14

Hilbert Theory

When the algebraists of the 19th century were studying invariants, one of their main concerns was to find a finite set of invariants from which all the others could be expressed as polynomials. In particular they needed to prove that algebras of invariants are finitely generated. In modern geometric terms this result is needed to construct an algebraic variety whose coordinate ring is the ring of invariants which should parameterize in some sense the orbits of the group. Finiteness of the invariants was first proved by Gordan for binary forms by a complicated induction, and then for invariants of forms in any number of variables by Hilbert, who formulated the proofs in a rather abstract way, founding modern commutative algebra. The proof of Hilbert extends immediately to linearly reductive groups. Hilbert asked, in the 14th problem of his famous list, whether this (or rather a more general statement) is always true. It was only in the 1970s that Nagata produced a counterexample. At the same time interest in invariant theory had resurged and the finiteness theorem was also proved for reductive groups, which in characteristic 0 coincide with linearly reductive groups, but not in positive characteristic.

In this chapter we want to give a rather brief introduction to these ideas. We treat in detail some elementary topics and give some ideas of other more advanced topics.

The subject now goes under the name *Geometric Invariant Theory*. It is now a rather rich and deep topic and there are systematic treatments available at least for parts of it.

1 The Finiteness Theorem

1.1 Finite Generation

As already mentioned, one of the themes of 19th century invariant theory was to show that algebras of invariants are finitely generated. Hilbert proved that this is a consequence of the linear reductivity of the group. The main formal ingredient for such a group is *Reynold's operator*, which we discussed in Chapter 6, §2.4. Since

G is linearly reductive, if M is a rational representation we have a canonical G-equivariant map $r_M : M \to M^G$. If $f : M \to N$ is a G-equivariant map of rational representations, we have the commutative diagram:

$$\begin{array}{ccc} M & \xrightarrow{r_M} & M^G \\ {\scriptstyle f}\downarrow & & {\scriptstyle f}\downarrow \\ N & \xrightarrow{r_N} & N^G \end{array}.$$

In particular if G acts rationally as automorphisms of an algebra R and $a \in R^G$ we have:

(Reynold's identity) $$r_R(ab) = ar_R(b), \quad \forall a \in R^G, \quad \forall b \in R.$$

Theorem. *Let G be a linearly reductive group acting on a finite-dimensional vector space V. Then the algebra of invariants is finitely generated.*

Proof. Denote by R the algebra of polynomials and by $S := R^G$ the invariants. Consider the space S^+ of invariant polynomials without constant term and form the ideal RS^+ of R. By the Hilbert basis theorem, this is finitely generated and $RS^+ = \sum_{i=1}^k Ru_i$, $u_i \in S^+$. We may assume that the u_i are homogeneous. Given $u \in S^+$ we thus have $u = \sum_{i=1}^k x_i u_i$, $x_i \in R$. If we apply now Reynold's identity, we obtain $u = \sum_{i=1}^k r_R(x_i)u_i$. In other words the ideal generated by the elements u_i in S is S^+. Now let $T := F[u_1, \ldots, u_k]$. We want to show that $T = S$. We proceed by induction. Assume we know that $T_i = S_i$, $i < N$. We want to prove that $T_N = S_N$. Pick $u \in S_N$ and write it as $u = \sum_{i=1}^k v_i u_i$, $v_i \in S$, comparing the degrees we may assume that $\deg v_i + \deg u_i = N$. In particular $\deg v_i < N$, so by induction $v_i \in T$ and the claim follows. □

2 Hilbert's 14th Problem

2.1 Hilbert's 14th Problem

The 14th problem of Hilbert's famous list of 23 problems, presented in the International Congress of Mathematicians in Paris 1900, asks whether the ring of invariants for any group action is finitely generated. In fact Hilbert formulates a more general question: given a finitely generated domain $F[a_1, a_2, \ldots, a_k]$ with quotient field G and an intermediate subfield $F \subset H \subset G$, is the algebra $F[a_1, a_2, \ldots, a_k] \cap H$ finitely generated over F?

In fact even the first question has a negative answer, as shown by Nagata. The groups for which one can find counterexamples are in fact rather special, being isomorphic to the additive group of a finite-dimensional vector space $\mathbb{C}^m$. At the moment the best result is due to Mukai who gives an example of infinite generation for $m = 3$. For $m = 1$ an old result of Weizenbock shows that instead we have finite generation, while for $m = 2$ the answer is unknown.

Let us quickly explain Weizenbock's result.

The additive group $\mathbb{C}$ is identified with the subgroup U^+ of $SL(2, \mathbb{C})$ of matrices $\begin{vmatrix} 1 & t \\ 0 & 1 \end{vmatrix}$. From Chapter 7, §1.5 and §3.4 it follows that, in every rational representation $\rho : \mathbb{C} \to GL(n, \mathbb{C})$, the matrices induced by $\mathbb{C}$ are unipotent and there is a nilpotent matrix N such that $\rho(t) = e^{tN}$.

Now N is a direct sum of Jordan blocks of sizes $n_1, \ldots, n_k$, but then the direct sum of the irreducible representations of $SL(2, \mathbb{C})$ of dimensions $n_1, n_2, \ldots, n_k$ restricted to U^+ give the representation V from which we started. At this point one has to verify that the invariants under U^+ of V coincide with the invariants of $SL(2, \mathbb{C})$ on $V \oplus \mathbb{C}^2$. This argument is essentially what we will develop in the next chapter when we discuss covariants, and so we leave it to the reader.

3 Quotient Varieties

We want to discuss quotients in the simplest sense for affine and projective varieties. For a more systematic treatment see [MF], [DL].

From the results of Chapter 7 we can use the fact that, given an algebraic group G acting on a variety X, each orbit Gx is open in its closure $\overline{Gx}$, which is then a union of orbits. All the orbits in $\overline{Gx}$ different from Gx are then necessarily of dimension strictly less than the dimension of Gx. In particular we will use systematically the fact that an orbit of minimal dimension is necessarily closed.

First, let us extend Theorem 1.1. We assume that we are still working over the complex numbers.

Theorem 1. *(1) If a linearly reductive group G acts on an affine variety V, the ring of invariants $\mathbb{C}[V]^G$ is finitely generated.*

(2) If $W \subset V$ is a G-stable subvariety and $\mathbb{C}[W] = \mathbb{C}[V]/I$, the induced map of coordinate rings $\mathbb{C}[V]^G \to \mathbb{C}[W]^G$ is surjective.

Proof. From the general theory of semisimple representations (Chapter 6), if a linearly reductive group G acts on a space M and N is stable, then $M = N \oplus P$ decomposes as direct sum of subrepresentations. $M^G = N^G \oplus P^G$, and so the projection $M^G \to (M/N)^G = P^G$ is surjective. In particular this proves (2).

Now from Chapter 7, Theorem 1.3, given an action of an affine group G on an affine variety V, there exists a linear representation U of G and a G equivariant embedding of V in U. Therefore we have a surjective mapping $\mathbb{C}[U]^G \to \mathbb{C}[V]^G$. From 2.1 $\mathbb{C}[U]^G$ is finitely generated, hence so is $\mathbb{C}[V]^G$. □

We can now give a basic definition.

Definition. Given an action of an affine group G on an affine variety V the ring $\mathbb{C}[V]^G$ is the coordinate ring of an affine variety denoted $V//G$ and called the *categorical quotient* of V by G.

Of course the fact that $\mathbb{C}[V]^G$ is the coordinate ring of an affine variety depends (from the general theory of affine varieties) on the fact that it is finitely generated.

The previous theorem implies furthermore that if W is a G-stable subvariety of V, we have an inclusion $W//G \subset V//G$ as a subvariety.

The natural inclusion $\mathbb{C}[V]^G \subset \mathbb{C}[V]$ determines a canonical *quotient map* $\pi : V \to V//G$.

Theorem 2. *(1) The mapping π is constant on G-orbits.*

(2) The mapping π is surjective.

(3) Given any point $q \in V//G$, the G-stable subvariety $\pi^{-1}(q)$ of V contains a unique closed G-orbit.

Proof. (1) is clear since the map is given by invariant functions.

(2) Let $q \in V//G$ be a point. It is given by a maximal ideal $m \subset \mathbb{C}[V]^G$. We have to prove that there is a maximal ideal $n \subset \mathbb{C}[V]$ with $m = n \cap \mathbb{C}[V]^G$. Since every ideal is contained in a maximal ideal, it suffices to show that the ideal $m\mathbb{C}[V]$ is a proper ideal, or equivalently that $m = m\mathbb{C}[V] \cap \mathbb{C}[V]^G$.

Then let $a = \sum_i s_i m_i \in \mathbb{C}[V]^G$ with $s_i \in \mathbb{C}[V]$, $m_i \in m$. Apply Reynold's identity $a = R(a) = \sum_i R(s_i)m_i$, and hence $a \in m$ as desired.

(3) Since $\pi^{-1}(q)$ is a G-stable subvariety it contains an orbit of minimal dimension which is then necessarily closed. To complete (3) it is thus sufficient to show that two distinct closed orbits A_1, A_2 map to two distinct points in $V//G$. For this observe that $A_1 \cup A_2$ is an algebraic variety (since the two orbits are closed) and $\mathbb{C}[A_1 \cup A_2] = \mathbb{C}[A_1] \oplus \mathbb{C}[A_2]$ since they are disjoint. Then $\mathbb{C}[A_1 \cup A_2]^G = \mathbb{C}[A_1]^G \oplus \mathbb{C}[A_2]^G = \mathbb{C} \oplus \mathbb{C}$ is the coordinate ring of 2 points which, from the preceding discussion, means exactly that these two orbits map to two distinct points. □

One expresses the meaning of the previous theorem by saying that $V//G$ *parameterizes the closed orbits* of the G-action on V.

Another way of expressing part of the previous theorem is to say that invariants separate closed orbits, that is, given two distinct closed orbits A_1, A_2, there is an invariant with value 1 on A_1 and 0 on A_2.

4 Hilbert–Mumford Criterion

4.1 Projective Quotients

One often wants to apply invariant theory to projective varieties. The setting will be this. We have a linear algebraic group G acting linearly on a vector space V and thus projectively on $P(V)$. Suppose that $W \subset P(V)$ is a projective variety which is stable under the action of G. We would like to define $W//G$ as projective variety. To do it let us first consider the homogeneous coordinate ring $\mathbb{C}[C(W)]$ of the cone of W. The invariant ring $\mathbb{C}[C(W)]^G$ is thus a graded ring. As we have already seen when computing explicit invariants, the generators of this ring can be taken to be homogeneous but not necessarily of the same degree. Thus in order to obtain a

projective variety the idea is to take a sufficiently large degree m and consider the space of functions in $\mathbb{C}[C(W)]^G$ which are homogeneous of degree m. Considering these functions as homogeneous coordinates, this space gives a map of W into a projective space. However this map is not defined for the points of W where all the invariants vanish.

It is therefore important to understand from the beginning which are the points in $C(W)$ or even in V where all invariants vanish; these points are called the *unstable points*. Of course in the affine picture these points are just the preimage under the quotient $V \to V//G$ of the image of 0. Therefore we have that:

Proposition 1. *A vector $v \in V$ is unstable, or all invariants without constant term vanish on it, if and only if 0 is in the closure of the orbit Gv.*

Proof. An invariant is constant on an orbit and its closure. Thus if 0 is in the closure of the orbit Gv, any homogeneous invariant of degree > 0 vanishes at v. Conversely, assume all such invariants vanish at v. Take in the closure of Gv an orbit C of minimal dimension which is then necessarily closed. If $C \neq 0$, we could find an invariant f with $f(0) = 0$ and $f(C) \neq 0$, which is a contradiction. □

One needs a simpler criterion to see that a vector is unstable, and this is furnished by the Hilbert–Mumford criterion.

Theorem. *A vector v is unstable if and only if there is a 1-parameter subgroup $\rho : \mathbb{C}^* \to G$ such that $\lim_{t\to 0} \rho(t)v = 0$.*

In other words 0 is also in the closure of the orbit that one has under a single 1-parameter subgroup.

Let us give an idea of the proof of Hilbert in the case of $GL(n, \mathbb{C})$.

The proof goes essentially in 3 steps.

Step 1. In the first step, using the fact that $0 \in \overline{Gv}$, one constructs an analytic curve $\lambda : D \to \overline{Gv}$ where $D = \{t \in \mathbb{C} \mid |t| < 1\}$ with $\lambda(0) = 0$, $\lambda(t) \in Gv$, $\forall t \neq 0$.

Step 2. Next, by eventually passing to a parameter s with $t = s^k$ one can lift this curve to G for the nonzero values of s, i.e., one finds an analytic map $\mu : D - \{0\} \to GL(n, \mathbb{C})$ with a pole at 0 so that $\mu(t)v = \lambda(t)$.

Step 3. Now consider the matrix $\mu(t)$ with entries $\mu_{i,j}(t)$ some Laurent series. We want to apply a method like the one leading to the elementary divisors to write the function $\mu(t)$ in the form $a(t)\rho(t)b(t)$, where $a(t), b(t)$ are convergent power series (without polar part) with values in $GL(n, \mathbb{C})$, while $\rho(t)$ is a diagonal matrix with entries t^{m_i} for some integers m_i. If we can achieve this, then we see that

$$0 = \lim_{t\to 0} \lambda(t) = \lim_{t\to 0} \rho(t)v = \lim_{t\to 0} \mu(t)v.$$

In more detail, to prove the first two steps we need the following:

Lemma. *(a) Let V be an irreducible variety and U a nonempty open set of V. If $p \in V$, there is an irreducible curve $C \subset V$ so that $p \in C$, $C \cap U \neq \emptyset$.*

(b) Let $\rho : W \to V$ be a dominant map of irreducible varieties and $p \in V$. There is a curve $B \subset W$ with $p \in \overline{\rho(B)}$.

Proof. (a) Let $n = \dim V$. If $n = 1$ there is nothing to prove. Since this is a *local statement,* we can assume $V \subset k^n$ affine. Let $X_1, \ldots X_k$ be the irreducible components of $V - U$ which are not points. Choose a point $p_i \in X_i$ for each i and $p_i \neq p$. Then choose a hyperplane H passing through p, which does not contain V and does not pass through any of the p_i. Then by a basic result (cf. [Ha], [Sh]) $H \cap V$ is a union of irreducible varieties V_i of dimension $n - 1$. By our choice, none of them is contained in $V - U$; otherwise it would contain one of the X_j. Take one V_i with $p \in V_i$. We have that $U' := V_i \cap U$ is a nonempty open set. We can thus continue and finish by induction.

(b) We know that the image of ρ contains a nonempty open set U, and by the previous part we can find a curve C in V meeting U and with $p \in C$. Consider $Z := \rho^{-1}(C)$. There is at least one irreducible component Z^0 of Z which maps to C in a nonconstant way. Take any point of Z^0 mapping to some $q \in C \cap U$ and consider $\rho^{-1}(q)$ and the set $T := Z^0 - \rho^{-1}(q)$, open in Z^0. By (a) there is an irreducible curve $B \subset Z^0$ with $q \in B$ and $B \cap T \neq \emptyset$. The map ρ, restricted to B, maps B to C, it is not constant, so it is dominant and satisfies the requirements. □

The next properties we need are specific to curves. We give them without proofs (cf. [Ha], [Sh], [Fu]):

Proposition 2. *Given a map $\rho : C \to B$ of irreducible curves, one can complete $C \subset \overline{C}$, $B \subset \overline{B}$ to two projective curves $\overline{C}, \overline{B}$ so that the map extends to these curves.*

The extended map $\overline{\rho}$ is now surjective, and thus given a point $p \in B$ there is a point $q \in C$ with $\overline{\rho}(q) = p$.

The final property of curves that we need is the *local analytic description.*

Proposition 3. *Given a curve C and a point $p \in C$ there is an analytic map f of a disk D to C such that $f(0) = p$ and f restricted to $D - \{0\}$ is an analytic isomorphism to an open set of C.*[141]

All these statements justify the first two steps of the proof of the H-M criterion.

The analytic coordinate can be replaced in positive characteristic by a formal power series argument which still can be used to prove the theorem.

The third step is an easy Gaussian elimination. We construct the two matrices $a(t), b(t)$ as products of elementary operations on rows and columns as follows. First, permuting rows and columns (i.e., multiplying on the right and left by permutation matrices) we may assume that the order of pole of $\mu_{1,1}(t)$ is the highest of

[141] Now open means in the usual complex topology and **not** in the Zariski topology.

all entries of the matrix. Next, for each $i = 2, \ldots, n$, $\mu_{i,1}(t)\mu_{1,1}(t)^{-1}$ is holomorphic, and subtracting from the i^{th} row the first multiplied by $\mu_{i,1}(t)\mu_{1,1}(t)^{-1}$, one can make 0 all the elements of the first column except the first, and similarly for the first row. Next write $\mu_{1,1}(t) = t^{n_1} f(t)$ with $f(t)$ holomorphic and $f(0) \neq 0$. To divide the first row by $f(t)$ is equivalent to multiplying by a diagonal matrix with holomorphic entries $f(t)^{-1}, 1, \ldots, 1$.

After this step $\mu(T)$ becomes a block matrix $\begin{vmatrix} t^{n_1} & 0 \\ 0 & \mu_1(t) \end{vmatrix}$, and now we continue by induction.

In order to extend the proof to any linearly reductive group one has to replace the last step of Gaussian elimination with a similar argument. This can be done using the Bruhat decomposition.

The Hilbert–Mumford criterion is quite effective in determining unstable points. For instance Hilbert showed:

Proposition (Hilbert). *Consider the action of $SL(2)$ on homogeneous polynomials of degree n (the binary forms). Such a homogeneous form defines n points (its roots), perhaps with some coincidences and multiplicities, on the projective line. A form is unstable if and only if one of its zeroes has multiplicity $> n/2$.*

Proof. Every 1-parameter group is conjugate to one contained in the standard diagonal torus, and up to conjugacy and reparametrization, we can assume it is the 1-parameter group $t \to \begin{vmatrix} t^{-1} & 0 \\ 0 & t \end{vmatrix}$. This group transforms a form $f(x, y) = \sum_{i=0}^{n} a_i x^{n-i} y^i$ into the form $\sum_{i=0}^{n} a_i (tx)^{n-i} (t^{-1}y)^i = \sum_{i=0}^{n} a_i t^{n-2i} x^{n-i} y^i$. Computing the limit, we have

$$\lim_{t \to 0} \sum_{i=0}^{n} a_i t^{n-2i} x^{n-i} y^i = 0$$

if and only if $a_i = 0$, $\forall n - 2i \leq 0$. This implies that x^{n-k} divides $f(x, y)$, where k is the minimum integer for which $n - 2k > 0$. Hence the point $(0, 1)$ is a root of multiplicity $n - k > n/2$. □

The reader can try to determine the unstable points in the various examples in which we constructed the invariants explicitly. For instance, for the conjugation action of m-tuples of matrices one has:

An m-tuple of matrices is unstable if and only if it can be simultaneously conjugated to an m-tuple of strictly upper triangular matrices. This happens if and only if the given matrices generate a nilpotent subalgebra of the algebra of matrices.

5 The Cohen–Macaulay Property

5.1 Hilbert Series

Let $A = F[a_1, \ldots, a_k]$ be a finitely generated algebra over a field F. A theorem which is now standard, but is part of the ideas developed by Hilbert, and known

as the *Hilbert basis theorem*, is that A is the quotient $A = F[x_1, \ldots, x_k]/J$ of a polynomial ring modulo a finitely generated ideal. In other words once an algebra is finitely generated, then it is also *finitely presented* by generators and relations.

Suppose now that A (as usual with algebras of invariants) is also a graded algebra, $A = \bigoplus_{i=0}^{\infty} A_i$. We assume that $A_0 = F$ and the elements a_i are homogeneous of some degrees $h_i > 0$. In this case we also have that A_i is a finite-dimensional vector space, so if we denote by $d_i := \dim_F A_i$ we have $d_i < \infty$ and we can form the *Hilbert series*:

$$H_A(t) := \sum_{i=0}^{\infty} d_i t^i. \tag{5.1.1}$$

The same construction can be performed when we consider a finitely generated graded module $M = \sum_{i=1}^{k} Au_i$ over a finitely generated graded algebra $A = F[a_1, \ldots, a_k]$.

Let us then make the basic remark. Let $f : M \to N$ be a graded morphism of graded modules. Let i be the degree of f, this means that $f(M_k) \subset N_{k+i}$ for all k. We have that $\operatorname{Ker} f$ and $\operatorname{Im} f$ are graded submodules of M, N respectively. We have for all k an exact sequence:

$$0 \to (\operatorname{Ker} f)_k \to M_k \xrightarrow{f} N_{k+i} \to (\operatorname{Coker} f)_{k+i} \to 0$$

from which

$$\dim((\operatorname{Ker} f)_k) - \dim(M_k) + \dim(N_{k+i}) - \dim((\operatorname{Coker} f)_{k+i}) = 0.$$

We multiply by t^{k+i} and sum to get

$$H_{\operatorname{Coker} f}(t) - t^i H_{\ker f}(t) = H_N(t) - t^i H_M(t). \tag{5.1.2}$$

Theorem. *Let M be a finitely generated graded module over the graded polynomial ring $F[x_1, \ldots, x_m]$ where $\deg x_i = h_i$. Then, for some integeres u, v*

$$H_M(t) = \frac{p(t)}{\prod_{i=1}^{m}(1 - t^{h_i})}, \quad p(t) = \sum_{i=-u}^{v} a_i t^i, \quad a_i \in \mathbb{Z}. \tag{5.1.3}$$

If $M_i = 0$ when $i < 0$, then $p(t)$ is a polynomial in t ($u = 0$).

Proof. By induction on m, if $m = 0$, then M is a finite-dimensional graded vector space and the statements are clear. Assume $m > 0$ and consider the map $f : M \xrightarrow{x_m} M$ given by multiplication by x_m. It is a graded morphism of degree h_m, and by construction, $\operatorname{Ker} f$ and $\operatorname{Coker} f$ are both finitely generated graded modules annihilated by x_m. In other words they can be viewed as $F[x_1, \ldots, x_{m-1}]$ modules, and by induction

$$H_{\ker f}(t) = \frac{p_1(t)}{\prod_{i=1}^{m-1}(1 - t^{h_i})}, \quad H_{\operatorname{Coker} f}(t) = \frac{p_2(t)}{\prod_{i=1}^{m-1}(1 - t^{h_i})}.$$

From 5.1.2,

$$t^{h_m} H_{\ker f}(t) - H_{\operatorname{Coker} f}(t) = (1 - t^{h_m}) H_M(t) \implies H_M(t) = \frac{t^{h_m} p_1(t) - p_2(t)}{\prod_{i=1}^{m}(1 - t^{h_i})}. \quad \square$$

Notice in particular that:

Proposition. *For the graded polynomial ring* $A := F[x_1, \ldots, x_m]$ *where* $\deg x_i = h_i$, *we have*

$$H_A(t) = \frac{1}{\prod_{i=1}^{m}(1 - t^{h_i})}. \tag{5.1.4}$$

Proof. This follows from the previous proof, or from the fact that if we have two graded vector spaces $M = \oplus M_i$, $N = \oplus N_j$ and set $(M \otimes N)_k := \bigoplus_{i+j=k} M_i \otimes N_j$, then we have

$$H_{M\otimes N}(t) = H_M(t)H_N(t), \quad F[x_1, \ldots, x_m] = F[x_1] \otimes F[x_2] \otimes \cdots \otimes F[x_m],$$

$$H_{F[x]}(t) = \frac{1}{1 - t^{\deg x}}.$$

5.2 Cohen–Macaulay Property

There are two special conditions on graded algebras which are useful and which appear for algebras of invariants: the *Cohen–Macaulay* and the *Gorenstein* property.

These conditions are not exclusive to graded algebras but for simplicity we formulate them in this important case (cf. [E]).

Definition 1. A finitely generated graded algebra $A = F[a_1, \ldots, a_m]$ is said to be Cohen–Macaulay if there exist homogeneous elements $u_1, \ldots, u_k \in A$ (a regular system of parameters) with the two properties:

(i) The elements u_i are algebraically independent, i.e., the algebra they generate is a polynomial ring in the u_i.
(ii) The ring A is a finite free module over $B := F[u_1, \ldots, u_k]$.

Condition (ii) implies the existence of homogeneous elements $p_1, \ldots, p_r$ such that

$$A = \bigoplus_{i=1}^{r} F[u_1, \ldots, u_k]p_i. \tag{5.2.1}$$

If h_i, $i = 1, \ldots, k$, is the degree of u_i and ℓ_j, $j = 1, \ldots, r$, the degree of p_j, we deduce

$$H_A(t) = \frac{\sum_{j=1}^{r} t^{\ell_j}}{\prod_{i=1}^{k}(1 - t^{h_i})}. \tag{5.2.2}$$

When A is C-M, a regular system of parameters is clearly not unique. Nevertheless one can prove (cf. [E]) that if $v_1, \ldots, v_s \in A$ and $A/(v_1, \ldots, v_s)$ is finite dimensional, then $s \geq k$. If furthermore $s = k$, then $v_1, \ldots, v_s$ is a regular system of parameters.

The Gorenstein property is subtler and it is best to explain it first for a finite-dimensional graded algebra. Assume $A = F[a_1, \ldots, a_k] = \bigoplus_{i=0}^{N} A_i$ with $A_N \neq 0$, such that the highest degree component is finite dimensional. For the Gorenstein property we need two conditions:

(i) $\dim A_N = 1$.

Let $A_N = Fu_N$. Define $t : A \to F$ by $t(a) = \begin{cases} 0 & \text{if } a \in A_i, i < N; \\ t(fu_N) = f, & f \in F. \end{cases}$

(ii) The symmetric bilinear form $t(ab)$ on A is nondegenerate.

Definition 2. A finitely generated graded algebra $A = F[a_1, \ldots, a_m]$ is said to be Gorenstein if there exists a regular system of parameters $u_1, \ldots, u_k \in A$ such that the finite-dimensional algebra $D := F[a_1, \ldots, a_m]/(u_1, \ldots, u_k)$ is Gorenstein.

One can prove again that if the property is verified for one single system of parameters it is verified by all systems.

For a finite-dimensional algebra A with maximum degree N, the Gorenstein property implies that $t(ab)$ establishes an isomorphism between A_i and A^*_{N-i} for all i. In particular we have a consequence for the Hilbert series of a Gorenstein algebra, it is of the form 5.2.2, with the further restriction that the numerator $p(t)$ is a polynomial with nonnegative integer coefficients, constant term 1 and with the symmetry $p(t) = t^N p(t^{-1})$ where $N = \deg p(t)$.

An important theorem of Hochster and Roberts [HR] (see also [B-H] for a short proof due to Knop) is:

Theorem. *If G is a linearly reductive group and M a rational representation, then the ring of invariants of G acting on M is Cohen–Macaulay. If furthermore G is contained in the special linear group, the ring of invariants is even Gorenstein.*

It is in fact quite interesting to see explicitly these properties for the rings of invariants that we studied in Chapter 11. A lot of interesting combinatorics is associated to this property (cf. [Gar], [Stan]).