$

Therefore,

$$\lim_{t\to\infty} \lambda(t) \cdot f(X,Y) = 0$$

if and only if $a_i = 0$ for $i \geq \frac{d}{2}$. This condition is equivalent with $Y^{\lceil (d+1)/2 \rceil}$ divides $f(X,Y)$. Every 1-PSG for SL_2 is actually conjugate to

$$t \mapsto \begin{pmatrix} t^k & 0 \\ 0 & t^{-k} \end{pmatrix}$$

for some k. It follows that

$$f(X,Y) \in \mathcal{N} \Leftrightarrow f(X,Y) \text{ has a zero of multiplicity } > \tfrac{d}{2}.$$

Proposition 2.9. *Suppose that $f_1, f_2, \ldots, f_r \in K[V]^G$ are homogeneous invariants of positive degree such that $\mathcal{Z}(f_1, f_2, \ldots, f_r) = \mathcal{N}$. Then $K[V]^G$ is a finite $K[f_1, \ldots, f_r]$-module, i.e., there exist finitely many $u_1, \ldots, u_t$ such that $K[V]^G = Fu_1 + \cdots + Fu_t$ where $F = K[f_1, \ldots, f_r]$.*

Proof. Let $h_1, \ldots, h_s$ such that $K[V]^G = K[h_1, \ldots, h_s]$. We can choose an l such that for all i we have

$$h_i^l \in K[V]f_1 + \cdots + K[V]f_r$$

and therefore

$$h_i^l = \mathcal{R}_V(h_i^l) \in K[V]^G f_1 + \cdots + K[V]^G f_r.$$

The $K[f_1, \ldots, f_r]$-module

$$K[V]^G/(f_1, \ldots, f_r)K[V]^G$$

is spanned by the images of all $h_1^{a_1} h_2^{a_2} \cdots h_s^{a_s}$ with $a_1, \ldots, a_s \in \{0, 1, 2, \ldots, l-1\}$. From the homogeneous Nakayama Lemma (Exercise 1.26) it follows that these elements generate $K[V]^G$ as a $K[f_1, \ldots, f_r]$-module. □

2.3. **Homogeneous Systems of Parameters.**

Definition 2.10. A set of homogeneous polynomials $p_1, \ldots, p_s \in K[V]^G$ is called a *homogeneous system of parameters (HSOP)* if

(1) $K[V]^G$ is a finite module over $P := K[p_1, \ldots, p_s]$.
(2) $p_1, \ldots, p_s$ are algebraically independent.

Lemma 2.11. *A set of homogeneous polynomials $p_1, \ldots, p_s \in K[V]^G$ is a HSOP if and only of $\mathcal{Z}(p_1, \ldots, p_s) = \mathcal{N}$ and $s = \dim K[V]^G$.*

Exercise 2.12. *Prove the previous lemma.*

The following result is a corollary of the Noether Normalization Lemma (although it was already used by Hilbert):

Theorem 2.13. *The invariant ring $K[V]^G$ has a homogeneous system of parameters.*

Proof. We will sketch the proof. Choose $f_1, \ldots, f_r \in K[V]^G$ homogeneous such that $\mathcal{Z}(f_1, \ldots, f_r) = \mathcal{N}$ (for example take homogeneous nonconstant generators of the invariant ring). Define $d_i := \deg(f_i)$ for all i and $d = \operatorname{lcm}(d_1, \ldots, d_r)$. Also define $\widehat{f_i} = f_i^{d/d_i}$ for all i. Note that $\widehat{f_1}, \ldots, \widehat{f_r} \in K[V]^G$ are all of degree d, and $\mathbb{Z}(\widehat{f_1}, \ldots, \widehat{f_r}) = \mathcal{N}$. Instead of looking at Zariski closed subsets in V, we will look at Zariski closed subsets in $V/\!\!/G$. For polynomials $g_1, \ldots, g_s \in K[V]^G$ we will denote their common zero set in $V/\!\!/G$ by $\mathcal{Z}_{V/\!\!/G}(g_1, \ldots, g_s)$. Since

$$\mathcal{Z}(\widehat{f_1}, \ldots, \widehat{f_r}) = \mathcal{N} = \pi^{-1}(0)$$

and π is surjective, we have that

$$\mathcal{Z}_{V/\!/G}(\widehat{f}_1, \dots, \widehat{f}_r) = \{0\}.$$

Here $0 \in V/\!/G$ is defined as $\pi(0)$, the image of $0 \in V$ under π. We will define p_i $(0 \leq 1 \leq s = \dim K[V]^G)$ by

$$p_i = \sum_{j=1}^{r} \alpha_{i,j} \widehat{f}_j.$$

for some suitable $\alpha_{i,j}$. Now for suitable choices of $\alpha_{1,1}, \dots, \alpha_{1,r}$ we have that $\mathcal{Z}_{V/\!/G}(p_1)$ has dimension $s-1$. Then for suitable choices of $\alpha_{2,1}, \dots, \alpha_{2,r}$ we get $\dim \mathcal{Z}_{V/\!/G}(p_1, p_2) = s-2$. So eventually we will get $\dim \mathcal{Z}_{V/\!/G}(p_1, \dots, p_s) = 0$. Scalar multiplication on V also induces an action of $K^\star$ on $V/\!/G$. If $x \in \mathcal{Z}_{V/\!/G}(p_1, \dots, p_s)$ then also $\lambda \cdot x \in \mathcal{Z}_{V/\!/G}(p_1, \dots, p_s)$ for all $\lambda \in K^\star$, because $p_1, \dots, p_s$ are homogeneous. Since the dimension of $\mathcal{Z}_{V/\!/G}(p_1, \dots, p_s)$ is 0, x must be a fixed point of $K^\star$. The only fixed point in $V/\!/G$ is 0, so it follows that

$$\mathcal{Z}_{V/\!/G}(p_1, \dots, p_s) = \{0\}$$

and

$$\mathcal{Z}(p_1, \dots, p_s) = \pi^{-1}(0) = \mathcal{N}.$$

From Lemma 2.11 it follows that $p_1, p_2, \dots, p_s$ is a HSOP. □

3. The Cohen-Macaulay property

Suppose that $R = \bigoplus_{d=0}^{\infty} R_d$ is a graded ring of dimension s with $R_0 = K$. The maximal homogeneous ideal of R is $\mathfrak{m} = \bigoplus_{d=1}^{\infty} R_d$. Let M be a finitely generated graded R-module. The dimension $\dim(M)$ of the module M is defined as the dimension of $R/\operatorname{Ann}(M)$ where

$$\operatorname{Ann}(M) = \{f \in R \mid f \cdot a = 0 \text{ for all } a \in M\}$$

is the annihilator of M.

A regular sequence of length r for the module M is a sequence of nonzero homogeneous $f_1, f_2, \dots, f_r \in \mathfrak{m}$ such that multiplication by f_i is injective on the module $M/(f_1, f_2, \dots, f_{i-1})M$ for $i = 1, 2, \dots, r$. We define $\operatorname{depth}(M)$ as the largest integer r for which there exists a regular sequence of length r for the module M. It can be shown that $\operatorname{depth}(M) \leq \dim(M)$ (see [11, Proposition 18.2]). The module M is called *Cohen-Macaulay* if $\operatorname{depth}(M) = \dim(M)$. For more details on Cohen-Macaulay modules, the reader is referred to [5]. The ring R is called Cohen-Macaulay if it is Cohen-Macaulay as a module over itself. The following result will not be proven here.

Lemma 3.1. *If $R = \bigoplus_{d=0}^{\infty} R_d$ is a finitely generated graded Cohen-Macaulay ring over $R_0 = K$ of dimension s and $p_1, \dots, p_s \in R$ is a HSOP, then $p_1, p_2, \dots, p_s$ is a regular sequence.*

Proof. See for example [2, Theorem 4.3.5], [22] or [36]. □

The following theorem is the main result in this section.

Theorem 3.2 (Hochster-Roberts, [18]). *If G is linearly reductive, then $K[V]^G$ is Cohen-Macaulay.*

We will sketch a proof in this section. More detailed proofs can be found in [18], [5] and [9, 2.5.2]. Note that if $p_1, \dots, p_s \in K[V]^G$ is a HSOP, then by Lemma 3.1 we have that $p_1, \dots, p_s$ is a regular sequence. The following result we will prove later:

Lemma 3.3. *If $p_1, \dots, p_s \in K[V]^G$ is a HSOP, then $K[V]^G$ is a free P-module, with $P = K[p_1, \dots, p_s]$, i.e.,*

$$K[V]^G = Ph_1 \oplus \cdots \oplus Ph_l$$

for certain homogeneous $h_1, \dots, h_l \in K[V]^G$.

Proof of Theorem 3.2. We will now start the sketch of the proof of the Hochster-Roberts Theorem. Recall that we have the Reynolds operator $\mathcal{R} : K[V] \to K[V]^G$. Therefore it will be enough to prove the following theorem:

Theorem 3.4. *Let $R := K[x_1, \dots, x_n]$ and let $S \subseteq R$ be a graded subring. Also suppose that $\varphi : R \to S$ is an S-module homomorphism with $\varphi(s) = s$ for all $s \in S$. Then S is Cohen-Macaulay.*

Proof. We will prove the theorem only in positive characteristic! The theorem is true also in characteristic 0, but in order to prove it in characteristic 0 one has to pass to positive characteristic and this step we will not present here.

Assume that K is an algebraically closed field of characteristic $p > 0$.

Definition 3.5. If q is a power of p, and $I = (f_1, \dots, f_r) \subseteq R$ is an ideal, then $I^{[q]}$ is defined as

$$I^{[q]} = (f_1^q, \dots, f_r^q).$$

Exercise 3.6. *Prove that $I^{[q]}$ is well-defined, i.e., the definition does not depend on the choice of the generators $f_1, \dots, f_r$.*

If $I \subseteq R$ is an ideal and $f \in R$ then the *colon ideal* $(I : f)$ is defined by

$$(I : f) = \{a \in R \mid af \in I\}.$$

Proposition 3.7. *We have*

$$(I^{[q]} : f^q) = (I : f)^{[q]}.$$

Proof. The inclusion $\supseteq$ is easy: If $af \in I$, then $(af)^q \in I^{[q]}$, so $a^q \in (I^{[q]}, f^q)$.

We will prove the inclusion $\subseteq$. Suppose that $I = (f_1, \dots, f_r)$. Let us assume that $a \in (I^{[q]} : f^q)$. We have

$$af^q = \sum_{j=1^r} a_j f_j^q.$$

We can write

$$a = \sum_i b_i m_i$$

where $b_i \in K[x_1^q, \dots, x_n^q]$ for all i, and the m_i run over all monomials $x_1^{e_1} \cdots x_n^{e_n}$ with $0 \leq e_1, \dots, e_n \leq q-1$. Since $K[x_1, \dots, x_n]$ is a free module over $K[x_1^q, \dots, x_n^q]$, generated by the m_i's, it follows that the b_i's are unique. In a similar fashion we can write

$$a_j = \sum_i b_{i,j} m_i.$$

for all j. We obtain

$$\sum_i (b_i f^q) m_i = \sum_i (\sum_{j=1}^r b_{i,j} f_j^q) m_i$$

Comparing coefficients gives us

$$b_i f^q = \sum_{j=1}^r b_{i,j} f_j^q.$$

for all i. We have assumed that K is algebraically closed. In particular we can choose $c_i, c_{i,j} \in K$ such that $c_i^q = b_i$ and $c_{i,j}^q = b_{i,j}$ for all i and j. So we have

$$(c_i f)^q = c_i^q b_i^q = \sum_{j=1}^r c_{i,j}^q f_j^q = (\sum_{j=1}^r c_{i,j} f_j)^q.$$

Hence we get

$$c_i f = \sum_{j=1}^r c_{i,j} f_j.$$

It follows that $c_i \in (I : f)$ and $b_i \in (I : f)^{[q]}$ for all i. We conclude that $a \in (I : f)^{[q]}$. □

Definition 3.8. Suppose that $I \subseteq R$ is an ideal. The *tight closure* $I^\star$ of I is the ideal of all $f \in R$ for which there exist a nonzero $c \in R$ and a constant N such that $cf^q \in I^{[q]}$ for every p-power q with $q \geq N$.

Theorem 3.9. *For any ideal I of R we have $I^\star = I$.*

Proof. Suppose that $f \in I^\star$. There exists $c \in R \setminus \{0\}$ such that $cf^q \in I^{[q]}$ for $q \gg 0$ and q a p-power. Then we have

$$c \in \bigcap_{q \gg 0} (I^{[q]} : f^q) = \bigcap_{q \gg 0} (I : f)^{[q]} \subseteq \bigcap_{q \gg 0} (I : f)^q$$

If $(I : f) \neq R$ then $\bigcap_{q \gg 0} (I : f)^q = (0)$ and we have a contradiction because c is nonzero. Therefore $(I : f) = R$, and $f \in I$. □

We continue with the proof of Theorem 3.4. Suppose that $f_1, \dots, f_s$ is a homogeneous system of parameters of S. We write $(f_1, \dots, f_s)_S$ for the ideal in S generated by $f_1, \dots, f_s$ and $(f_1, \dots, f_s)_R$ for the ideal in R generated by $f_1, \dots, f_s$. We will show that $f_1, f_2, \dots, f_r$ is a regular sequence in S. Suppose that $a_r f_r = \sum_{i=1}^{r-1} a_i f_i$ with $a_1, \dots, a_r \in S$. We will prove that $a_r \in (f_1, \dots, f_{r-1})_S$. It suffices to prove that $a_r \in (f_1, \dots, f_{r-1})_R$ because by applying ϕ it would follow that $a_r \in (f_1, \dots, f_{r-1})_S$. Define $A := K[f_1, \dots, f_s]$. Choose $g_1, \dots, g_l \in S$ linearly independent over the field $K(f_1, \dots, f_s)$. Define

$$F = Ag_1 \oplus \cdots \oplus Ag_l.$$

There exists an element $c \in A$ such that $cR \subseteq F$. Now

$$c(a_r f_r)^q = c \sum_{i=1}^{r-1} a_i^q f_i^q \in (f_1^q, \dots, f_{r-1}^q)F.$$

Because F is a free module and $f_1^q, f_2^q, \dots, f_r^q$ is a regular sequence for this module, we obtain

$$c a_r^q \in (f_1^q, \dots, f_{r-1}^q)F$$

for all p-powers q. It follows that

$$c a_r^q \in (f_1^q, \dots, f_{r-1}^q)_R = (f_1, \dots, f_{r-1})^{[q]}.$$

Therefore,

$$a_r \in (f_1, \dots, f_{r-1})^\star = (f_1, \dots, f_{r-1}).$$

□

4. Hilbert series

4.1. **Basic properties of Hilbert series.** Suppose that $V = \bigoplus_{d=a}^{\infty} V_d$ is a graded vector space such that $\dim V_d < \infty$ for all d. Then we can define the formal power series $H(V,t)$ by

$$H(V,t) = \sum_{d=a}^{\infty} (\dim V_d) t^d.$$

The series $H(V,t)$ is called the *Hilbert series* of V (also called *Poincaré series* or *Molien series*). We will be particularly interested in the Hilbert series of invariant rings.

Example 4.1. Let $R = K[x_1, \dots, x_n]$. We can define a grading on R by $\deg(x_i) = d_i$. Now R is spanned by the monomials $x_1^{a_1} \cdots x_n^{a_n}$ with $a_1, \dots, a_n \geq 0$. Therefore, the Hilbert series of R are equal to

$$H(R,t) = \sum_{a_1, \dots, a_n \geq 0} (t^{d_1})^{a_1} \cdots (t^{d_n})^{a_n} = \frac{1}{(1 - t^{d_1}) \cdots (1 - t^{d_n})}.$$

If V, V', V'' are graded vector spaces

$$0 \to V' \to V \to V'' \to 0$$

is an exact sequence of graded vector spaces (with the appropiate finiteness conditions) then $H(V,t) = H(V',t) + H(V'',t)$. This is useful to for computing Hilbert series.

If $J \subseteq R := K[x_1, \dots, x_n]$ is a graded ideal, and $<$ is a monomial ordering compatible with the grading on R, then

$$H(J,t) = H(\mathrm{lm}(J), t)$$

where $\mathrm{lm}(J)$ is the ideal of leading monomials as before. Indeed, the reader may check that $\dim J_d = \dim \mathrm{lm}(J)_d$ for all d.

In his 1890 paper, Hilbert showed that every ideal $J \subseteq R$ has a finite free resolution. In particular this implies that $H(J,t)$ is a rational function for any graded ideal J of R (also $H(M,t)$ is a rational function for any finitely generated graded R-module M).

Exercise 4.2. *Prove by induction on the number of generators, then $H(I,t)$ is a rational function for any monomial ideal I of R, thus proving that $H(J,t)$ is rational for any graded ideal J of R.*

Suppose that $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ are homogeneous. Put $d_i = \deg(f_i)$. Consider the polynomial ring $K[y_1, \dots, y_r]$ with $\deg(y_i) = d_i$ for all i. We can define a surjective ring homomorphism

$$K[y_1, \dots, y_r] \to K[f_1, \dots, f_r]$$

by $y_i \mapsto f_i$ for all i. Let J be the kernel of this homomorphism. We have an exact sequence

$$0 \to J \to K[y_1, \dots, y_r] \to K[f_1, \dots, f_r] \to 0.$$

This implies that

$$H(K[f_1, \dots, f_r], t) = H(K[y_1, \dots, y_r], t) - H(J,t).$$

We have seen that $H(K[y_1, \dots, y_r], t)$ and $H(J,t)$ are rational, therefore $H(K[f_1, \dots, f_r], t)$ is rational.

To compute $H(K[f_1, \dots, f_r], t)$ in practice, we have to be able to find the ideal J. This can be done again using Gröbner basis techniques. Consider the ideal

$$\mathfrak{a} \subseteq K[x_1, \dots, x_n, y_1, \dots, y_r]$$

defined by

$$\mathfrak{a} = (f_1 - y_1, \dots, f_r - y_r).$$

Then J is the intersection of $\mathfrak{a}$ with $K[y_1, \dots, y_r]$. To compute this intersection, we can use Gröbner bases as in Exercise 1.7.

In particular if V is a representation and G is a linearly reductive group, then $K[V]^G$ is finitely generated by homogeneous invariants, so $H(K[V]^G, t)$ is a rational function. If we have found generators of $K[V]^G$, then $H(K[V]^G, t)$ can be computed as above. This is however not the way we go about it in practice. As we will see later, $H(K[V]^G, t)$

can be computed *a priori*, i.e., without knowing the generators. This is quite useful. Suppose that $f_1, \dots, f_r \in K[V]^G$ are homogeneous, but we are not sure if they are generators. Then $f_1, \dots, f_r$ generate $K[V]^G$ if and only if

$$H(K[f_1, \dots, f_r], t) = H(K[V]^G, t).$$

So comparison of Hilbert series gives us a criterion whether we have found a set of generating invariants of the invariant ring.

We give another application of Hilbert series. We will prove Lemma 3.3.

Proof of Lemma 3.3. Suppose that V is a representation of a linearly reductive algebraic group G. Let $p_1, \dots, p_s$ be a homogeneous system of parameters of $K[V]^G$ and put $P = K[p_1, \dots, p_s]$. The ring $K[V]^G$ is Cohen-Macaulay and $p_1, p_2, \dots, p_s$ is a regular sequence. The ring $K[V]^G/(p_1, \dots, p_s)$ is finite dimensional. Choose $h_1, \dots, h_l \in K[V]^G$ homogeneous such that their images span $K[V]^G/(p_1, \dots, p_s)$. By the Homogeneous Nakayama Lemma (see Exercise 1.26) we have

$$K[V]^G = Ph_1 + Ph_2 + \dots + Ph_l.$$

We claim that the sum on the right hand side is direct. It suffices to show that

$$H(K[V]^G, t) = H(Ph_1 \oplus Ph_2 \oplus \dots \oplus Ph_l, t).$$

First we evaluate the right-hand side. Let $d_i = \deg(p_i)$ for all i and $e_j = \deg h_j$ for all j. We have

$$H(P, t) = \frac{1}{(1 - t^{d_1})(1 - t^{d_2}) \cdots (1 - t^{d_s})}$$

and

$$H(Ph_1 \oplus \dots \oplus Ph_l, t) = \frac{t^{e_1} + t^{e_2} + \dots + t^{e_l}}{(1 - t^{d_1})(1 - t^{d_2}) \cdots (1 - t^{d_s})}. \tag{5}$$

Now we will compute $H(K[V]^G, t)$. Consider the exact sequence

$$0 \to p_r K[V]^G/(p_1, \dots, p_{r-1}) \to K[V]^G/(p_1, \dots, p_{r-1}) \to K[V]^G/(p_1, \dots, p_r) \to 0.$$

Note that since $p_1, \dots, p_r$ is regular, we get

$$H(p_r K[V]^G/(p_1, \dots, p_{r-1}), t) = t^{d_r} H(K[V]^G/(p_1, \dots, p_{r-1}), t).$$

We have

$$H(K[V]^G/(p_1, \dots, p_r), t) = H(K[V]^G/(p_1, \dots, p_{r-1}), t) - H(p_r K[V]^G/(p_1, \dots, p_{r-1}), t) =$$
$$= (1 - t^{d_r}) H(K[V]^G/(p_1, \dots, p_{r-1}), t).$$

By induction we obtain

$$H(K[V]^G/(p_1, \dots, p_s), t) = (1 - t^{d_1})(1 - t^{d_2}) \cdots (1 - t^{d_s}) H(K[V]^G, t). \tag{6}$$

Since the images of $h_1, \dots, h_l$ in $K[V]^G/(p_1, \dots, p_s)$ form a basis, we have

$$H(K[V]^G/(p_1, \dots, p_s), t) = t^{e_1} + t^{e_2} + \dots + t^{e_l} \tag{7}$$

Combining (6), (7) and (5) gives us

$$H(K[V]^G,t)=\frac{t^{e_1}+t^{e_2}+\cdots+t^{e_l}}{(1-t^{d_1})(1-t^{d_2})\cdots(1-t^{d_s})}=H(Ph_1\oplus\cdots\oplus Ph_l,t).$$

□

4.2. **Computing Hilbert series a priori.** For a linearly reductive group G and a representation V it is possible to compute the Hilbert series $H(K[V]^G,t)$ *a priori*, i.e., without knowing explicit generators of the invariant ring $K[V]^G$. For finite groups, there is *Molien's formula* for the invariant ring. For connected reductive groups there is a formula due to Weyl. There is a particularly nice formula for the SL_2 by Springer (see [37]). Littelmann and Procesi used this formula to compute the Hilbert series of binary forms up to a large degree ([4]).

To understand the formula's for the Hilbert series of invariant rings for connected reductive groups in general, one needs to understand the representation theory of G and Weyl's character formula in particular. This is somewhat beyond the scope of this paper. We will discuss here Molien's formula and we also will show how to compute the Hilbert series of the invariant ring for the multiplicative group $K^\star$.

Suppose that G is a finite group and $\rho_V: G\to \mathrm{GL}(V)$ is a representation over a field K of characteristic 0. Now $I-t\rho_V(g)$ is an endomorphism of V with a parameter t in it. The expression $\det(I-t\cdot\rho_V(g))$ is a polynomial of degree $n:=\dim V$ in t.

Theorem 4.3 (Molien's formula)**.**

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

Proof. Suppose that $\rho_W: G\to\mathrm{GL}(W)$ is a representation of G. Then

$$\frac{1}{|G|}\sum_{g\in G}\mathrm{trace}(\rho_W(g))=\mathrm{trace}\Big(\frac{1}{|G|}\sum_{g\in G}\rho_W(g)\Big)=\dim W^G.$$

because

$$\frac{1}{|G|}\sum_{g\in G}\rho_W(g)$$

is just the projection onto W^G (the Reynolds operator).

For any $g\in G$, $\rho_V(g)$ can be diagonalized (since it has finite order). We may assume that

$$g\cdot x_i=\lambda_i x_i$$

for $i=1,\ldots,n$. Since $K[V]_d$ is spanned by all monomials of degree d, we get the following formula of the trace of the action of g on $K[V]_d$:

$$\mathrm{trace}(\rho_{K[V]_d(g)})=\sum_{\substack{a_1,\ldots,a_n\geq 0\\ a_1+\cdots+a_n=d}}\lambda_1^{a_1}\cdots\lambda_n^{a_n}.$$

We multiply this with t^d and sum it over all d to get

$$\sum_{d\geq 0}\mathrm{trace}(\rho_{K[V]_d(g)})t^d = \sum_{a_1,a_2,\dots,a_n\geq 0}\lambda_1^{a_1}\cdots\lambda_n^{a_n}t^{a_1+\cdots+a_n} =$$

$$= \frac{1}{(1-\lambda_1 t)\cdots(1-\lambda_n t)} = \frac{1}{\det(I-t\rho_V(g))}.$$

Now finally

$$H(K[V]^G,t) = \sum_{d\geq 0}(\dim K[V]^G_d)t^d = \sum_{d\geq 0}\frac{1}{|G|}\sum_{g\in G}\mathrm{trace}(\rho_{K[V]_d}(g))t^d =$$

$$= \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(I-t\rho_V(g))}.$$

□

Example 4.4. Consider the action of the alternating group A_4 on $V := K^4$ by permuting the coordinates. The expression $\det(I-t\rho_V(g))$ only depends on the conjugacy class of g. For $e\in A_4$ we get

$$\det(I-t\rho_V(e)) = \det(I-tI) = \det((1-t)I) = (1-t)^4.$$

If g is equal to (1 2)(3 4) or conjugate to it, then

$$\det(I-t\rho_V(g)) = (1-t^2)^2.$$

If g is equal to (1 2 3) or conjugate to it, then

$$\det(I-t\rho_V(g)) = (1-t^3)(1-t).$$

There is only one element of A_4 conjugate to e, namely e itself. There are 3 elements of A_4 conjugate to (1 2)(3 4), and 8 elements of A_4 conjugate to (1 2 3). By Molien's formula we have

$$H(K[V]^G,t) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(I-t\rho_V(g))} = \frac{1}{(1-t)^4}+\frac{3}{(1-t^2)^2}+\frac{8}{(1-t^3)(1-t)} =$$

$$\frac{1-t^2+t^4}{(1-t)(1-t^2)^2(1-t^3)} = \frac{1+t^6}{(1-t)(1-t^2)(1-t^3)(1-t^4)}.$$

The elementary symmetric functions

$$\begin{aligned}
e_1 &= x_1+x_2+x_3+x_4\\
e_2 &= x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4\\
e_3 &= x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4\\
e_4 &= x_1x_2x_3x_4
\end{aligned}$$

form a homogeneous system of parameters. Now

$$H(K[e_1,e_2,e_3,e_4],t)=\frac{1}{(1-t)(1-t^2)(1-t^3)(1-t^4)}.$$

We see that

$$H(K[V]^G,t)=(1+t^6)H(K[e_1,e_2,e_3,e_4],t). \tag{8}$$

Since e_1,e_2,e_3,e_4 is a homogeneous system of parameters, and $K[V]^G$ is Cohen-Macaulay, we have that $K[V]^G$ is a free $K[e_1,e_2,e_3,e_4]$-module. From (8) it follows that $K[V]^G$ is a free module over $K[e_1,e_2,e_3,e_4]$ with generators 1 and h where h is some invariant of degree 6. In fact we can take

$$h=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4).$$

Suppose now that $G=K^\star$ is the multiplicative group and $\rho_V:K^\star\to V$ is a representation. The action of G on V is diagonalizable. For a diagonal action of $K^\star$, the Hilbert series counts the number of ivnariant monomials in each degree. The Hilbert series of the invariant ring does not really depend on the base field we are working over. For the field $K=\mathbb{C}$ we have the following formula for the Hilbert series of the invariant ring.

Theorem 4.5.

$$H(K[V]^G,t)=\frac{1}{2\pi i}\int_{S^1}\frac{1}{\det(I-t\rho_V(z))}\frac{dz}{z} \tag{9}$$

where $S^1\subset\mathbb{C}$ *is the unit circle* $\{z;|z|=1\}$.

Proof. The action of a torus is diagonalizable. We may assume that with respect to some basis of V, $\rho_V(z)$ has the diagonal matrix

$$\begin{pmatrix} z^{a_1} & & & \\ & z^{a_2} & & \\ & & \ddots & \\ & & & z^{a_n}\end{pmatrix}$$

The coefficient of t^d in the power series of

$$\frac{1}{(1-tx_1)\cdots(1-tx_n)} \tag{10}$$

is equal to the sum of all monomials in $x_1,x_2,\dots,x_n$ of degree d. Note that $z^{-1}\cdot x_i=z^{a_i}x_i$ for all i. We apply the action of $z\in K^\star$ to (10). Then the coefficient of t^d in the power series of

$$\frac{1}{(1-tz^{a_1}x_1)(1-tz^{a_2}x_2)\cdots(1-tz^{a_n}x_n)} \tag{11}$$

is equal to the sum of all $z^{-1} \cdot m$ where m is a monomial of degree d. The coefficient of $t^d z^0$ in (11) is equal to the sum over all invariant monomials of degree d. If we now put $x_1 = x_2 = \cdots = x_n = 1$ then we see that the coefficient of $t^d z^0$ in

$$\frac{1}{(1 - tz^{a_1}) \cdots (1 - tz^{a_n})} \tag{12}$$

is exactly the number of invariant monomials of degree d, which is $\dim K[V]^G_d$. In particular we see now that the coefficient of z^0 in (12) is exactly the Hilbert series of the invariant ring $H(K[V]^G, t)$. Note that power series of (12) in t is uniform convergent on $|z| = 1$, if $|t| < 1$.

Finally we note that if $f(z)$ is a Laurent polynomial in z, then

$$\frac{1}{2\pi i} \int_{S^1} f(z) \frac{dz}{z}$$

is equal to the coefficient of z^0 in $f(z)$. If we apply this to (12) then the theorem follows because the right-hand side of (9) is equal to

$$\frac{1}{2\pi i} \int_{S^1} \frac{1}{(1 - tz^{a_1})(1 - tz^{a_2}) \cdots (1 - tz^{a_n})} \frac{dz}{z}.$$

□

The following example illustrates how this theorem can be used to compute Hilbert series of invariant rings for the multiplicative group using the residue theorem for complex functions.

Example 4.6. Consider the action of $K^\star$ on K^2 by

$$\lambda \cdot (x_1, x_2) = (\lambda^{-1} x_1, \lambda^3 x_2).$$

We compute $H(K[V]^{K^\star}, t)$. By the theorem, we have

$$H(K[V]^{K^\star}, t) = \frac{1}{2\pi i} \int_{S^1} \frac{1}{(1 - z^{-1} t)(1 - z^3 t)} \frac{dz}{z}. \tag{13}$$

To compute the righthand side we use the Residue Theorem. We assume that $|t| < 1$. We look for poles inside the unit circle. The only poly is $z = t$. The residue at $z = t$ is

$$\lim_{z \to t} \frac{z - t}{(1 - z^{-1} t)(1 - z^3 t) z} = \lim_{z \to t} \frac{1}{1 - z^3 t} = \frac{1}{1 - t^4}.$$

The Residue Theorem says that (13) is equal to the sum of the residues inside the unit circle. We conclude that

$$H(K[V]^{K^\star}, t) = \frac{1}{1 - t^4}.$$

This is indeed true, since one easily checks that $K[V]^{K^\star}$ is the polynomial ring in the degree 4 monomial $x_1^3 x_2$.

Computing the Hilbert series of the invariant ring a priori can be used to compute generators of the invariant ring. We will discuss now how one can use homogeneous systems of parameters and Hilbert series to obtain generators of the invariant ring for a finite group G.

First we search for a homogeneous system of parameters. For this we observe that $p_1, \dots, p_r$ form a regular sequence if and only if $K[V]^G/(p_1, \dots, p_r)$ has dimension $n-r$. This is true if and only if $K[V]/(p_1, \dots, p_r)$ has dimension $n-r$. The latter statement can be checked using a Gröbner basis computation. Also note that if $p_1, \dots, p_n$ is a homogeneous system of parameters for $K[V]^G$, then the denominator of $H(K[V]^G, t)$ has to divide

$$(1-t^{d_1}) \cdots (1-t^{d_s})$$

(where $d_i = \deg(p_i)$). This gives us additional conditions for the degrees of $p_1, \dots, p_n$.

After we have found the homogeneous system of parameters, we search for secondary invariants, i.e., module generators of $K[V]^G$ over $P = K[p_1, \dots, p_n]$. We know that $K[V]^G$ is a free P-module, say

$$K[V]^G = Ph_1 \oplus \cdots \oplus Ph_l.$$

If $e_j = \deg(h_j)$ then we have

$$H(K[V]^G, t) = \frac{\sum_j t^{e_j}}{(1-t^{d_1}) \cdots (1-t^{d_n})}.$$

Since we know $H(K[V]^G, t)$ and $d_1, \dots, d_n$, we can compute $e_1, \dots, e_l$. So we know exacty in which degrees to look for secondary invariants.

4.3. **Degree bounds.** We give here a brief discussion on degree bounds for generators of invariant rings. For a more extensive discussions, see [10, 33, 34].

Suppose that V is a representation of a linearly reductive group G. We define the following constant

$$\beta(K[V]^G) = \min\{d \mid K[V]^G \text{ is generated in degree } \leq d\}.$$

We would like to have good upper bounds for $\beta(K[V]^G)$. For finite groups we have the following bound.

Theorem 4.7. *If the characteristic of K does not divide $|G|$, then*

$$\beta(K[V]^G) \leq |G|.$$

In characteristic 0 this was proven by Noether ([31]). If the characteristic does not divide the group order $|G|$, the so-called nonmodular case, then this inequality is still true. This was recently proven by Fleischmann (see [12]), and by Fogarty independently (cf. [13]).

Suppose that $G = T = (K^\star)^r$ is a torus. If $z = (z_1, \dots, z_r) \in T$, and $b = (b_1, \dots, b_r) \in \mathbb{Z}^r$, then z^b is an abbreviation for $z_1^{b_1} \cdots z_r^{b_r}$. If V is a representation of G then the action of G is diagonalizable. We assume that $\rho(z_1,\dots,z_r)$ is given by the matrix

$$\begin{pmatrix} z^{a_1} & & & \\ & z^{a_2} & & \\ & & \ddots & \\ & & & z^{a_n} \end{pmatrix}$$

for certain $a_1, a_2, \dots, a_n \in \mathbb{Z}^r$. We will assume that the action is faithfull, i.e., the vectors $a_1, \dots, a_n$ span $\mathbb{Z}^r$. The following degree bound was proven by Wehlau (see [40]):

Theorem 4.8.

$$\beta(K[V]^T) \leq \max\{n-r-1, 1\} r! \operatorname{volume}(\mathcal{C}_V)$$

where $\mathcal{C}_V$ is the convex hull of $a_1, a_2, \dots, a_n \in \mathbb{Z}^r \subseteq \mathbb{R}^r$.

A first general degree bound for invariants of connected reductive groups was found by Popov (see [33, 34]). This bound was radically sharpened by the author (cf. [8]). Let us introduce the following constant:

$$\gamma(K[V]^G) = \min\{d \mid K[V]^G \text{ is finite over } K[K[V]^G_{\leq d}]\} = \\ = \{d \mid \text{ invariants of degree} \leq d \text{ have } \mathcal{N} \text{ as zero set}\}. \tag{14}$$

Good bounds for $\gamma(K[V]^G)$ exists, see for example Popov (see [33, 34]) and Hiss (cf. [19]). The following bound was proven by the author:

Theorem 4.9.

$$\beta(K[V]^G) \leq \max\{2, \tfrac{3}{8} s \gamma^2(K[V]^G)\}$$

where $s = \dim K[V]^G$.

Example 4.10. For the group SL_2 acting on the binary forms of degree d, one can prove that

$$\gamma(K[V_d]^{\mathrm{SL}_2}) \leq 2d^3.$$

From Theorem 4.9, it follows that

$$\beta(K[V]^G) \leq \tfrac{3}{8}(d-2)(2d^3)^2 \leq \tfrac{3}{2}d^7.$$

This result is slightly worse than the bound $2d^6$ found by Jordan ([20, 21, 26]).

References

[1] William W. Adams and Phillippe Loustaunau, *An Introduction to Gröbner Bases*, Americal Mathematical Society, Graduate Studies in Mathematics **3**, Providence, RI, 1994.

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

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

[4] A. E. Brouwer and A. M. Cohen, *The Poincaré series of the polynomials invariant under* SU_2 *in its irreducible representations of degree* ≤ 17, Math. Centrum Amsterdam, ZW **134/79** (1979), 1–20.

[5] Winfried Bruns and Jürgen Herzog, *Cohen-Macaulay Rings*, Cambridge University Press, Cambridge, 1993.

[6] David Cox and John Little and Donal O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, New York, Berlin, Heidelberg, 1992.

[7] Harm Derksen, *Computation of invariants for reductive groups*, Adv. in Math. **141** (1999), 366–384.

[8] Harm Derksen, *Polynomial bounds for rings of invariants*, Proc. Amer. Math. Soc. **129** (2001), no. 4, 955–963.

[9] Harm Derksen and Gregor Kemper, *Computational Invariant Theory*, Invariant Theory and Algebraic Transformation Groups I, Encyclopaedia of Mathematical Sciences **130**, Springer-Verlag, Berlin, 2002.

[10] Harm Derksen and Hanspeter Kraft, *Constructive invariant theory*, Algèbre non commutative, groupes quantiques et invariants (Reims, 1995), 221–244, Sémin. Congr. **2**, Soc. Math. France, Paris, 1997.

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

[12] Peter Fleischmann, *The Noether bound in invariant theory of finite groups*, Adv. Math. **156** (2000), no. 1, 23–32.

[13] John Fogarty, *On Noether's bound for polynomial invariants of a finite group*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 5–7.

[14] Paul Gordan, *Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Funktion mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist*, J. Reine Angew. Math. **69** (1868), 323–354.

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

[16] David Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–370.

[17] David Hilbert,*Mathematische Probleme*, Archiv für Math. und Physik **1** (1901), 44–63. Also in: Gesammelte Abhandlungen Band III (1970), Springer Verlag, Berlin Heidelberg New York, 290–329.

[18] Melvin Hochster and Joel L. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Adv. in Math. **13** (1974), 115-175.

[19] Karin Hiss, *Constructive invariant theory for reductive algebraic groups*, Thesis Brandeis University, Waltham, 1996.

[20] Camille Jordan, *Mémoire sur les covariants des formes binaires*, J. de Math. **3** (2), 1876, 177–232.

[21] Camille Jordan, *Sur les covariants des formes binaires*, J. de Math. **3** (5), 1879, 345–378.

[22] Gregor Kemper, *Computational invariant theory*, The Curves Seminar at Queen's, Volume XII, in: Queen's Papers in Pure and Applied Math. **114** (1998), 5–26.

[23] Hanspeter Kraft, *Geometrische Methoden in der Invariantentheorie* Aspects of Mathematics, D1. Friedr. Vieweg & Sohn, Braunschweig, 1984.

[24] Hanspeter Kraft, Peter Slodowy and Tonny A. Springer, eds., *Algebraische Transformationsgruppen und Invariantentheorie*, DMV Seminar **13**, Birkhäuser Verlag, Basel, 1989.

[25] Hanspeter Kraft and Claudio Procesi, *Classical Invariant Theory, a Primer*, preprint, available at: `http://www.math.unibas.ch/~kraft/`

[26] Hanspeter Kraft and Jerzy Weyman, *Degree bounds for invariants and covariants of binary forms*, preprint, available at: `http://www.math.unibas.ch/~kraft/`

[27] Martin Kreuzer and Lorenzo Robbiano, *Computational Commutative Algebra 1*, Springer-Verlag, Berlin, 2000.

[28] Peter Littelmann and Claudio Procesi, *On the Poincaré series of the invariants of binary forms*, J. Algebra **133** (1990), no. 2, 490–499.

[29] D. Luna, *Slices étales*, Bull. Math. Soc. France, 1973, Memoire 33, 81–105.

[30] Masayoshi Nagata, *On the* 14^{th} *Problem of Hilbert*, Am. J. Math. **81** (1959), 766–772.

[31] Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1916), 89–92.

[32] Peter Olver, *Classical invariant theory*, London Mathematical Society Student Texts **44**, Cambridge University Press, Cambridge, 1999.

[33] Vladimir Popov, *Constructive invariant theory*, Young tableaux and Schur functors in algebra and geometry (Toruń, 1980), 303–334, Astrisque, 87–88, Soc. Math. France, Paris, 1981.

[34] Vladimir Popov, *The constructive theory of invariants*, Izv. Akad. Nauk SSSR Ser. Mat. **45** (1981), no. 5, 1100–1120, 1199.

[35] Vladimir L. Popov and Ernest B. Vinberg, *Invariant Theory*, in: N. N. Parshin, I. R. Shafarevich, eds., *Algebraic Geometry IV*, Encyclopaedia of Mathematical Sciences **55**, Springer-Verlag, Berlin, Heidelberg, 1994.

[36] W. Smoke, *Dimension and multiplicity of graded algebras*, J. Algebra **21** (1972), 149–173.

[37] Tonny Springer, *On the invariant theory of* SU_2, Nederl. Akad. Wetensch. Indag. Math. **42** (1980), no. 3, 339–345.

[38] Bernd Sturmfels, *Algorithms in invariant theory*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1993.

[39] Wolmer V. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*, Algorithms and Computation in Mathematics **2**, Springer-Verlag, Berlin, Heidelberg, New York, 1998.

[40] David L. Wehlau, *Constructive invariant theory for tori*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 1055–1066.