INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

SMR.761/4

Workshop on Commutative Algebra
and its Relation to
Combinatorics and Computer Algebra

(16 - 27 May 1994)

Algebraic and Combinatorial Reciprocity Laws

W. Bruns
FB Naturwissenschaften Mathematik
Universität Osnabrück
Standort Vechta
49377 Vechta
Germany

These are preliminary lecture notes, intended only for distribution to participants

ALGEBRAIC AND COMBINATORIAL RECIPROCITY LAWS

Lecture Notes for a Workshop on Commutative Algebra
ICTP, Trieste, Italy, May 1994

WINFRIED BRUNS

FB Naturwissenschaften Mathematik
Universität Osnabrück
Standort Vechta
49377 Vechta, Germany

Preface

The theme of these notes is the duality between a Cohen–Macaulay graded algebra and its canonical module. This duality manifests itself in numerous homological and combinatorial theorems.

The first three section represent what in my opinion should be the basic knowledge of someone interested in the combinatorial aspects of commutative algebra. I have tried to indicate all the major ideas on which the theory is built.

In Section 4 the usual direction from commutative algebra to combinatorics is reversed: a combinatorial identity leads to the identification of the canonical module of the ring of invariants of a finite group.

In Section 5 we discuss the theory of normal semigroup rings. It emerges from an intriguing interplay of combinatorial, topological, and algebraic aspects. Once we have determined the canonical module, we can harvest plenty of combinatorial theorems about lattice points in rational polytopes, among them Ehrhart's remarkable reciprocity law.

Section 6 is much more elementary. We prove a reciprocity law for the number of walks in a directed graph from the formula that relates the Hilbert series of a module M, that of the ring, and the Poincaré series of M defined by a graded free resolution.

The homological and combinatorial theory of commutative rings is the topic of the book [1], *Cohen–Macaulay rings* by Jürgen Herzog and me (Cambridge University Press, 1993). There the reader will find a fully expanded version of the material of Sections 1–5, and, among other things, a chapter on Stanley–Reisner rings.

There are almost no references to the original sources in the text. I have however added a small bibliography of papers and books that deal with commutative algebra and combinatorics.

1 Graded K-algebras

Let K be a field, and R a finitely generated, positively graded K-algebra, i.e. R is the direct sum

$$R = \bigoplus_{i=0}^{\infty} R_i$$

of K-vector spaces, and the multiplication on R satisfies the rule $R_i R_j \subset R_{i+j}$; furthermore $R = K[x_1, \ldots, x_n]$ for suitable elements $x_1, \ldots, x_n \in \bigcup_{i>0} R_i$. In particular $R_0 = K$, and R is a Noetherian ring. In order to have a compact terminology we simply say that *R is a graded K-algebra.*

The elements of the *i-th graded component* R_i are *homogeneous of degree i* or *i-forms*, and similar conventions apply to the graded R-modules below. By $\mathfrak{m}$ we always denote the *graded (*or *irrelevant) maximal ideal*:

$$\mathfrak{m} = \bigoplus_{i=1}^{\infty} R_i.$$

A typical example of a graded K-algebra is a polynomial ring $S = K[X_1, \ldots, X_n]$: in its *standard grading* a polynomial f is homogeneous if all the monomials occuring in f have the same (total) degree, and a monomial $X_1^{a_1} \cdots X_n^{a_n}$ has degree $a_1 + \cdots a_n$. As a K-algebra, S is generated by the degree 1 elements X_i. More generally, if a graded K-algebra is generated by elements of degree 1, then we call it a *homogeneous* K-algebra. (Some authors prefer the name *standard* K-algebra.)

However, we are free to assign arbitrary positive degrees a_i to the indeterminates of S: then the degree of $X_1^{e_1} \cdots X_n^{e_n}$ is $a_1 e_1 + \cdots a_n e_n$, and the i-forms are the K-linear combinations of the monomials of degree i.

Suppose that the graded K-algebra R is generated by homogeneous elements $x_1, \ldots, x_n$ of degrees $a_1, \ldots, a_n$; then the assignment $\pi : X_i \mapsto x_i$ makes R a residue class K-algebra of S, and the natural epimorphism is compatible with the gradings: the image of an i-form is an i-form, and $R_i = S_i/(S_i \cap \operatorname{Ker} \pi)$.

In general, if the ideal $\mathfrak{a}$ is generated by homogeneous elements, then the residue class ring $R/\mathfrak{a}$ is a graded K-algebra with $(R/\mathfrak{a})_i = R/(R_i \cap \mathfrak{a})$.

A graded R-module is an R-module that as a K-vector space is a direct sum

$$M = \bigoplus_{i \in \mathbf{Z}} M_i.$$

satisfying the rule $R_i M_j \subset M_{i+j}$. (It would be more precise to say that a graded R-module is an R-module together with such a decomposition.) Note that the elements

of M may have negative degrees. If M is a Noetherian R-module, then $M_i = 0$ for $i \ll 0$; if it is Artinian, then $M_i = 0$ for $i \gg 0$; in both cases one has $\dim_K M_i < \infty$ for all i. Every element x of M has a unique representation as a sum $x = \sum_i x_i$ of elements $x_i \in M_i$, which are called the *homogeneous components* of x.

One can change the grading of M by a *shift* $s \in \mathbb{Z}$: one sets $M(s)_i = M_{i+s}$. In other words, the degree j homogeneous elements of M have degree $j - s$ in $M(s)$.

A submodule U of M is *graded* if $U = \bigoplus_i U \cap M_i$. If U is a graded submodule, then M/U is a graded module with homogeneous components $M_i/(U \cap M_i)$. Obviously a submodule U is graded if and only if contains the homogeneous components of each of its elements. The annihilator of a graded module is a graded ideal.

A homomorphism $\varphi_i\colon M \to N$ of graded R-modules is called *homogeneous* if $\varphi(M_i) \subset N_i$ for all $i \in \mathbb{Z}$, and M and N are *isomorphic* as graded modules if and only if there exists a homogeneous isomorphism $\varphi_i\colon M \to N$. Though all the modules $M(s)$ are isomorphic as plain R-modules, they are in general non-isomorphic as graded modules. The kernel, image, and cokernel of a homogeneous homomorphism are graded modules in a natural way. The graded modules form a category whose morphisms are the homogeneous homomorphisms.

It is absolutely essential that the homomorphisms in complex of graded modules are homogeneous. The (co)homology modules of such a (co)chain complex are graded so that one can use graded homological algebra.

Dimension and depth. A guiding principle in the theory of graded rings is that all the local properties and invariants of a graded module should be determined by the localizations with respect to graded prime ideals.

The basic lemma on which this principle rests is the following.

Lemma 1.1. *Let R be a graded K-algebra.*
(a) *For every prime ideal $\mathfrak{p}$ the ideal $\mathfrak{p}^*$ that is generated by the homogeneous elements in $\mathfrak{p}$ is a prime ideal.*
(b) *Let M be a graded R-module.*
(i) *If $\mathfrak{p} \in \operatorname{Supp} M$, then $\mathfrak{p}^* \in \operatorname{Supp} M$.*
(ii) *If $\mathfrak{p} \in \operatorname{Ass} M$, then $\mathfrak{p}$ is graded; furthermore $\mathfrak{p}$ is the annihilator of a homogeneous element.*

Proposition 1.2. *Let R be a graded K-algebra. Then* $\dim R = \dim R_{\mathfrak{m}}$.

Let $\mathfrak{p}$ be a minimal prime ideal of R. Then, by virtue of the lemma, $\mathfrak{p}$ is graded, and thus $\mathfrak{p} \subset \mathfrak{m}$. From the dimension theory of affine algebras it follows that $\dim R/\mathfrak{p} = \dim R_{\mathfrak{m}}/\mathfrak{p}R_{\mathfrak{m}}$. This implies the proposition.

There is no (standard) global notion of depth. Therefore we set

$$\operatorname{depth} M = \operatorname{depth} M_{\mathfrak{m}}$$

for a finite graded R-module (we use *finite* as a short form of 'finitely generated'). Recall that the depth of a finite module over a local ring is the length of a maximal M-sequence (also called a regular sequence on M) contained in $\mathfrak{m}$. That this definition of depth is justified, will be seen at several occasions below.

For the construction of sequences of elements with good properties the next lemma is basic.

Lemma 1.3. *Let R be a graded K-algebra and I an ideal generated by elements of positive degree. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals such that $I \not\subset \mathfrak{p}_i$ for $i = 1, \ldots, n$.*
(a) *Then there exists a homogeneous element $x \in I$, $x \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$.*
(b) *If K is infinite and I is generated by m-forms, then x can be chosen as an m-form.*

We indicate the proof of (b) which implies (a) if K is infinite (we can always replace I by an ideal with the same radical). It is very short: the K-vector space I_m is not the union of the finitely many proper subspaces $I_m \cap \mathfrak{p}_i$.

In the next proposition grade(I, M) denotes the length of a maximal M-sequence contained in the ideal I. Suppose that M and I are graded. Then a sequence $\boldsymbol{y}$ of homogeneous elements is a (maximal) M-sequence in I if and only if $\boldsymbol{y}$ is a (maximal) $M_{\mathfrak{m}}$-sequence in $I_{\mathfrak{m}}$. This follows from the fact that the associated prime ideals of a graded module are graded, and therefore contained in $\mathfrak{m}$. That there exist homogeneous M-sequences of length grade(I, M) is stated in the next proposition.

Proposition 1.4. (a) *Let R be a graded K-algebra, and let I be an ideal in R generated by homogeneous elements of positive degree. Set $h = \operatorname{height} I$ and $g = \operatorname{grade}(I, M)$ where M is a finite R-module. Then there exist sequences $\boldsymbol{x} = x_1, \ldots, x_h$ and $\boldsymbol{y} = y_1, \ldots, y_g$ of homogeneous elements of I such that $\operatorname{height}(x_1, \ldots, x_i) = i$ for $i = 1, \ldots, h$ and $\boldsymbol{y}$ is an M-sequence.*
(b) *If K is infinite and I is generated by m-forms, then the x_i and y_i can be chosen as m-forms.*

It is enough to find x_1 and y_1 because we may use induction on n after having replaced all objects by their reductions modulo x_1 or y_1. But the choice of x_1 or y_1 only requires the avoidance of finitely many prime ideals none of which contains I.

Graded Noether normalization. The existence of Noether normalizations of affine algebras is a fact of fundamental importance. If R is a graded K-algebra, then the Noether normalization can be chosen to be graded. The construction of a graded Noether normalization is equivalent to finding a homogeneous system of parameters.

Definition 1.5. A sequence of homogeneous elements $x_1, \ldots, x_n$ is called a *homogeneous system of parameters* if $n = \dim R$ and $\mathfrak{m} = \operatorname{Rad}(x_1, \ldots, x_n)$.

Note that a sequence $x_1, \ldots, x_n$ of homogeneous elements is a homogeneous system of parameters for R if and only if $x_1, \ldots, x_n$ represents a system of parameters for the localization $R_{\mathfrak{m}}$.

Theorem 1.6. *Let K be a field and R a graded K-algebra. Set $d = \dim R$.*
(a) *The following are equivalent for homogeneous elements $x_1, \ldots, x_d$:*
(i) *$x_1, \ldots, x_d$ is a homogeneous system of parameters;*
(ii) *R is an integral extension of $K[x_1, \ldots, x_d]$;*
(iii) *R is a finite $K[x_1, \ldots, x_d]$-module.*

(b) *There exist homogeneous elements $x_1, \dots, x_d$ satisfying one, and therefore all, of the conditions in* (a). *Moreover, such elements are algebraically independent over K.*
(c) *If R is a homogeneous K-algebra and K is infinite, then such $x_1, \dots, x_d$ can be chosen to be of degree* 1.

Part (a) is essentially a statement about affine algebras. The rest follows from 1.4.

Graded free resolutions. Let M be a graded R-module, generated by homogeneous elements x_i, $i \in I$. Then the direct sum $F_0 = \bigoplus_{i \in I} R(-\deg x_i)$ is a free graded R-module admitting a surjective homogeneous homomorphism $\varphi_0 \colon F_0 \to M$: the map which for each i maps a homogeneous basis element e_i to x_i extends to a unique R-linear map $\varphi_0 \colon F_0 \to M$. It is evidently surjective and homogeneous. The kernel U_0 of φ_0 is again a graded module to which we can apply the same construction, obtaining a surjective homogeneous homomorphism $\varphi_1 \colon F_1 \to U_0$, and an infinite iteration of this process leads to a *graded free resolution*

$$F_\bullet \colon \cdots \longrightarrow F_m \xrightarrow{\varphi_m} F_{m-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0$$

of M. (In the language of homological algebra, the category of graded modules has enough projective modules.)

Suppose that M is finite, and choose a minimal homogeneous system $x_1, \dots, x_m$ of generators; 'minimal' just means that no proper subset generates M. The kernel of the map φ_0 defined by $x_1, \dots, x_m$ is again a finitely generated graded module with a minimal homogeneous system $y_1, \dots, y_p$ of generators. Therefore we have a presentation

$$F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

in which all the entries of a matrix representing φ_1 are in $\mathfrak{m}$: they are homogeneous and cannot be non-zero elements of K; otherwise one of the x_i would be a linear combination of the others. This implies that $M/\mathfrak{m}M \cong F_0/\mathfrak{m}F_0$. In particular the number m and the degrees of the elements $x_1, \dots, x_m$ are uniquely determined (up to a permutation): exactly $\dim_K(M/\mathfrak{m}M)_i$ among the x_j have degree i.

Theorem 1.7. *A finitely generated graded R-module M has a minimal graded free resolution*

$$F_\bullet \colon \cdots \longrightarrow \bigoplus_j R(-j)^{\beta_{ij}} \longrightarrow \bigoplus_j R(-j)^{\beta_{i-1,j}} \longrightarrow \cdots \longrightarrow \bigoplus_j R(-j)^{\beta_{0j}};$$

it is uniquely determined up to an isomorphism of complexes of graded R-modules.

In the summands $\bigoplus_j R(-j)^{\beta_{ij}}$ we have collected all the summands $R(-j)$ of F_i, in other words, β_{ij} is the number of degree j elements in a minimal homogeneous system of generators of $\operatorname{Ker} \varphi_{i-1}$. It follows by induction on i that the modules $\operatorname{Ker} \varphi_{i-1}$ and the numbers β_{ij} are uniquely determined by M.

Definition 1.8. The module $\operatorname{Ker}\varphi_{i-1}$ is the *i-th graded syzygy module* of M. The numbers β_{ij} are called the *i-th graded Betti numbers* of M. The numbers $\beta_i = \sum_j \beta_{ij}$ are the *Betti numbers* of M.

The numerical information in a complex like $F_\bullet$ is represented by the generating function of the assignment $(i,j) \mapsto \beta_{ij}$,

$$P_{F_\bullet}(t,u) = \sum_{i,j} \beta_{ij} t^j u^i.$$

We call this power series in the variables t and u the *Poincaré biseries* of $F_\bullet$. If $F_\bullet$ is the minimal graded free resolution of M then we write $P_M(t,u)$ for $P_{F_\bullet}(t,u)$ and call it the Poincaré biseries of M.

The entries of the matrices representing the maps φ_i (with respect to the decompositions $F_i = \bigoplus_j R(-j)^{\beta_{ij}}$) are homogenous elements of $\mathfrak{m}$. Therefore $F_\bullet \otimes R_\mathfrak{m}$ is a minimal free resolution of $M_\mathfrak{m}$. This argument shows that a graded module behaves homologically like a module over a local ring.

The Auslander–Buchsbaum formula tells us that $\operatorname{proj\,dim} M_\mathfrak{m} + \operatorname{depth} M_\mathfrak{m} = \operatorname{depth} R_\mathfrak{m}$, if $\operatorname{proj\,dim} M_\mathfrak{m} < \infty$. Since $\operatorname{proj\,dim} M_\mathfrak{m} = \operatorname{proj\,dim} M$, we can write the Auslander–Buchsbaum formula as $\operatorname{proj\,dim} M + \operatorname{depth} M = \operatorname{depth} R = n$.

The fundamental theorem about free resolutions of graded modules is *Hilbert's syzygy theorem.*

Theorem 1.9. *Let $R = K[X_1, \ldots, X_n]$, and M a finite graded R-module. Then M has a finite free resolution*

$$0 \longrightarrow \bigoplus_j R(-j)^{\beta_{pj}} \longrightarrow \cdots \longrightarrow \bigoplus_j R(-j)^{\beta_{0j}} \longrightarrow M \longrightarrow 0$$

with $p = \operatorname{proj\,dim} M = \operatorname{proj\,dim} M_\mathfrak{m} \leq n$.

Below we will see that the combination of Noether normalization and Hilbert's syzygy theorem is a very powerfool tool.

Graded Cohen–Macaulay rings and modules. A Noetherian ring R is called Cohen–Macaulay if all its localizations $R_\mathfrak{p}$ are Cohen–Macaulay, i.e. they satisfy the condition $\dim R_\mathfrak{p} = \operatorname{depth} R_\mathfrak{p}$. If R is a graded K-algebra, then we need to test only a single localization.

Proposition 1.10. *Let R be a graded K-algebra, and suppose S is a graded Noether normalization of R. Then the following are equivalent:*
(a) *R is Cohen–Macaulay;*
(b) *$R_\mathfrak{m}$ is Cohen–Macaulay.*
(c) *R is a free S-module;*

Let $\boldsymbol{x}$ be the homogeneous system of parameters generating S. If $R_\mathfrak{m}$ is Cohen–Macaulay, then $\boldsymbol{y}$ is a $R_\mathfrak{m}$-sequence. By the arguments given above 1.4, $\boldsymbol{y}$ is an R-sequence, so that the Auslander–Buchsbaum formula implies $\operatorname{proj\,dim}_S R = 0$.

Now let $\mathfrak{p}$ be a prime ideal in R. If R is free over S, then $R_{S\cap\mathfrak{p}}$ is free over $S_{S\cap\mathfrak{p}}$. Therefore $S_{S\cap\mathfrak{p}}$ contains a regular $R_{S\cap\mathfrak{p}}$-sequence $\boldsymbol{y}$ of length $\dim S_{S\cap\mathfrak{p}} = \dim R_{\mathfrak{p}}$; $\boldsymbol{y}$ is also $R_{\mathfrak{p}}$-regular. It follows that $R_{\mathfrak{p}}$ is Cohen–Macaulay.

A finite module M over a Noetherian ring R is called a *Cohen–Macaulay module* if $\dim M_{\mathfrak{p}} = \operatorname{depth} M_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \in \operatorname{Supp} M$. The previous proposition holds similarly for Cohen–Macaulay modules if we replace R by $R/(\operatorname{Ann} M)$ in (c). A Cohen–Macaulay module M is *maximal* if $\dim M = \dim R$.

The grading of Hom *and* Ext. Let N be a graded R-module. In order to compute the modules $\operatorname{Ext}^i_R(M,N)$ we form the complex $\operatorname{Hom}_R(F_\bullet, N)$ where $F_\bullet$ is a graded free resolution as above. The module $\operatorname{Hom}_R(R(-j), N)$ is graded in a natural way: $\operatorname{Hom}_R(R(-j), N)$ is a free graded R-module with a base element of degree j, and therefore the direct sum of the K-vector spaces L_k spanned by all those $f \in \operatorname{Hom}_R(R(-j), N)$ for which $f(e) \in N_{k+j}$. Since Hom commutes with *finite* direct sums, we see that $\operatorname{Hom}_R(F_\bullet, N)$ is a complex of graded R-modules (with homogeneous maps!).

Proposition 1.11. *Let M and N be graded R-modules. Suppose that M is finite. Then $\operatorname{Ext}^i_R(M,N)$ is a graded R-module in a natural way.*

For an arbitrary graded R-module M, the module $\operatorname{Hom}_R(M,N)$ need not carry a grading. Therefore, in the category of graded R-modules, one replaces $\operatorname{Hom}_R(M,N)$ by the graded Hom functor

$$^*\operatorname{Hom}_R(M,N) = \bigoplus_{i\in\mathbb{Z}} {}^\circ\operatorname{Hom}(M(-i),N),$$

where $^\circ\operatorname{Hom}(M(-i),N)$ is the K-vector space of homogeneous R-linear maps $M \to N$. It is easily seen that $^*\operatorname{Hom}_R(M,N)$ is an R-submodule of $\operatorname{Hom}_R(M,N)$ in a natural way.

The introduction of a graded tensor product is unnecessary: the tensor product of graded modules M and N is always graded with $(M \otimes_R N)_k = \sum_{i+j=k} M_i \otimes_K N_j$. Therefore the modules $\operatorname{Tor}^R_i(M,N)$ are also graded.

Graded injective resolutions. Since a graded R-modules has a graded free resolution, it is projective in the category of all R-modules if and only if it is so in the category of graded R-modules. The situation for 'injective' is slightly more complicated. Nevertheless there exist enough injectives.

Theorem 1.12. *Let M be a graded R-module. Then M has a resolution*

$$0 \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \cdots \longrightarrow I^m \longrightarrow \cdots$$

by graded R-modules I^i that are injective objects in the category of graded R-modules.

Over a *Noetherian* ring the direct sum of injective modules is injective. If we combine this fact with Zorn's lemma and the (defining) property of injective modules, namely to be direct summands in each of their overmodules, then we get that

every injective module is the direct sum of indecomposable such modules, and moreover one can 'describe' the indecomposable injective modules. All this carries over to the graded category. We content ourselves with a very special case given in 1.14 below.

Graded K-duals. Let M be a graded R-module. We consider the *graded K-dual*

$$M^\vee = \bigoplus_{i\in\mathbb{Z}} \mathrm{Hom}_K(M_{-i}, K).$$

A priori $M^\vee$ is just a graded K-vector space, but we can easily turn it into a graded R-module: for a j-form $x \in R$, and $\varphi \in \mathrm{Hom}_K(M_{-i}, K)$ we set $x\varphi = \varphi \circ \vartheta_x$ where ϑ_x denotes multiplication by x. Then this operation is extended bilinearly over $R \times M$. It is not hard to check that $^\vee$ defines a functor from the category of graded R-modules into itself.

We list some important properties of the graded K-dual:

Proposition 1.13. (a) *The additive contravariant functor $^\vee$ is exact;*
(b) $M^{\vee\vee} \cong M$ *for all graded R-modules M such that* $\dim_K M_i < \infty$ *for all i; in particular* $M^{\vee\vee} \cong M$ *for all Noetherian and Artinian graded R-modules;*
(c) $M^\vee \cong {}^*\mathrm{Hom}_R(M, R^\vee)$ *for all graded R-modules M;*
(d) *if M is Noetherian (Artinian), then $M^\vee$ is Artinian (Noetherian).*

Part (a) is obvious, and (b) is not much more than the reflexivity of finite-dimensional K-vector spaces. For (b) one should note that $M^\vee$ is a vector subspace of $\mathrm{Hom}_K(M, K)$. Therefore one obtain the isomorphism by restricting the natural isomorphism $\mathrm{Hom}_R(M, \mathrm{Hom}_K(R, K)) \cong \mathrm{Hom}(M, K)$ to the appropriate subspaces. Because of (a) and (c) the functor $\mathrm{Hom}_R(\_, R^\vee)$ is exact on the category of graded R-modules so that $R^\vee$ is an injective object in that category. Since it contains $K \cong (R^\vee)_0$ in a natural way and is an essential extension of K, it is the injective hull of K, in fact, also in the category of all R-modules.

Theorem 1.14. *The graded R-module $R^\vee$ is the (graded) injective hull of the R-module K. Moreover every (graded) injective R-module M is the direct sum $(R^\vee)^m$ of $m = \dim_K \mathrm{Hom}_R(K, M)$ copies of $R^\vee$.*

Proposition 1.13 and Theorem 1.14 show that the graded K-dual is the graded analogue of what Matlis duality is for complete local rings.

Local cohomology. What has been said above shows that the theory of local rings has a graded counterpart (which, in a sense, is even simpler). This analogy includes local cohomology.

Definition 1.15. For a (graded) R-module we set

$$\Gamma_\mathfrak{m}(M) = \{x \in M : \mathfrak{m}^j x = 0 \text{ for some } j\}.$$

Note that $\Gamma_\mathfrak{m}(M)$ is a (graded) submodule of M. Moreover, if $f : M \to N$ is an R-linear map, then $f(\Gamma_\mathfrak{m}(M) \subset \Gamma_m(N)$, and therefore $\Gamma_\mathfrak{m}$ defines a covariant left exact functor.

Definition 1.16. The i-the local cohomology $H^i_{\mathfrak{m}}(\_)$ is the i-th right derived functor of $\Gamma_{\mathfrak{m}}$, i.e. if $I^\bullet$ is ω (graded) injective resolution of M, then $H^i_{\mathfrak{m}}(M)$ is the i-th cohomology of $\Gamma_{\mathfrak{m}}(I^\bullet)$; especially $\Gamma_{\mathfrak{m}}(M) = H^0_{\mathfrak{m}}(M)$.

The preceding definitions make sense with and without the parentheses, and moreover, if M is a graded R-module, then they yield the same result: it does not matter whether local cohomology is computed from an injective resolution in the category of graded R-modules or from one in the category of all R-modules, except that in the first case we obtain a natural grading. This follows from part (a) of the following proposition; cf. 1.11.

Proposition 1.17. (a) *For any R-module M and all $i \geq 0$ one has*

$$H^i_{\mathfrak{m}}(M) \cong \varinjlim \operatorname{Ext}^i_R(R/\mathfrak{m}^k, M).$$

(b) *A short exact sequence $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ gives rise to a long exact sequence*

$$\begin{aligned} 0 \longrightarrow \Gamma_{\mathfrak{m}}(M_1) \longrightarrow \Gamma_{\mathfrak{m}}(M_2) \longrightarrow \Gamma_{\mathfrak{m}}(M_3) \longrightarrow H^1_{\mathfrak{m}}(M_1) \longrightarrow \cdots \\ \longrightarrow H^{i-1}_{\mathfrak{m}}(M_3) \longrightarrow H^i_{\mathfrak{m}}(M_1) \longrightarrow H^i_{\mathfrak{m}}(M_2) \longrightarrow \cdots \end{aligned}$$

(c) *If M is a finite graded R-module, then the modules $H^i_{\mathfrak{m}}(M)$ are Artinian;*

Since injective resolutions are very hard to grasp, it is difficult to understand local cohomology if one has just its definition. Fortunately one can access it also from another complex, which in some cases yields an effective computation; the most notable case is Hochster's determination of the local cohomology of the Stanley–Reisner ring of a simplicial complex (see [1], Chapter 5). We define the complex $C^\bullet$ by

$$\begin{aligned} C^\bullet : 0 \longrightarrow C^0 \longrightarrow C^1 \longrightarrow \cdots \longrightarrow C^n \longrightarrow 0, \\ C^t = \bigoplus_{1 \leq i_1 < i_2 < \cdots < i_t \leq n} R_{x_{i_1} x_{i_2} \cdots x_{i_t}}, \end{aligned}$$

where the differentiation $d^t : C^t \to C^{t+1}$ is given on the component

$$R_{x_{i_1} \cdots x_{i_t}} \longrightarrow R_{x_{j_1} \cdots x_{j_{t+1}}}$$

to be the homomorphism $(-1)^{s-1} \cdot \mathrm{nat} : R_{x_{i_1} \cdots x_{i_t}} \to (R_{x_{i_1} \cdots x_{i_t}})_{x_{j_s}}$ if $\{i_1, \ldots, i_t\} = \{j_1, \ldots, \hat{j_s}, \ldots, j_{t+1}\}$ and 0 otherwise.

Theorem 1.18. *Let M be an R-module. Then $H^i_{\mathfrak{m}}(M) \cong H^i(M \otimes_R C^\bullet)$ for all $i \geq 0$.*

One consequence of 1.18 is the behaviour of local cohomology under a change of rings.

Proposition 1.19. *Let R and S be graded K-algebras with maximal graded ideals $\mathfrak{m}$ and $\mathfrak{n}$. Suppose that $\varphi\colon R \to S$ is a homomorphism of graded K-algebras for which* $\mathrm{Rad}(\varphi(\mathfrak{m})S) = \mathfrak{n}$. *Then $H^i_{\mathfrak{m}}(M) \cong H^i_{\mathfrak{n}}(M)$ (as graded modules over R) for all i and all graded S-modules M.*

The natural map of R-modules

$$\mathrm{Ext}^i_R(R/\mathfrak{m}^k, M) \to (\mathrm{Ext}^i_R(R/\mathfrak{m}^k, M))_{\mathfrak{m}} = \mathrm{Ext}^i_{R_{\mathfrak{m}}}(R_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})^k, M_{\mathfrak{m}})$$

is an isomorphism. Since the local cohomology of $M_{\mathfrak{m}}$ as a module over the local ring $R_{\mathfrak{m}}$ is the direct limit of the $\mathrm{Ext}^i_{R_{\mathfrak{m}}}(R_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})^k, M)$, we see that in fact

$$H^i_{\mathfrak{m}}(M) \cong H^i_{\mathfrak{m}R_{\mathfrak{m}}}(M_{\mathfrak{m}})$$

so that one has an alternative approach to graded local cohomology: $H^i_{\mathfrak{m}R_{\mathfrak{m}}}(M_{\mathfrak{m}})$ is a graded R-module in a natural way. At least one can use the isomorphism above in order to reduce assertions about graded local cohomology to 'local' local cohomology, for example *Grothendieck's vanishing theorem.*

Theorem 1.20. *Let M be a finite graded R-module of depth t and dimension d. Then*
(a) $H^i_{\mathfrak{m}}(M) = 0$ *for* $i < t$ *and* $i > d$,
(b) $H^t_{\mathfrak{m}}(M) \neq 0$ *and* $H^d_{\mathfrak{m}}(M) \neq 0$.

2 Hilbert functions

Let R be a graded K-algebra as above, and M be a graded R-module. If all the graded components M_i are finite-dimensional vector spaces, then we can define the Hilbert function and the Hilbert series of M; in particular this is possible if M is a Noetherian or Artinian R-module:

Definition 2.1. Let M be a finite graded R-module. The numerical function $H(M,\_)\colon \mathbb{Z} \to \mathbb{Z}$ with $H(M,n) = \dim_K M_n$ for all $n \in \mathbb{Z}$ is the *Hilbert function* of M, and $H_M(t) = \sum_{n\in\mathbb{Z}} H(M,n)t^n$ is the *Hilbert series* of M.

In the following we shall occasionally have to assume that K is an infinite field. This is never a problem. The Hilbert function of $M \otimes_K L$ as a graded module over $R \otimes_K L$ coincides with that of M for all extension fields L of M. Furthermore the homological properties of M are stable under such extensions; see [1].

Hilbert series and free resolutions. In our investigation of Hilbert functions we follow Hilbert's approach via free resolutions. (See [1] for a 'modern' treatment.)

Theorem 2.2. *Let R be a graded K-algebra, and M be a finite graded R-module. Then*

$$H_M(t) = H_R(t) \cdot P_M(t,-1).$$

Suppose first that M has a finite free resolution

$$0 \longrightarrow \bigoplus_j R(-j)^{\beta_{pj}} \longrightarrow \cdots \longrightarrow \bigoplus_j R(-j)^{\beta_{0j}} \longrightarrow M \longrightarrow 0.$$

The Hilbert series of $\bigoplus_j R(-j)^{\beta_{ij}}$ is $H_R(t)\sum_j \beta_{ij}t^j H_R(t)$, and so the formula follows since the Hilbert series is additive on exact sequences.

For the applications we have in mind it is however important to note that the theorem is equally valid if the minimal free resolution has infinite length. Then one considers the vector spaces in each degree separately: this is possible since in each degree there exist only finitely many non-zero terms. Namely, if we set $s_i = \min\{j\colon \beta_{ij} \neq 0\}$, then the 'minimal shifts' s_i are strictly ascending.

Suppose that S is the polynomial ring $K[X_1,\ldots,X_d]$ with a grading defined by $\deg X_i = a_i$. Then

$$H_S(t) = \frac{1}{(1-t^{a_1})\cdots(1-t^{a_d})}.$$

This follows easily by induction on d: we have an exact sequence

$$0 \longrightarrow S(-a_d) \xrightarrow{X_d} S \longrightarrow S' \longrightarrow 0, \qquad S' = K[X_1, \ldots, X_{d-1}],$$

and the additivity of the Hilbert function implies $(1 - t^{a_1})H_S(t) = H_{S'}(t)$.

Theorem 2.3. *Let R be a graded K-algebra, and $M \neq 0$ a finite graded R-module of dimension d. Then there exist positive integers $a_1, \ldots, a_d$, and $Q(t) \in \mathbb{Z}[t, t^{-1}]$ such that*

$$H_M(t) = \frac{Q(t)}{\prod_{i=1}^{d}(1 - t^{a_i})} \qquad \textit{with} \quad Q(1) > 0.$$

For the proof we choose a Noether normalization $S \subset R/(\operatorname{Ann} M)$. Then M is a finite S-module in a natural way, and $S \cong K[X_1, \ldots, X_d]$. By Hilbert's syzygy theorem M has a graded free resolution

$$0 \longrightarrow \bigoplus_j R(-j)^{\beta_{pj}} \longrightarrow \cdots \longrightarrow \bigoplus_j R(-j)^{\beta_{0j}} \longrightarrow M \longrightarrow 0.$$

We choose $Q(t) = P_M(t, -1) = \sum_{i=1}^{p}(-1)^i(\sum_j \beta_{ij}t^j)$. Since $\dim M = \dim S$, M has positive rank over S, and $Q(1) = \operatorname{rank}_S M$ by the additivity of rank.

Generating functions of the type occuring in Theorem 2.3 appear frequently in combinatorics, and one can describe their associated numerical functions very precisely. A function $P\colon \mathbb{Z} \to \mathbb{C}$ is called a *quasi-polynomial (of period g)* if there exist a positive integer g and polynomials P_i, $i = 0, \ldots, g-1$, such that for all $n \in \mathbb{Z}$ one has $P(n) = P_i(n)$ where $n = mg + i$ with $0 \leq i \leq g - 1$.

Theorem 2.4 (Serre). *Let R be a graded K-algebra, and $M \neq 0$ a finite graded R-module of dimension d. Then*
(a) *there exists a uniquely determined quasi-polynomial P_M with $H(M, n) = P_M(n)$ for all $n \gg 0$; the minimal period of P_M divides $a_1 \cdots a_d$;*
(b) *$H(M, n) - P_M(n) = \sum_{i=0}^{d}(-1)^i \dim_k H^i_{\mathfrak{m}}(M)_n$ for all $n \in \mathbb{Z}$;*
(c) *one has*

$$\begin{aligned} \deg H_M(t) &= \max\{n\colon H(M, n) \neq P_M(n)\} \\ &= \max\{n\colon \sum_{i=0}^{d}(-1)^i \dim_k H^i_{\mathfrak{m}}(M)_n \neq 0\}. \end{aligned}$$

(Here $\deg H_M(t)$ denotes the degree of the rational function $H_M(t)$.)

Part (a) and the first equation in (c) are exercises in rational generating functions; it is obviously sufficient to prove them for the function $(1 - t^{a_1})^{-1} \cdots (1 - t^{a_d})^{-1}$. For (b), note that the general behaviour of local cohomology under ring extensions allows us to replace R again by a Noether normalization S of $R/(\operatorname{Ann} M)$. The right hand side in (b) is additive on exact sequences as every Euler characteristic formed from a series of derived functors. (The K-dimensions of the local cohomology modules are finite: $H^i_{\mathfrak{m}}(M)$ is Artinian.) Therefore induction on $\operatorname{proj\,dim} M$ reduces the theorem to the case $M = S$ which is then handled by induction on $\dim S$: for $S = K$ the theorem is indeed true.

Definition 2.5. (a) The quasi-polynomial P_M is called the *Hilbert quasi-polynomial* of M.
(b) The degree $a(R)$ of the rational function $H_R(t)$ is called the *a-invariant* of the graded K-algebra R.

By Theorem 2.4, we have $a(R) < 0$ if and only the equation $P_R(n) = H(R,n)$ holds for all $n \geq 0$. At least in the Cohen–Macaulay case the a-invariant has a satisfactory homological interpretation:

Proposition 2.6. *Let R be a graded Cohen–Macaulay K-algebra of dimension d. Then*

$$a(R) = \max\{i\colon H^d_{\mathfrak{m}}(R)_i \neq 0\}.$$

Homogeneous K-algebras. The exponents a_i in the denominator of $H_M(t)$ are the degrees of the elements in a homogeneous system of parameters of $R/(\operatorname{Ann} M)$. As pointed out above, we may freely assume that K is infinite; by 1.6 we can then choose a system of parameters among the 1-forms, if R is a homogeneous K-algebra.

Theorem 2.7. *Let R be a homogeneous K-algebra, and M a finite graded R-module of dimension d. Then there exists $Q_M(t) \in \mathbb{Z}[t,t^{-1}]$ such that*

$$H_M(t) = \frac{Q_M(t)}{(1-t)^d} \qquad \text{with} \quad Q_M(1) \neq 0.$$

In particular it follows that the Hilbert quasi-polynomial of M is a true polynomial now, and therefore one uses the term *Hilbert polynomial* for modules over homogeneous K-algebras.

Theorem 2.8. *Let R be a homogeneous K-algebra, and $M \neq 0$ a finite graded R-module of dimension $d > 0$. Then the Hilbert polynomial of M can be written*

$$P_M(n) = \frac{e(M)}{(d-1)!}n^{d-1} + \text{terms of lower degree.}$$

where $e(M) > 0$ is an integer, namely $e(M) = Q_M(1)$.

That the degree of the Hilbert polynomial is $d-1$, can be considered as a statement about generating functions; however, there is also a direct proof in terms of commutative algebra. (See [1], 4.1.3.) That the leading term of the Hilbert polynomial is a rational number with denominator $(d-1)!$ follows simply from the fact that every integer valued polynomial is a $\mathbb{Z}$-linear combination of the binomial coefficients $\binom{n+k}{k}$ viewed as functions of n.

Definition 2.9. The number $e(M) = Q_M(1)$ is the *multiplicity* of M. (Note that $Q_M(1) = \dim_K M$ if $\dim M = 0$, and recall that, more generally, $Q_M(1)$ is the rank of M over a Noether normalization of $R/(\operatorname{Ann} M)$ generated by 1-forms.)

The numerator polynomial of $H_M(t)$ is uniquely determined. This fact justifies the following definition.

Definition 2.10. We write $Q_M(t) = \sum_i h_i t^i$, and call the sequence $(h_i)_{i\in\mathbf{Z}}$ the *h-vector* of M.

The concept of h-vector is a bridge between combinatorics and commutative algebra. For example, if Δ is a simplicial complex, then the h-vector of Δ and the h-vector of the Stanley-Reisner ring $K[\Delta]$ coincide. The next theorem indicates that a ring-theoretic property can be combinatorially significant.

Proposition 2.11. *Assume that in addition to the assumptions of* 2.8 *the module M is Cohen-Macaulay. Then the h-vector of M is non-negative.*

Choose an M-regular 1-form $x \in R$. Then we have an exact sequence

$$0 \longrightarrow M(-1) \xrightarrow{x} M \longrightarrow M/xM \longrightarrow 0.$$

The additivity of the Hilbert series implies $H_{M/xM}(t) = (1-t)H_M(t)$. Therefore M and M/xM have the same h-vector, and by induction it is enough to proof the assertion in the case in which dim $= 0$. In that case $h_i = H(M,i) \geq 0$ for all i.

For $M = R$ one can give much stronger bounds for the h-vector. If $\boldsymbol{x}$ is a homogeneous system of parameters of R, then $R/(\boldsymbol{x})$ is a zero dimensional K-algebra with the same h-vector as R. Therefore one can apply Macaulay's theorem about the Hilbert functions of zero dimensional homogeneous algebras (see [1], Section 4.2). For example, if the Stanley-Reisner ring of a simplicial complex Δ is Cohen-Macaulay, then the h-vector of Δ satisfies the bounds provided by Macaulay's theorem.

The reader may have noticed that 2.7, 2.8, and 2.11 do not really require R to be homogeneous. What we precisely need is that R has a homogeneous system of parameters consisting of 1-forms, at least after an extension of K to an infinite field. This is equivalent to $R/(R_1)$ being a finite dimensional vector space, and we call such graded algebras *almost homogeneous*.

3 Graded canonical modules

We introduce the graded canonical module of a graded Cohen-Macaulay K-algebra as an object with distinguished numerical invariants.

Definition 3.1. Let R be a Cohen–Macaulay graded K-algebra of dimension d. A finite graded R-module C is a *graded canonical module* of R if there exist homogeneous isomorphisms

$$\operatorname{Ext}^i_R(K,C) \cong \begin{cases} 0 & \text{for } i \neq d, \\ K & \text{for } i = d. \end{cases}$$

Note that the condition $\operatorname{Ext}^i_R(K,C) = 0$ for $i = 0, \ldots, d-1$ implies that C is a maximal Cohen–Macaulay R-module. The fact that $\operatorname{Ext}^i_R(K,C) = 0$ for all $i > d$ is a similarly strong condition; see [1], Section 3.1 for the the local version of the next theorem. (It does not matter whether the invariants in 3.2 are measured in the category of graded R-modules or in that of all R-modules.)

Theorem 3.2 (Bass). *Let M be a finite graded R-module and $t = \operatorname{depth} R$. Then the following conditions are equivalent:*
(a) *M has finite injective dimension as an R-module;*
(b) $\operatorname{inj\,dim}_R M = \operatorname{depth} R$;
(c) $\operatorname{Ext}^i_R(K,M) = 0$ *for all* $i > t$.

A graded K-algebra is necessarily Cohen–Macaulay if it has a non-zero finite graded module of finite injective dimensiom. This fact, called *Bass' conjecture*, was proved by Peskine and Szpiro; that it similarly holds for all Noetherian local rings, is due to Roberts. (For a proof in the equicharacteristic case see [1], Chapter 9.)

As we will see, every Cohen–Macaulay graded K-algebra has a uniquely determined graded canonical module.

Existence and uniqueness. In dimension 0 the situation is very simple.

Proposition 3.3. *Suppose R is a graded K-algebra of dimension 0. Then $R^\vee$ is the unique graded canonical module of R.*

The proposition follows readily from our observations about injective modules in Section 1.

One method to show the existence and uniqueness of ω_R in general is the reduction of all steps to the special case in which the dimensions of all the algebras involved are equal to 0. This method is carried out in all details in [1], at least in the local case (which, if one has it available, makes the extension to the graded case very easy). The reduction to dimension 0 is by taking residue classes with respect to homogeneous regular sequences, and it is based on the following lemma of Rees.

Lemma 3.4. *Let R be a graded K-algebra, and M and N graded R-modules; if $x \in R$ is a homogeneous element of degree a which is R- and M-regular and annihilates N, then*

$$\operatorname{Ext}_R^{i+1}(N, M)(-a) \cong \operatorname{Ext}_{R/(x)}^{i}(N, M/xM) \qquad \text{for all } i \geq 0.$$

Given modules C and C' over R that satisfy the conditions for being a graded canonical module, we immediately conclude from this lemma that $(C/\boldsymbol{x}C)(\sum \deg x_i)$ and $(C'/\boldsymbol{x}C')(\sum \deg x_i)$ are canonical modules of $R/(\boldsymbol{x})$ if $\boldsymbol{x} = x_1, \ldots, x_d$ is a homogeneous R-sequence. In particular, if $\boldsymbol{x}$ is a maximal such sequence, then $(C/\boldsymbol{x}C)(\sum \deg x_i)$ and $(C'/\boldsymbol{x}C')(\sum \deg x_i)$ are isomorphic $R/(\boldsymbol{x})$-modules. The next proposition shows that we can indeed lift this isomorphism to an isomorphism of C and C', thereby establishing the uniqueness of the canonical module.

Proposition 3.5. *Let R be a Cohen–Macaulay graded K-algebra of dimension d, and C a graded canonical module of R*
(a) *If M is a graded maximal Cohen–Macaulay R-module, then $\operatorname{Hom}_R(M, C)$ is a maximal Cohen–Macaulay module, and for every R-sequence $\boldsymbol{x}$ we have a homogeneous isomorphism*

$$\operatorname{Hom}_R(M, C) \otimes R/(\boldsymbol{x}) \cong \operatorname{Hom}_{R/(\boldsymbol{x})}(M/\boldsymbol{x}M, C/\boldsymbol{x}C).$$

Furthermore $\operatorname{Ext}_R^j(M, C) = 0$ for all $j > 0$.
(b) *More generally, if M is a Cohen–Macaulay R-module of dimension t, then $\operatorname{Ext}_R^j(M, C) = 0$ if and only if $j = d - t$; $\operatorname{Ext}_R^{d-t}(M, C)$ is also Cohen–Macaulay of dimension t, and*

$$\operatorname{Ext}_R^{d-t}\Big(\operatorname{Ext}_R^{d-t}(M, C), C\Big) \cong M.$$

Now that we know the canonical module is unique we denote it by

$$\omega_R.$$

The proposition, whose proof is an exercise in exact sequences, implies in particular that

$$\operatorname{Hom}_R(\omega_R, \omega_R) \cong \operatorname{Hom}_R\Big(\operatorname{Hom}_R(R, \omega_R), \omega_R\Big) \cong R.$$

It also helps us in establishing the existence of the canonical module. Suppose first that $R = S = K[x_1, \ldots, x_d]$ with $\deg X_i = a_i$. As a first attempt we try S as its own graded canonical module. Since S is a maximal Cohen–Macaulay S-module, Rees' lemma implies that $K(\sum a_i)$ is the graded canonical module of K, and this is obviously false. But we only need to correct the grading: $S(-\sum a_i)$ is the graded canonical module of S.

Now let R be an arbitrary Cohen–Macaulay graded K-algebra. We choose a graded Noether normalization $S \subset R$, $S = K[X_1, \ldots, X_d]$. As we have just seen, S has a graded canonical module ω_S. Set $C = \operatorname{Hom}_S(R, \omega_S)$. Then the proposition

implies that C is a maximal Cohen–Macaulay S-module, and therefore it is such an R-module (use the sequence $\boldsymbol{x} = x_1, \ldots, x_d$). Furthermore

$$\begin{aligned}(C/\boldsymbol{x}C)(\textstyle\sum \deg x_i) &= \operatorname{Hom}_{S/(\boldsymbol{x})}(S/(\boldsymbol{x}), R/\boldsymbol{x}R)\\ &= \operatorname{Hom}_K(K, R/\boldsymbol{x}R) = (R/\boldsymbol{x}R)^\vee,\end{aligned}$$

so that C is indeed the graded canonical module of R (use Rees' lemma).

Theorem 3.6. *Let R be a Cohen–Macaulay graded K-algebra. Then R has a unique graded canonical module ω_R.*

In establishing this theorem we have used the fact that R contains a polynomial K-algebra over which it is a finite graded module. One can also compute the canonical module from a representation as a residue class ring, or more generally from an arbitrary representation of R as a module-finite extension.

Proposition 3.7. *Let R and S be Cohen–Macaulay graded K-algebras, and suppose that $\varphi\colon S \to R$ is a homogeneous K-algebra homomorphism such that R is a finite graded S-module with respect to φ. Then $\omega_R \cong \operatorname{Ext}^t_S(R, \omega_S)$, where $t = \dim S - \dim R$.*

Using appropriate regular sequences, first in the kernel of φ, and then in $S/\operatorname{Ker}\varphi$, one reduces the proposition to the case $\dim R = \dim S = 0$. In this case it amounts to the isomorphism $R^\vee \cong \operatorname{Hom}_S(R, S^\vee)$. We have stated in 1.13 that $R^\vee$ and $\operatorname{Hom}_S(R, S^\vee)$ are isomorphic as S-modules, but this isomorphism is easily seen to be compatible with the R-module structure.

Forgetting the grading, we may consider R as a Noetherian ring, and ask the question whether a graded canonical module localizes to a canonical module of the local ring $R_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec} R$. This is indeed the case.

Proposition 3.8. *Let Let R be a Cohen–Macaulay graded K-algebra. Then $(\omega_R)_\mathfrak{p}$ is a canonical module of $R_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec} R$.*

The easiest (though perhaps not the most systematic) way for proving the proposition is to write R as a residue class ring of a polynomial ring S. Choose $\mathfrak{q} \in \operatorname{Spec} R$ to be the preimage of $\mathfrak{p}$ in S. Then $\dim S_\mathfrak{q} - \dim R_\mathfrak{p} = \dim S - \dim R$, and so the proposition follows from 3.5 and its local counterpart (and the fact that $\omega_{S_\mathfrak{q}} \cong S_\mathfrak{q}$, since $S_\mathfrak{q}$ is a regular local ring).

Gorenstein graded K-algebras. A Noetherian ring R is called *Gorenstein* if it is Cohen–Macaulay and $\omega_{R_\mathfrak{p}} \cong R_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$.

Proposition 3.9. *Let R be a Cohen–Macaulay graded K-algebra. Then the following are equivalent:*
(a) *$\omega_R \cong R(a)$ for some integer a;*
(b) *R is Gorenstein;*
(c) *$R_\mathfrak{m}$ is Gorenstein.*

The implication (c) $\Rightarrow$ (a) holds since a finite graded module M is free if and only if $M_{\mathfrak{m}}$ is free. The rest is trivial. The number a is (a) is easily identifiable: $a = a(R)$, as will be seen below.

Graded local duality. The importance of the canonical module rests to a large extent on its role as the *dualizing module* in *Grothendieck's local duality theorem.*

Theorem 3.10. *Let R be a Cohen–Macaulay graded K-algebra of dimension d. Then*
(a) $\omega_R \cong (H^d_{\mathfrak{m}}(R))^\vee$, *and*
(b) *for all finite graded R-modules and all integers i there exist natural homogeneous isomorphisms*

$$(H^{d-i}_{\mathfrak{m}}(M))^\vee \cong \operatorname{Ext}^i_R(M, \omega_R).$$

For the proof we refer to [1] where 'local' local duality is treated in detail. The reader should check that the argument given there works in the category of graded R-modules.

The Hilbert function of the canonical module. The duality between R and ω_R is also expressed by the Hilbert function of ω_R.

Theorem 3.11. *Let R be a d-dimensional Cohen–Macaulay graded K-algebra, M a maximal Cohen–Macaulay graded R-module, and $M' = \operatorname{Hom}_R(M, \omega_R)$. Then*
(a) $H_{M'}(t) = (-1)^d H_M(t^{-1})$, *and*
(b) *if R is a domain and M is a Cohen–Macaulay graded R-module with $H_M(t) = t^q H_{\omega_R}(t)$ for some q, then $M(q) \cong \omega_R$.*

For part (a) we use a Noether normalization S to simplify the situation:

$$\operatorname{Hom}_R(M, \omega_R) \cong \operatorname{Hom}_R\big(M, \operatorname{Hom}_S(R, \omega_S)\big) \cong \operatorname{Hom}_S\big(M, S(a(S)\big),$$

and since M is free S-module, it suffices to consider $M = S(b)$ for some $b \in \mathbb{Z}$. Then everything boils down to the identity $1/(1-t^{-1}) = -t/(1-t)$.

Replacing M by $M(q)$ we may assume that $q = 0$ in (b). Note that (a) implies the equation $H_{M'}(t) = H_R(t)$. Let x be a non-zero degree 1 element of M'. Then the map $R \to M'$, $r \mapsto rx$, is injective since a maximal Cohen–Macaulay R-module is torsionfree and every non-zero element of R is R-regular. The equality of Hilbert series then yields $Rx = M'$. Since $M \cong M''$, we have $M \cong R' \cong \omega_R$.

Corollary 3.12 (Stanley). *With the notation and hypothesis of* 3.11 *suppose that R has the Hilbert series $H_R(t) = \sum_{i=0}^s h_i t^i / \prod_{j=1}^d (1-t^{a_j})$.*
(a) *Then $H_{\omega_R}(t) = (-1)^d H_R(t^{-1})$, equivalently,*

$$H_{\omega_R}(t) = \frac{t^{\sum a_j - s} \sum_{i=0}^s h_{s-i} t^i}{\prod_{j=1}^d (1-t^{a_j})}.$$

(b) *If R is Gorenstein, then $H_R(t) = (-1)^d t^{a(R)} H_R(t^{-1})$.*
(c) *Suppose R is a domain, and $H_R(t) = (-1)^d t^q H_R(t^{-1})$ for some integer q. Then R is Gorenstein.*

The corollary implies in particular that

$$a(R) = -\min\{i\colon (\omega_R)_i \neq 0\};$$

this equation follows also from local duality and 2.4.

If R is almost homogeneous, then the equation $H_R(t) = (-1)^d t^{a(R)} H_R(t^{-1})$ just says that the h-vector of R is a palindrome, and if the h-vector of an almost homogeneous Cohen–Macaulay integral domain is palindromic, then R is Gorenstein!

As an application of 2.11 one obtains an equality for the h-vector of an almost homogeneous Cohen–Macaulay domain.

Theorem 3.13 (Stanley). *Let R be an almost homogeneous Cohen–Macaulay K-algebra with h-vector $(h_0, \ldots, h_s)$, $s = a(R) + \dim R$. Suppose that R is an integral domain. Then*

$$\sum_{i=0}^{j} h_i \leq \sum_{i=0}^{j} h_{s-i} \qquad \text{for all} \quad j = 0, \ldots, s.$$

Set $a = a(R)$. We choose a non-zero element $x \in (\omega_R)_{-a}$). Then, by the same argument as above, we have an exact sequence

$$0 \longrightarrow R \longrightarrow \omega_R(-a) \longrightarrow N \longrightarrow 0.$$

From standard arguments on depth it follows that N is a Cohen–Macaulay R-module of dimension $\dim R - 1$. According to 2.11 it has a non-negative h-vector. This h-vector can be computed from those of R and ω, and its non-negativity implies the inequalities claimed.

4 Invariants of finite groups

In the invariant theory of finite groups ring theory and combinatorics are inextricably connected. Let K be a field of characteristic 0, and $G \subset \mathrm{GL}_n(K)$ a finite linear group. The group G operates on the polynomial ring $R = K[X_1, \ldots, X_n]$ in a natural way: we can identify each indeterminate with an element of the canonical basis of K^n, and then, for every $g \in G$ consider the automorphism of R induced by the substitution $X_i \mapsto g(X_i)$; we simply denote this automorphism by g. The set

$$R^G = \{s \in R\colon g(s) = s \text{ for all } g \in G\}$$

of *G-invariants* is a K-subalgebra of R. Evidently a polynomial s is invariant if and only if its homogeneous components are invaraiant; therefore R^G is a graded subalgebra of R.

The group G operates linearly on each vector space R_m. By Maschke's theorem, R_m is a direct sum of irreducible representations of G. It follows that R itself is the direct sum of such representations. There are only finitely many isomorphism classes of irreducible representations $\Omega_0, \ldots, \Omega_r$ of G where we let Ω_0 is the trivial representation on K (i.e. $g(x) = x$ for all $x \in K$). For each j we form the vector subspace N_j by taking the sum of all irreducible representations in G that belong to the isomorphism class Ω_j; in particular $N_0 = R^G$.

Let V be an irreducible representation, and s an invariant. Then $g(sv) = g(s)g(v) = sg(v)$ for all $v \in V$ and $g \in G$. Thus sV and V are isomorphic representations of G. It follows that $sN_j \subset N_j$ for all $s \in R$ and all j, in other words each N_j is an R^G-submodule of R.

The next observation is that R is an integral extension of R^G. In fact each element s of R is a zero of the monic polynomial

$$\prod_{g \in G} (Y - g(s)) \in R^G[Y].$$

Theorem 4.1. (a) *R^G is a graded Cohen–Macaulay K-algebra, and R is a finite R^G-module.*
(b) *As an R^G-module R splits into the direct sum $R^G = N_0 \oplus N_1 \oplus \cdots \oplus N_r$.*
(c) *Each N_i is a maximal Cohen–Macaulay R^G-module (provided $N_i \neq 0$).*

Part (b) has been shown above. For the proof of (a) let us first notice that R is a finitely generated R^G-algebra; being integral over R^G, it is a module-finite extension of R^G. Next observe that for each ideal $\mathfrak{a} \in R^G$ one has $R^G \cap \mathfrak{a}R = \mathfrak{a}$ because of (b).

Thus R^G is a Noetherian ring, and therefore a finitely generated K-algebra. We choose a homogeneous system of parameters in R^G; it is also a homogeneous system of parameters of R, therefore an R-sequence, and finally an N_i-sequence since N_i is a direct R^G-module summand of R for each i. In particular R^G is a Cohen–Macaulay ring.

The Hilbert series of the N_i are given by a classical formula of Molien. Therefore one calls them *Molien series*. We restrict ourselves to those N_i for which the corresponding irreducible representation has K-dimension 1. This means, for each $x \in N_i$ one has

$$g(x) = \chi_i(g)x$$

where $\chi_i : G \to K^\times$ is a group homomorphism. We write R^χ for N_i, and denote its Molien series by $M_\chi(t)$. Typical examples are the powers $\det^u$ of the determinant map, i.e. $\chi(g) = (\det g)^u$ for some $u \in \mathbb{Z}$.

Let us define the linear operator ρ^χ on R by

$$\rho^\chi(r) = |G|^{-1} \sum_{g \in G} \chi(g)^{-1} g(r).$$

It is easy to check that $\rho^\chi(R) = R^\chi$ and $\rho^\chi(r) = r$ for $r \in R^\chi$. The operator ρ^χ is a K-endomorphism of the graded K-vector space R. Let ρ_i^χ denote its restriction to R_i; then $\rho_i^\chi = (\rho_i^\chi)^2$, and therefore

$$\dim R_i^\chi = \dim \operatorname{Im} \rho_i^\chi = \operatorname{Tr} \rho_i^\chi = |G|^{-1} \sum_{g \in G} \chi(g)^{-1} \operatorname{Tr} g|_{R_i}.$$

Here Tr denotes the trace, and we use its linearity. Combining the formulas yields

$$M_\chi(t) = |G|^{-1} \sum_{g \in G} \chi(g)^{-1} \sum_{i=0}^{\infty} (\operatorname{Tr} g|_{R_i}) t^i.$$

(All this remains correct for irreducible representations of dimension $w > 1$ if we replace the factor $|G|^{-1}$ by $w|G|^{-1}$ and denote the character of the representation by χ; in order to check that ρ^χ has the desired properties one needs some elementary facts about group representations.)

Theorem 4.2 (Molien's formula). *Let K be a field of characteristic 0, V a finite dimensional K-vector space, G a finite subgroup of* $\mathrm{GL}(V)$, *and $\chi : G \to K^\times$ a group homomorphism. Then the Molien series of R^χ is given by*

$$M_\chi(t) = |G|^{-1} \sum_{g \in G} \frac{\chi(g)^{-1}}{\det(\mathrm{id} - tg)}.$$

We need to show that

$$\frac{1}{\det(\mathrm{id} - tg)} = \sum_{i=0}^{\infty} (\operatorname{Tr} g|_{R_i}) t^i$$

for each $g \in G$. In fact, this equation holds for an arbitrary element $g \in \mathrm{GL}(V)$. In order to prove it we may extend K to an algebraically closed field. Then, for a suitable basis $X_1, \ldots, X_n$ of V, g is given by an upper triangular matrix whose diagonal entries are the eigenvalues $\lambda_1, \ldots, \lambda_n$ of g (as an element of $\mathrm{GL}(V)$).

The monomials of total degree i in $X_1, \ldots, X_n$ form a basis of the vector space R_i. If these monomials are ordered lexicographically, then $g|_{R_i}$ is again represented by an upper diagonal matrix whose diagonal entry corresponding to the monomial $X^{\boldsymbol{a}} = X_1^{a_1} \cdots X_n^{a_n}$ is $\lambda^{\boldsymbol{a}} = \lambda_1^{a_1} \cdots \lambda_n^{a_n}$. Therefore

$$\operatorname{Tr} g|_{R_i} = \sum_{|\boldsymbol{a}|=i} \lambda^{\boldsymbol{a}},$$

and the expansion of the product of the geometric series $1/(1-\lambda_j t)$, $j = 1, \ldots, n$, gives us

$$\sum_{i=0}^{\infty} (\operatorname{Tr} g|_{R_i}) t^i = \sum_{i=0}^{\infty} \sum_{|\boldsymbol{a}|=i} \lambda^{\boldsymbol{a}} t^i = \prod_{j=1}^{n} \frac{1}{1-\lambda_j t}.$$

Using that $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$ are the eigenvalues of g^{-1}, we finally get

$$\prod_{j=1}^{n} \frac{1}{1-\lambda_j t} = \prod_{j=1}^{n} \frac{\lambda_j^{-1}}{\lambda_j^{-1} - t} = \frac{\det g^{-1}}{\det(g^{-1} - t\,\mathrm{id})} = \frac{1}{\det(\mathrm{id} - gt)}.$$

We use Molien's formula in order to determine the canonical module of R^G.

Theorem 4.3 (Watanabe). *Let K be a field of characteristic 0, V a K-vector space of dimension n, $R = S(V)$, and G a finite subgroup of $\mathrm{GL}(V)$.*
(a) *Then $R^{\det^{-1}}(-n)$ is the canonical module of R^G.*
(b) *In particular R^G is Gorenstein if $G \subset \mathrm{SL}(V)$.*

Set $S = R^G$ and $\chi = \det^{-1}$. It was observed above that N is a maximal Cohen–Macaulay S-module. Furthermore

$$\begin{aligned} M_\chi(t) &= |G|^{-1} \sum_{g \in G} \frac{\det g}{\det(\mathrm{id} - tg)} = |G|^{-1} \sum_{g \in G} \frac{1}{\det(g^{-1} - t\,\mathrm{id})} \\ &= |G|^{-1} \sum_{g \in G} \frac{1}{\det(g - t\,\mathrm{id})} = |G|^{-1} \sum_{g \in G} \frac{(-1)^n t^{-n}}{\det(\mathrm{id} - t^{-1} g)} \\ &= (-1)^n t^{-n} M_G(t^{-1}). \end{aligned}$$

As the Molien series are Hilbert series, we may apply 3.11 to conclude that $N(-n)$ is the canonical module of S. This proves (a).

If $G \subset \mathrm{SL}(V)$, then, by (a), S is isomorphic to the canonical module of S. As a canonical module is canonical, S is Gorenstein.

The use of combinatorial methods in the investigation of rings of invariants of finite groups is by no means limited to the preceding theorem. For further results, for example the Shepard–Todd–Chevalley–Serre theorem on the invariants of reflection groups or a partial converse to part (b) of 4.3 we refer the reader to [1], Chapter 6.

5 Normal semigroup rings

Let $D \subset \mathbb{R}^n$ be a convex cone, i.e. a subset closed under the formation of linear combinations with non-negative coefficients. The elements $z \in C = D \cap \mathbb{Z}^n$ form a semigroup with respect to addition, and therefore

$$K[C] = K[X^{z_1} \cdots X^{z_n} : (z_1, \ldots, z_n) \in C] \subset K[X_1^{\pm 1}, \ldots, X_n^{\pm n}]$$

is a well-defined K-algebra. In the following we write X^z for $X^{z_1} \cdots X^{z_n}$. In general $K[C]$ is not a finitely generated K-algebra, and one cannot say much about it. However, suppose that the cone D is a *finitely generated rational cone*, i.e. there exist $c_1, \ldots, c_m \in \mathbb{Q}^n$ such that D is the set of non-negative linear combinations of $c_1, \ldots, c_m$. Then $K[C]$ looks much more promising.

Theorem 5.1. *Suppose that D is a finitely generated rational cone. Then $K[C]$ is a finitely generated K-algebra and a normal integral domain. One has* $\dim K[C] = \dim D = \operatorname{rank} C$.

The rank of a semigroup $C \subset \mathbb{Z}^n$ is the rank of the subgroup generated by C. That $K[C]$ is finitely generated is essentially Gordan's lemma; it says that C is a finitely generated semigroup if D is a finitely generated rational cone. In order to see that $K[C]$ is normal, one uses a desription of D that is equivalent to being finitely generated: D is the intersection of finitely many vector half-spaces:

$$D = \bigcap_{i=1}^{r} H_i^+, \qquad H_i^+ = \{v \in V : \langle a_i, v \rangle \geq 0\};$$

here $\langle -, - \rangle$ is the scalar product. If D is rational, then the a_i can be chosen in $\mathbb{Q}^n$, and vive versa: a cone is rational and finitely generated if and only if it is the intersection of finitely many rational vector half-spaces H_i^+. Let $C_i = H_i^+ \cap \mathbb{Z}^n$. Then it is not hard to see that

$$C_i \cong \mathbb{Z}^{n-1} \oplus \mathbb{N}$$

as a semigroup. Thus $K[C_i] \cong K[X_1^{\pm 1}, \ldots, X_{n-1}^{\pm 1}, X^n]$ is a normal ring, and $K[C]$, the intersection of the $K[C_i]$, is also normal.

When $C \subset \mathbb{Z}^n$ is an arbitrary finitely generated semigroup, then $K[C]$ is called an *affine semigroup ring*. It turns out that the rings $K[C]$ introduced above, are exactly the normal ones among all affine semigroup rings. That explains the title we have given to this section of our notes.

Faces and prime ideals. From now on it is tacitly understood that all the cones D being considered are finitely generated and rational. By C we always denote the semigroup $D \cap \mathbb{Z}^n$.

A combinatorial object accompanying D is its *face lattice* $\mathcal{F}(D)$: the faces of D are the intersections

$$D \cap H_{i_1}^0 \cap \cdots \cap H_{i_j}^0, \qquad j = 0 \ldots, m$$

where H_i^0 denotes the hyperplane $\{v \in \mathbb{R}^n : \langle a_i, v\rangle = 0\}$ bordering H_i^+. The faces are partially ordered by inclusion; with this partial order they form a lattice. The maximal face is D itself, the minimal face is $H_1^0 \cap \cdots \cap H_m^0$.

Let A be the affine subspace of $\mathbb{R}^n$ generated by a face F of D. Then the interior of D with respect to the subspace topology on A is called the *relative interior* of F; we denote it by

$$\operatorname{relint} F.$$

To each face F of D we associate an ideal of $K[C]$ by setting

$$\mathfrak{P}(F) = (X^z : z \notin C \cap F).$$

Given an ideal $\mathfrak{a}$ of $K[C]$, we say that $\mathfrak{a}$ is *C-graded* if $\mathfrak{a}$ is generated by the monomials X^z contained in $\mathfrak{a}$.

Theorem 5.2. (a) *For all prime ideals $\mathfrak{p}$ of $K[C]$ the ideal generated by the monomials in $\mathfrak{a}$ is a C-graded prime ideal.*
(b) *The assignment $F \mapsto \mathfrak{P}(F)$ is a bijection between the set of non-empty faces of D and the set of C-graded prime ideals of $K[C]$.*

We refer to [1] for the proof. The reader should note that (a) is the C-graded variant of 1.1(a).

We want to apply the theory of graded rings as developed in Sections 1, 2, and 3 to $K[C]$; this makes only sense if the grading on $K[C]$ is compatible with the semigroup structure of C.

Definition 5.3. A decomposition

$$K[C] = \bigoplus_{i \in \mathbb{N}} K[C]_i$$

of the K-vector space $K[C]$ is an *admissible grading* if $K[C]$ is a graded K-algebra with respect to this decomposition, and furthermore each component $K[C]_i$ has a basis consisting of finitely many monomials X^z.

It is not hard to see which $K[C]$ can be endowed with an admissible grading.

Proposition 5.4. *The following are equivalent:*
(a) *if $z \in C$ and $-z \in C$, then $z = 0$;*
(b) *$\{0\}$ is the minimal face of D (i.e. D has an apex);*
(c) *there exists an embedding $C \to \mathbb{N}^m$ of semigroups for some $m \geq 0$;*
(d) *$K[C]$ has an admissible grading.*

It is clear that we may replace C by D in (a). If the conditions of 5.4 are satisfied, then C or D are called *positive*. Positive cones have *cross-sections* T.

Proposition 5.5. *Let D be a positive cone.*
(a) *Then for each $x \in \mathbb{R}^n$ with $-x \notin D$ there exists an affine hyperplane A such that $x \in A$ and $T = A \cap D$ is a bounded set generating the cone D.*
(b) *Such T is a convex polytope, and its faces (including $\emptyset$) correspond bijectively to the faces of D.*

In conjunction with 5.2 the previous proposition shows that the set of C-graded prime ideals of $K[C]$ has the same combinatorial structure as the face lattice of a polytope T.

Cell complexes. A *(finite regular) cell complex* is a non-empty topological space X together with a finite set Γ of subsets of X such that the following conditions are satisfied:
(i) $X = \bigcup_{e \in \Gamma} e$;
(ii) the subsets $e \in \Gamma$ are pairwise disjoint;
(iii) for each $e \in \Gamma$, $e \neq \emptyset$ there exists a homeomorphism from a closed i-dimensional ball $B^i = \{x \in \mathbb{R}^i : \|x\| \leq 1\}$ onto the closure $\bar{e}$ of e which maps the open ball $U^i = \{x \in \mathbb{R}^i : \|x\| < 1\}$ onto e;
(iv) $\emptyset \in \Gamma$.

By the invariance of dimension the number i in (iii) is uniquely determined by e, and e is called an *open i-cell*; $\emptyset$ is a (-1)-cell. By Γ^i we denote the set of the i-cells in Γ. The dimension of Γ is given by $\dim \Gamma = \max\{i : \Gamma^i \neq \emptyset\}$. It is finite since Γ is finite. One sets $|\Gamma| = X$.

A cell e' is a *face* of the cell $e \neq e'$ if $e' \subset \bar{e}$, and a subset Σ of Γ is a *subcomplex* if for each $e \in \Sigma$ all the faces of e are contained in Σ.

The classical examples of cell complexes are convex polytopes P together with their decomposition $P = \bigcup_{f \in \mathcal{F}(P)} \operatorname{relint} f$. For them the following property, which follows from (i)–(iv), is an elementary theorem:
(v) if $e \in \Gamma^i$ and $e' \in \Gamma^{i-2}$ is a face of e, then there exist exactly two cells e_1, $e_2 \in \Gamma^{i-1}$ such that e_j is a face of e and e' is a face of e_j.

Let us say that ε is an *incidence function* on Γ if the following conditions are satisfied:
(a) to each pair (e, e') such that $e \in \Gamma^i$ and $e' \in \Gamma^{i-1}$ for some $i \geq 0$, ε assigns a number $\varepsilon(e, e') \in \{0, \pm 1\}$;
(b) $\varepsilon(e, e') \neq 0 \iff e'$ is a face of e;
(c) $\varepsilon(e, \emptyset) = 1$ for all 0-cells e;
(d) if $e \in \Gamma^i$ and $e' \in \Gamma^{i-2}$ is a face of e, then

$$\varepsilon(e, e_1)\varepsilon(e_1, e') + \varepsilon(e, e_2)\varepsilon(e_2, e') = 0$$

where e_1 and e_2 are those $(i-1)$-cells such that e_j is a face of e and e' is a face of e_j (see (v) above).

Lemma 5.6. *Let Γ be a cell complex. Then there exists an incidence function on Γ.*

For a proof see [22] where the incidence numbers $\varepsilon(e, e')$ appear as topological data determined by orientations of the cells. Figure 5.1 indicates two incidence functions on the solid rectangle and how they are induced by orientations.

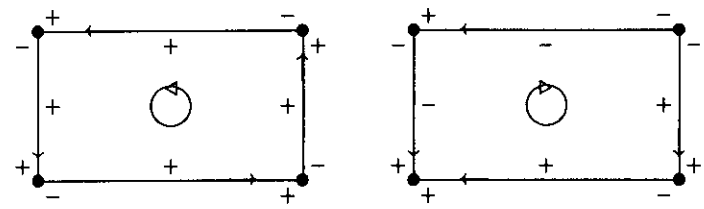

Figure 5.1

Let Γ be a cell complex of dimension $d-1$, and ε an incidence function on Γ. We define the *augmented oriented chain complex* of Γ to be the complex

$$\tilde{C}(\Gamma)\colon 0 \longrightarrow C_{d-1} \xrightarrow{\partial} C_{d-2} \longrightarrow \cdots \longrightarrow C_0 \xrightarrow{\partial} C_{-1} \longrightarrow 0$$

where

$$C_i = \bigoplus_{e \in \Gamma^i} \mathbb{Z}e \qquad \text{and} \qquad \partial(e) = \sum_{e' \in \Gamma^{i-1}} \varepsilon(e, e')e' \quad \text{for } e \in \Gamma^i,$$

$i = 0, \ldots, d-1$. That $\partial^2 = 0$ follows from the definition of an incidence function and property (v) of cell complexes. (The notation $\tilde{C}(\Gamma)$ is justified since the dependence of $\tilde{C}(\Gamma)$ on ε is inessential.) For simplicity of notation we set $\widetilde{H}_i(\Gamma) = H_i(\tilde{C}(\Gamma))$.

The fundamental importance of $\tilde{C}(\Gamma)$ in algebraic topology relies on the fact that it computes reduced singular homology:

Theorem 5.7. *Let Γ be a cell complex. Then $\widetilde{H}_i(\Gamma) = \widetilde{H}_i(|\Gamma|)$ for all $i \geq 0$ (and $\widetilde{H}_{-1}(\Gamma) = 0$).*

We use 5.7 via the following corollary:

Corollary 5.8. *Let Γ be a cell complex such that $|\Gamma|$ is homeomorphic to a closed ball B^n. Then $\widetilde{H}_i(\Gamma) = 0$ for all $i \geq -1$.*

Local cohomology. From now on D is a positive cone. By d we denote the rank of C. Recall that d equals the Krull dimension of $R = K[C]$.

We choose an admissible grading on $K[C]$. Independently of this choice, the ideal $\mathfrak{m}$ in $R = K[C]$ generated by the elements X^c, $c \in C \setminus \{0\}$, is the irrelevant maximal ideal. We want to construct a complex 'computing' $H^i_{\mathfrak{m}}(M)$ that resembles the combinatorial structure of D as closely as possible.

Fix a cross-section T of D, and let $\mathcal{F} = \mathcal{F}(T)$ be its face lattice, which we consider as a caell complex. We denote a face of D and its intersection with T by corresponding capital and small letters. Let F be a face of D. Then we set

$$R_F = R_{\{X^z\colon\, z \in C \cap F\}};$$

that is, we form the ring of fractions of R whose denominators are the monomials in $\{X^z\colon z \in C \cap F\}$. In particular, $R_D = K[\mathbb{Z}C]$ is the algebra generated by all monomials X^z where z belongs to the group $\mathbb{Z}C$ generated by C. Let

$$L^t = \bigoplus_{f \in \mathcal{F}^{t-1}} R_F, \qquad t = 0, \ldots, d,$$

and define $\partial\colon L^{t-1} \to L^t$ by specifying its component

$$\partial_{f',f}\colon R_{F'} \to R_F \qquad \text{to be} \quad \begin{cases} 0 & \text{if } F' \not\subset F, \\ \varepsilon(f,f')\,\text{nat} & \text{if } F' \subset F; \end{cases}$$

here ε is an incidence function on $\mathcal{F}$. It is clear that

$$L^\bullet\colon 0 \longrightarrow L^0 \xrightarrow{\partial} L^1 \longrightarrow \cdots \longrightarrow L^{d-1} \xrightarrow{\partial} L^d \longrightarrow 0$$

is a complex. In the special case $D = \mathbb{R}^n_+$, $K[C] = K[X_1, \ldots, X_n]$ we have seen it already: it is (up to the choice of the incidence function) the complex $C^\bullet$ of local cohomology. That $L^\bullet$ is exactly what we want, is shown by the next theorem.

Theorem 5.9. *For every $K[C]$-module M, and all $i \geq 0$,*

$$H^i_{\mathfrak{m}}(M) \cong H^i(L^\bullet \otimes M).$$

The first step in proving the theorem is the verification of the equation $H^0(L^0 \otimes M) = H^0_{\mathfrak{m}}(M)$. This amounts to the fact that the ideal generated by the monomials X^z contained in the 1-faces of D (i.e. the extremal rays of D) generate an $\mathfrak{m}$-primary ideal. This is true because their exponents z generate the cone D.

Now let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of $K[C]$-modules. Since all the summands of $L^\bullet$ are flat $K[C]$-modules, this yields an exact sequence

$$0 \to L^\bullet \otimes M_1 \to L^\bullet \otimes M_2 \to L^\bullet \otimes M_3 \to 0.$$

Therefore we have a long exact sequence

$$\cdots \to H^i(L^\bullet \otimes M_1) \to H^i(L^\bullet \otimes M_2) \to H^i(L^\bullet \otimes M_3) \to H^{i+1}(L^\bullet \otimes M_1) \to \cdots$$

Finally we must show that $H^i(L^\bullet \otimes M) = 0$ for all i if M is an injective $K[C]$-module. It suffices to consider the indecomposable modules $E(R/\mathfrak{p})$ where $\mathfrak{p}$ is a prime ideal of $R = K[C]$. (Each injective $K[C]$-module is the direct sum of indecomposables, and each indecomposable injective module is the injective hull of a residue class ring $R/\mathfrak{p}$.) Let G be the face of D such that $\mathfrak{P}(G)$ is the C-graded prime ideal generated by all the monomials in $\mathfrak{p}$. Let $\mathcal{G} = \mathcal{F}(g)$ denote the face lattice of the face $g = G \cap T$ of a cross-section T of D. The crucial point of the proof is that

$$L^\bullet \otimes E(R/\mathfrak{p}) \cong \operatorname{Hom}_{\mathbb{Z}}\big(\tilde{C}(\mathcal{G})(-1),\ E(R/\mathfrak{p})\big).$$

(As for graded modules, -1 denotes a shift.) Since g is a convex polytope, it is homeomorphic to a closed ball. So $\tilde{C}(\mathcal{G})$ is an exact complex. Since $\tilde{C}(\mathcal{G})$ is a complex of free $\mathbb{Z}$-modules, exactness is preserved in $\operatorname{Hom}_{\mathbb{Z}}(\tilde{C}(\mathcal{G})(-1),\ E(R/\mathfrak{p}))$.

Cohen–Macaulay property and canonical module. The modules L^i appearing in the complex $L^\bullet$ are direct sums

$$L^i = \bigoplus_{z \in \mathbb{Z}^n} (L^i)_z,$$

$(L_i)z$ being spanned by the copies of the monomial of X^z appearing in the direct summands R_F. The maps of $L^\bullet$ respect this decomposition, and in order to compute its cohomology we analyze each components $(L^\bullet)_z$. Given $z \in \mathbb{Z}^n$, the crucial point is to determine those faces F of D for which $(R_F)_z \neq 0$. As we shall see, this is the case if and only if the face F is not 'visible' from z.

Let P be a polyhedron in a $\mathbb{R}$-vector space V. Let $x, y \in V$. We say that y is *visible* from x if $y \neq x$ and the line segment $[x, y]$ does not contain a point $y' \in P$, $y' \neq y$. A subset $S \subset V$ is *visible* if each $v \in S$ is visible.

Proposition 5.10. *Let P be a polytope in $\mathbb{R}^n$ with face lattice $\mathcal{F}$, and $x \in \mathbb{R}^n$ a point outside P. Set $\mathcal{S} = \{F \in \mathcal{F}: F \text{ visible from } x\}$. Then $\mathcal{S}$ is a subcomplex of $\mathcal{F}$; its underlying space $S = \bigcup_{F \in \mathcal{S}} F$ is the set of points $y \in P$ which are visible from x, and is homeomorphic to a closed ball.*

Just look at a polytope if you don't believe the proposition. Figure 5.2 illustrates the following lemma. Let $C = \mathbb{N}^2 \subset \mathbb{R}^2$, and F be the positive X-axis, G the positive Y-axis. Then $K[C]_F = K[X, Y, X^{-1}]$, and $(K[C]_F)_z \neq 0$ for $z \notin C$ exactly when z is in the second quadrant (including the negative X-axis). Thus $(K[C]_F)_z \neq 0$ if and only if F is not visible from z. Similar arguments work for the faces $\{0\}$, G, and C.

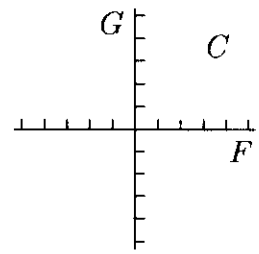

Figure 5.2

Lemma 5.11. *$(R_F)_z \neq 0$ (and therefore $(R_F)_z \cong K$) if and only if F is not visible from z.*

Now we can describe the cohomology of $L^\bullet$. In order to have a compact notation, we set $\operatorname{relint} C = C \cap \operatorname{relint} D$, and $\operatorname{relint}(-C) = \mathbb{Z}^n \cap \operatorname{relint}(-D)$. Then, with a self-explaining notation, $\operatorname{relint}(-C) = -\operatorname{relint} C$.

Theorem 5.12. (a) *If $z \in \operatorname{relint}(-C)$, then $(L^\bullet)_z$ is isomorphic to $0 \to K \to 0$ with K in homological degree d. Consequently $H^i(L^\bullet)_z = 0$ for $i \neq d$, and $H^d(L^\bullet)_z \cong K \cong (L^\bullet)_z$.*

(b) *Suppose that $z \notin \operatorname{relint}(-C)$. Let T be a cross-section of D with face lattice $\mathcal{F}$, and $\mathcal{S} = \{F \cap T: F \subset \mathcal{F}(D) \text{ visible from } z\}$. Then*

(i) $(L^\bullet)_z \cong \operatorname{Hom}_{\mathbb{Z}}\big((\tilde{C}(\mathcal{F})/\tilde{C}(\mathcal{S}))(-1),\ K\big)$,

(ii) $\widetilde{H}_i(\mathcal{F}) = \widetilde{H}_i(\mathcal{S}) = 0$ *for all* i,

(iii) $(H^i(L^\bullet))_z = 0$ *for all* i.

Part (a) is easy to see: for $z \in \operatorname{relint}(-C)$ one has $z \in R_F$ if and only if $F = D$. (With some justification, one can call $\operatorname{relint} D$ the *voyeur space* relative to D: from every point of it one can see every point of $D \setminus \operatorname{relint} D$.) The rest requires a careful discussion based on 5.10 and 5.11.

The previous theorem allows us not only to show that normal semigroup rings are Cohen–Macaulay, but also to determine their canonical modules.

Theorem 5.13. (a) (Hochster) $R = K[C]$ *is a Cohen–Macaulay ring, and*
(b) (Danilov, Stanley) *the ideal* I *generated by the monomials* X^c *with* $c \in \operatorname{relint} C$ *is the graded canonical module of* $K[C]$ *(with respect to any admissible grading).*

In fact, we have $H^i_{\mathfrak{m}}(R) = 0$ for $i = 0, \ldots, d-1$ by 5.9 and 5.12. Therefore $\operatorname{depth} R = d$ by 1.20, and it follows that R is Cohen–Macaulay.

For (b) one first shows that $I^\vee$ is isomorphic as an R-module to $K[\mathbb{Z}C]/U$ where the submodule(!) U is the K-vector subspace spanned by all the monomials X^z, $z \in \mathbb{Z}C$, $z \notin \operatorname{relint}(-C)$. Thus $I^\vee \cong H^d_{\mathfrak{m}}(R)$, and local duality implies $I \cong \omega_R$.

Corollary 5.14. $K[C]$ *is Gorenstein if and only if there exists* $c \in \operatorname{relint} C$ *with* $\operatorname{relint} C = c + C$.

One must only check that I is a principal ideal if and only if it is generated by a monomial.

Combinatorial applications. One of the most beautiful combinatorial applications of commutative algebra is the study of the Ehrhart function of a convex polytope. The Ehrhart function counts the lattice points in a polytope and all its multiples, i.e. its images under the maps $x \mapsto mx$, $M \in \mathbb{N}$.

Let $P \subset \mathbb{R}^n$ be a polytope of dimension d. Since P is bounded, we may define its *Ehrhart function* by

$$E(P,m) = |\{z \in \mathbb{Z}^n \colon \frac{z}{m} \in P\}|, \quad m \in \mathbb{N},\ m > 0, \quad \text{and} \quad E(P,0) = 1.$$

and its *Ehrhart series* by

$$E_P(t) = \sum_{m \in \mathbb{N}} E(P,m) t^m.$$

It is clear that $E(P,m) = |\{z \in \mathbb{Z}^n \colon z \in mP\}|$ where $mP = \{mp \colon p \in P\}$. Similarly as above we set

$$E^+(P,m) = |\{z \in \mathbb{Z}^n \colon \frac{z}{m} \in \operatorname{relint} P\}| \quad \text{for } m > 0, \quad E^+(P,0) = 0,$$

and

$$E_P^+(t) = \sum_{m \in \mathbb{N}} E^+(P,m)t^m.$$

Note that $E^+(P,m) = |\{z \in \mathbb{Z}^n : z \in \operatorname{relint} mP\}|$ for $m > 0$.

We define the cone $D \subset \mathbb{R}^{n+1}$ by $D = \mathbb{R}_+\{(p,1) : p \in P\}$. Then $C = D \cap \mathbb{Z}^{n+1}$ is a subsemigroup of $\mathbb{Z}^{n+1}$. Therefore one may consider the k-algebra $k[C]$. Suppose P is a rational polytope, i.e. the convex hull of fintely many points with rational coordinates. Then D is a finitely generated rational cone, and $K[C]$ is a normal semigroup ring. Let us fix a grading on $k[C]$ by assigning to $c = (c_1, \ldots, c_{d+1})$ the degree c_{d+1}. For this grading the Hilbert functions of $k[C]$ and of the ideal I generated by the monomials X^c, $x \in \operatorname{relint} C$, are given by

$$H(k[C],m) = E(P,m) \quad \text{and} \quad H(I,m) = E^+(P,m).$$

The grading under consideration is admissible for $k[C]$, and therefore we may apply our previous results. Part (b) of the following theorem is Ehrhart's remarkable reciprocity law for rational polytopes.

Theorem 5.15 (Ehrhart). *Let $P \subset \mathbb{R}^n$ be a d-dimensional rational polytope, $d > 0$. Then*
(a) *$E_P(t)$ is a rational function, and there exists a quasi-polynomial q with $E(P,m) = q(m)$ for all $m \geq 0$;*
(b) *$E_P^+(t) = (-1)^{d+1}E_P(t^{-1})$, equivalently*

$$E^+(P,m) = (-1)^d E(P,-m) \qquad \text{for all} \quad m \geq 1$$

where $E(P,-m) = q(-m)$ is the natural extension of $E(P,\_)$.

(a) Since $E_P(t)$ is the Hilbert series of a positively graded Noetherian k-algebra, it is a rational function. According to 2.4 we must show for the second statement in (a) that $E_P(t)$ has negative degree, or, equivalently, that the a-invariant of $k[C]$ is negative. By 5.13 the ring $k[C]$ is Cohen–Macaulay, and its graded canonical module is generated by the elements X^c, $c \in \operatorname{relint} C$. These have positive degrees under the grading of $k[C]$, and hence $a(k[C]) < 0$.

(b) By what has just been said, $E_P^+(t)$ is the Hilbert series of the canonical module of $k[C]$. Furthermore, $\dim k[C] = d+1$. Thus the first equation is a special case of 3.12. The second equation results from $\sum_{m \geq 1} E(P,-m)t^m = -E_P(t^{-1})$. (The reader may prove this identity as an exercise.)

The quasi-polynomial q in 5.15 is called the *Ehrhart quasi-polynomial of P*.

Suppose that P is even an *integral* polytope, that is, a polytope whose vertex set V is contained in $\mathbb{Z}^n$. Then, in addition to $k[C]$, we may also consider its subalgebra

$$k[V] = k[X^{(v,1)} : v \in V].$$

Obviously $k[V]$ is a homogeneous k-algebra. Let $c \in C$; then there exist $q_v \in \mathbb{Q}_+$ such that $c = \sum_{v \in V} q_v v$. If we multiply this equation by a suitable common denominator e

and interpret the result in terms of monomials, then we see that $(X^c)^e \in k[V]$. Thus $k[C]$ is integral over $k[V]$. Since it is also a finitely generated $k[V]$-algebra, it is even a finite $k[V]$-module. Thus $K[C]$ is almost homogeneous. In particular the Ehrhart quasi-polynomial of P is a polynomial and therefore called the *Ehrhart polynomial.* Furthermore $k[C]$ has a well defined h-vector, which one calls the h-vector of P, and a well-defined multiplicity. The multiplicity of $K[C]$ is an elementary geometric invariant of P.

Theorem 5.16. *Let $P \subset \mathbb{R}^n$ be an n-dimensional integral polytope, and let $k[C]$ the normal semigroup ring constructed above. Then*

$$e(k[C]) = n! \text{ vol } P.$$

Elementary arguments of measure theory show that the volume of P is

$$\text{vol } P = \lim_{m\to\infty} \frac{E(P,m)}{m^n}.$$

Being the Hilbert polynomial of a $(n+1)$-dimensional $k[V]$-module, $E(P,m)$ has degree n. Thus its leading coefficient is given by vol P. On the other hand, it is also given by $e(k[C])/n!$.

The restriction to n-dimensional polytopes $P \subset \mathbb{R}^n$ is only for simplicity; see [30], Section 4.6, for the general case. Using the fact that the volume of P is the leading coefficient of its Ehrhart polynomial one can derive classical formulas for vol P. For example,

$$\text{vol } P = \frac{1}{2}(E(P,1) + E^+(P,1) - 2) \qquad \text{for } n = 2, \text{ and}$$

$$\text{vol } P = \frac{1}{6}(E(P,2) - 3E(P,1) - E^+(P,1) + 3) \qquad \text{for } n = 3.$$

For the polytope P of figure 5.3 we obtain the following numerical data:

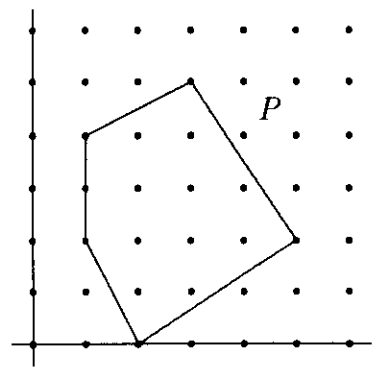

Figure 5.3

$$E(P,1) = 16, \quad E^+(P,1) = 10, \quad E(P,n) = 12n^2 + 3n + 1 \quad \text{vol}(P) = 12.$$

The h-vector of an integral polytope P is subject to the following restraints.

Theorem 5.17. *Let P be an integral polytope. Then*
(a) $h_i \geq 0$ *for all* i; $h_i = 0$ *for* $i < 0$ *and* $i > d$;
(b) (Stanley) $\sum_{i=0}^{j} h_i \leq \sum_{i=0}^{j} h_{s-i}$ *for all* $j = 0, \ldots, s$ *where* $s = \max\{i\colon h_i \neq 0\}$;
(c) (Hibi) $\sum_{i=d-j}^{d} h_i \leq \sum_{i=0}^{j+1} h_i$ *for all* $j = 0, \ldots, d$.

Part (a) follows from the facts that $K[C]_i = 0$ for $i < 0$ and that the a-invariant of $K[C]$ is negative. The inequality in (b) is an immediate consequence of 3.13. For (c) one uses that, according to 5.13 and with its notation, there is an exact sequence $0 \to \omega_R \to R \to R/I \to 0$; then one applies 2.11 to R/I.

6 Walks in directed graphs

In this section we want to investigate generating functions defined by the walks in a directed graph. The material below is much more elementary than that of the preceding sections since we will only use the relationship between the Poincaré biseries of a module, its Hilbert series and that of the underlying K-algebra R.

Let us first remark that the commutativity of R is not crucial for the validity of the equation

$$(*) \qquad H_M(t) = H_R(t) \cdot P_M(t, -1).$$

This is crucial for us since there is no reasonable way to work in a commutative setting below. (The only exception is that of a directed graph representing a partial order on its set of vertices: then we may choose R as the Stanley–Reisner ring of the corresponding simplicial complex.)

A directed graph G on the vertex set V is a subset of $V \times V$; we always assume V is finite. We want to study the numerical function counting the walks $(v_1, v_2, \ldots, v_n)$ in G, i.e. such sequences satisfying the condition $(v_i, v_{i+1}) \in G$. We call n the *degree* of the walk, and denote the number of degree n walks in G by $\chi_n(G)$; by convention, $\chi_0(G) = 1$. The generating function of $\chi_n(G)$ is

$$H_G(t) = \sum_{n=0}^{\infty} \chi_n(G) t^n.$$

Figure 6.1 shows a graph and its complementary graph $\bar{G} = (V \times V) \setminus G$. We have

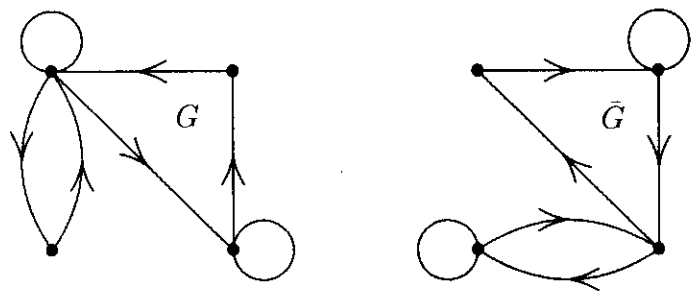

Figure 6.1

$H_G(t) = 1 + 4t + 7t^2 + 15t^3 + 30t^4 + \cdots$ and $H_{\bar{G}}(t) = 1 + 4t + 9t^2 + 23t^3 + 59t^4 + \cdots$ so that $H_G(t) H_{\bar{G}}(-t) = 1 + \textit{terms of degree} \geq 5$. It would be an incredible accident, if this equation were not a special case of a general theorem. Indeed, it is.

Theorem 6.1 (Carlitz–Scoville–Vaughan). $H_G(t)H_{\bar{G}}(-t) = 1$, *where* $\bar{G} = (V \times V) \setminus G$ *is the graph complementary to* G.

We prove 6.1 in a refined version. For a subset W of V let $\chi_n(G, \bar{W})$ the number of degree n walks in G starting in $\bar{W} = V \setminus W$, and $\chi_n(\bar{G}, W)$ the number of degree n walks in $\bar{G}$ starting in W (with the same convention for $n = 0$ as above). We introduce the corresponding generating functions

$$H_{\bar{W}}(t) = \sum_{n=0}^{\infty} \chi_n(G, \bar{W})t^n, \quad \text{and} \quad \bar{H}_W(t) = \sum_{n=0}^{\infty} \chi_n(\bar{G}, W)t^n.$$

Theorem 6.2 (Gessel). *With the notation just introduced,* $H_{\bar{W}}(t) = \bar{H}_W(-t)H_G(t)$, *equivalently*

$$\chi_n(G, \bar{W}) = \sum_{i=0}^{n} (-1)^i \chi_i(\bar{G}, W)\chi_{n-i}(G) \qquad \textit{for all} \quad n \in \mathbb{N}.$$

We want to derive 6.2 as a special instance of $(*)$. Let us first note that $(*)$ simplifies considerably if the free resolution is linear, i.e. it has the form

$$F_\bullet\colon \cdots \longrightarrow R(-i)^{\beta_i} \longrightarrow R(-(i-1))^{\beta_{i-1}} \longrightarrow \cdots \longrightarrow R^{\beta_0};$$

Then $P_{F_\bullet}(t, -1) = \sum_{i=0}^{\infty} \beta_i(-t)^i$.

One almost immediately associates sequences of vertices with sequences of indeterminates. However, since we cannot permute the vertices in a walk, we are forced to work with non-commuting indeterminates. This makes the algebra more cumbersome – we must strictly distinguish between 'left' and 'right', but simplifies the combinatorics tremendously.

So, let $K\langle G\rangle$ be the residue class algebra of the free K-algebra $K\langle V\rangle$ on V modulo the two-sided ideal $\mathfrak{a}$ generated by the products vv' for which $(v, v') \notin G$ (for simplicity we identify a vertex and its corresponding variable), and set $A = K\langle G\rangle$. It is clear that $H_G(t)$ is the Hilbert series of A: the monomials (in non-commuting variables) which form a K-basis of A are presented by the walks in G. Now we choose I as the right ideal generated by the elements $w \in W$. The monomials whose leftmost factor belongs to W form a K-basis of I, and so the residue classes of those monomials whose leftmost factor is outside W form a K-basis of the right A-module A/I. Thus $H_{\bar{W}}(t)$ is the Hilbert series of A/I.

We start the free resolution of A/I with the natural choice $F_0 = A$. Next let $F_1 = A^{(W)}$ be a free right A-module with basis e_w, $w \in W$. Then the assignment $e_w \mapsto w$ induces a homomorphism $\varphi_1\colon F_1 \to F_0$ with $\operatorname{Im}\varphi_1 = I$. Note that $I = \bigoplus_{w \in W} wA$. Thus $\operatorname{Ker}\varphi_1 = \bigoplus_{w \in W} e_w \operatorname{Ann} w$. Obviously $\operatorname{Ann} w$ is the right ideal generated by those $v \in V$ for which $wv \in \mathfrak{a}$, equivalently, for which $(w, v) \in \bar{G}$.

Applying the same argument to each of $\operatorname{Ann} w$ in place of I and iterating the procedure, we obtain a linear free resolution of A/I in which the basis of F_j corresponds bijectively to the walks $v_1, \ldots, v_j$ in $\bar{G}$ that start from a vertex $v_1 \in W$.

Corollary 6.3. *The following are equivalent:*
(()a) K has finite projective dimension over $K\langle G\rangle$;
(()b) $\bar{G}$ contains no cycles;
(()c) $H_G(t)^{-1}$ is a polynomial.

A proof by linear algebra. We would like to present another proof of 6.2 which uses the *transfer matrix* T of the graph G (over the real numbers $\mathbb{R}$). In order to define T we enumerate the vertices $v_1, \ldots, v_m \in V$. Then $T_{ij} = 1$ if $(v_i, v_j) \in G$, and $T_{ij} = 0$ otherwise. Let $\bar{T}$ be the transfer matrix of $\bar{G}$; then $E = T + \bar{T}$ is the matrix with all entries equal to 1. For a subset $W \subset V$ we define its *indicator* e_W as the *row* vector whose i-th component is 1 if $v_i \in W$, and 0 otherwise. It follows immediately by induction that for $n \geq 1$ the number of degree n walks starting from a vertex in a subset $X \subset V$ and ending in a vertex belonging to $Y \subset V$ is

$$\langle e_X T^{n-1}, e_Y \rangle$$

where $\langle \_, \_ \rangle$ denotes the standard scalar product in $\mathbb{R}^m$. In particular, the j-th component of $e_X T^{n-1}$ is the number of degree n walks starting in a vertex $v \in X$ and ending in v_j. The generating function $H_G(t)$ above can be written

$$H_G(t) = 1 + \sum_{n=1}^{\infty} \langle e_V T^{n-1}, e_V \rangle t^n.$$

Furthermore, if we set $\lambda(y) = \langle y, e_V \rangle$, $\tau(y) = yT$, $\varepsilon(y) = yE$, and $\bar{\tau}(y) = (\varepsilon - \tau)(y)$, then the equation for $\chi_n(G, \bar{W})$ in 3.1 reads

$$\lambda(\tau^{n-1}(e_{\bar{W}})) = \lambda(\tau^{n-1}(e_V)) + \sum_{i=1}^{n-1} (-1)^i \lambda(\bar{\tau}^{i-1}(e_W)) \lambda(\tau^{n-i-1}(e_V)) + (-1)^n \lambda(\bar{\tau}^{n-1}(e_W)).$$

The following lemma will show that one has an even stronger equation.

Lemma 6.4. *Let M be a left module over some ring R, $\tau \colon M \to M$ an endomorphism, $e \in M$, and $\lambda \colon M \to R$ an arbitrary map. We define $\varepsilon \colon M \to M$ by $\varepsilon(x) = \lambda(x)e$. Then*

$$(\tau - \varepsilon)^n(y) = \tau^n(y) - \sum_{i=1}^{n} \lambda\Big((\tau - \varepsilon)^{n-i}(y)\Big) \tau^{i-1}(e)$$

for all $x \in M$ and $n \in \mathbb{N}$.

One goes by induction on n. For the induction step one writes $(\tau - \varepsilon)^{n+1}(y) = (\tau - \varepsilon)((\tau - \varepsilon)^n(y))$, applies the induction hypothesis, and uses the definition of ε.

We apply the lemma to the maps introduced above. Note that indeed $\varepsilon(x) = \lambda(x)e_V$. Since λ is now linear, we obtain from the lemma with $y = e_W = e_V - e_{\bar{W}}$ that

$$(-1)^n \bar{\tau}^n(e_W) = \tau^n(e_V - e_{\bar{W}}) - \sum_{i=1}^{n} (-1)^{n-i} \lambda\Big(\bar{\tau}^{n-i}(e_W)\Big) \tau^{i-1}(e_V).$$

Solving for $\tau^n(e_{\bar{W}})$ yields

$$\tau^n(e_{\bar{W}}) = (-1)^{n+1}\bar{\tau}^n(e_W) + \sum_{i=1}^{n}(-1)^{n+1-i}\lambda\Big(\bar{\tau}^{n-i}(e_W)\Big)\tau^{i-1}(e_V) + \tau^n(e_V).$$

The j-th component of $\tau^n(e_{\bar{W}})$ is the number $\chi_{n+1}^{(j)}(G,\bar{W})$ of degree $n+1$ walks in G which start in $\bar{W}$ and end in the vertex v_j. If we modify the remaining notation accordingly, then we get a vectorial refinement of the second equation in 6.2 (we have replaced n by $n-1$ and i by $n-i$):

Theorem 6.5. *With the notation introduced,*

$$\chi_n^{(j)}(G,\bar{W}) = \sum_{i=0}^{n-1}(-1)^i\chi_i(\bar{G},W)\chi_{n-i}^{(j)}(G) \;+\; (-1)^n\chi_n^{(j)}(\bar{G},W) \qquad \textit{for} \quad n \geq 1.$$

To obtain 6.2, simply sum the equations in 6.5 over j. The question arises whether one can prove 6.5 homologically. This is indeed possible, and the homological approach explains the structure of the formula very well.

Let $A = K\langle G\rangle$. We observed in the proof of 6.2 that the maps in the free resolution $F_\bullet$ of A/I are composed of homomorphisms $A \to A$, $1 \mapsto w$, of right A-modules. But such a homomorphism is left multiplication by w, and left multiplication maps a left ideal into itself. This observation is the starting point for a decomposition of $F_\bullet$ that yields the formula in 6.5.

Let $A^{(j)} = Av_j$ be the *left* ideal of A generated by v_j. Then one has a decomposition $A = K \oplus \bigoplus_{j=1}^m A^{(j)}$ of K-vector spaces. Writing the free A-modules F_i in $F_\bullet$ as a direct sum of copies of A, namely $F_i = A^{\beta_i}$ with $\beta_i = \chi_i(\bar{G},W)$, one may similarly decompose F_i as

$$F_i = K^{\beta_i} \oplus \bigoplus_{j=1}^{m}(A^{(j)})^{\beta_i}.$$

Furthermore, for $i \geq 1$ we split the direct summand K^{β_i} into the direct sum

$$\bigoplus_{j=1}^{m} K^{\chi_i^{(j)}(\bar{G},W)}$$

where for each j we have collected the subspaces eK with base elements e of F_i corresponding to those direct summands A on which the map to a component of F_{i-1} is left multiplication by v_j. Finally we set $F_i^{(j)} = K^{\chi_i^{(j)}(\bar{G},W)} \oplus (A^{(j)})^{\beta_i}$ for $i \geq 1$, and $F_0^{(j)} = A^{(j)}$.

These decompositions are compatible with the grading of $F_\bullet$ and furthermore they even split $F_\bullet$ into a direct sum of complexes, since $F_i^{(j)}$ is mapped into $F_{i-1}^{(j)}$: the maps $A \to A$ which occur in $F_\bullet$ are left multiplications by an element $w \in V$

or 0. Taking both decompositions simultaneously we obtain an acyclic complex of K-vector spaces

$$0 \to (F_n^j)_n \longrightarrow (F_{n-1}^j)_n \longrightarrow \ldots \longrightarrow (F_1^j)_n \longrightarrow (F_0^j)_n$$

for each $n \geq 1$. Its Euler characteristic is the right hand side of the formula in 6.5 and the degree n piece of its homology is the vector space generated by all degree n monomials in A/I which end in v_j.

Remarks. The material of this section has been taken from Bruns–Herzog–Vetter [2], which furthermore contains some extensions of 6.2. Kobayashi [21] used a similar approach towards proving combinatorial identities. Fröberg [6] showed that the residue class algebras of a free algebra with respect to certain classes of homogeneous relations of degree 2 are Koszul algebras (i.e. K has a linear resolution). In the case $W = V$ the resolution in the proof of 6.2 is a (very simple) special case of Fröberg's construction, which gives the base elements in a free resolution as monomials in 'complementary' variables modulo 'complementary' relations.

References

1. W. Bruns and J. Herzog. *Cohen–Macaulay rings.* Cambridge University Press, 1993.
2. W. Bruns, J. Herzog and U. Vetter. Syzygies and walks. In *Proceedings of the workshop on commutative algebra, ICTP, Trieste, 1992.* World Sci. Publishing (to appear).
3. L. Carlitz, R. Scoville, and T. Vaughan. Enumeration of pairs of sequences by rises, falls and levels. *Manuscr. Math.* **19** (1976), 211–243.
4. V. I. Danilov. The geometry of toric varieties. *Russian Math. Surveys* **33** (1978), 97–154.
5. E. Ehrhart. *Polynômes arithméthiques et méthode des polyédres en combinatoire.* Birkhäuser, 1977.
6. R. Fröberg. Determination of a class of Poincaré series. *Math. Scand.* **37** (1975), 29–39.
7. I. Gessel. *Generating functions and enumeration of sequences.* Ph. D. Thesis, Massachussetts Institute of Technology, 1977
8. N. L. Gordeev. Finite groups whose algebras of invariants are complete intersections. *Math. USSR-Izv.* **28** (1987), 335–3379.
9. S. Goto and K. Watanabe. On graded rings, I. *J. Math. Soc. Japan* **30** (1978), 179–213.
10. S. Goto and K. Watanabe. On graded rings, II ($\mathbb{Z}^n$-graded rings). *Tokyo J. Math.* **1** (1978), 237–261.
11. T. Hibi. Distributive lattices, affine semigroup rings, and algebras with straightening laws. In M. Nagata and H. Matsumura (eds.), *Commutative algebra and combinatorics.* Advanced Studies in Pure Math. **11**, North–Holland, 1987, pp. 93–109.
12. T. Hibi. Ehrhart polynomials of convex polytopes, h-vectors of simplicial complexes, and nonsingular projective toric varieties. In J. E. Goodman, R. Pollack, and W. Steiger (eds.), *Discrete and computational geometry.* DIMACS Series **6**, Amer. Math. Soc., 1991, pp. 165–177.
13. T. Hibi. *Algebraic combinatorics on convex polytopes.* Carslaw Publications, 1992.
14. V. A. Hinič. On the Gorenstein property of the ring of invariants. *Math. USSR-Izv.* **10** (1976), .
15. M. Hochster. Rings of invariants of tori, Cohen–Macaulay rings generated by monomials, and polytopes. *Ann. of Math.* **96** (1972), 318–337.
16. M. Hochster. Invariant theory of commutative rings. In S. Montgomery (ed.), *Group actions on rings.* Contemp. Math. **43**, Amer. Math. Soc., 1985, pp. 161–179.
17. M. Hochster and J. A. Eagon. Cohen–Macaulay rings, invariant theory, and the generic perfection of determinantal loci. *Amer. J. Math.* **93** (1971), 1020–1058.

18. M.-N. ISHIDA. The local cohomology groups of an affine semigroup ring. In H. HIJIKATA ET AL. (eds.), *Algebraic geometry and commutative algebra in honor of Masayoshi Nagata. Vol. I.* Konikuniya, 1987, pp. 141–153.
19. V. KAC AND K. WATANABE. Finite linear groups whose ring of invariants is a complete intersection. *Bull. Amer. Math. Soc.* **6** (1982), 221–223.
20. F. KNOP. Der kanonische Modul eines Invariantenringes. *J. Algebra* **127** (1989), 40–54.
21. Y. KOBAYASHI Partial commutation, homology, and the Möbius inversion formula. In *Words, languages, and combinatorics (Kyoto 1990).* World Sci. Publishing, 1992, pp. 288–298
22. W. S. MASSEY. *Singular homology theory.* Springer, 1980.
23. H. NAKAJIMA. Affine torus embeddings which are complete intersections. *Tôhoku Math. J.* **38** (1986), 85–98.
24. H. NAKAJIMA AND K. WATANABE. The classification of quotient singularities which are complete intersections. In S. GRECO AND R. STRANO (eds.), *Complete intersections, Acireale 1983.* LNM **1092**, Springer, 1984, pp. 102–120.
25. T. ODA. *Convex bodies and algebraic geometry.* Springer, 1985.
26. U. SCHÄFER AND P. SCHENZEL. Dualizing complexes and affine semigroup rings. *Trans. Amer. Math. Soc.* **322** (1990), 561–582.
27. R. P. STANLEY. Hilbert functions of graded algebras. *Adv. in Math.* **28** (1978), 57–83.
28. R. P. STANLEY. Invariants of finite groups and their applications to combinatorics. *Bull. Amer. Math. Soc.* **1** (1979), 475–511.
29. R. P. STANLEY. *Combinatorics and commutative algebra.* Birkhäuser, 1983.
30. R. P. STANLEY. *Enumerative combinatorics, Vol. I.* Wadsworth & Brooks/Cole, 1986.
31. R. P. STANLEY. On the Hilbert function of a graded Cohen–Macaulay domain. *J. Pure Applied Algebra* **73** (1991), 307–314.
32. K. WATANABE. Certain invariant subrings are Gorenstein. I. *Osaka J. Math.* **11** (1974), 1–8.
33. K. WATANABE. Certain invariant subrings are Gorenstein. II. *Osaka J. Math.* **11** (1974), 379–388.