NORMAL SEMIGROUP RINGS

WINFRIED BRUNS

Introduction

The rings that from an algebraic point of view are classified as normal semigroup rings are the coordinate rings of affine toric varieties, i.e. the algebras generated by the semigroups $D \cap \mathbb{Z}^n$ where D is a finitely generated rational cone in $\mathbb{R}^n$. Since toric varieties are constructed by glueing affine toric varieties, the theory of normal semigroup rings covers all the local properties of toric varieties. They also appear in the global theory as the homogeneous coordinate rings of projective toric varieties.

A major result (see Section 3) on normal semigroup rings is Hochster's theorem saying that they are Cohen–Macaulay rings. We approach it by constructing a complex 'computing' local cohomology; our construction is natural in the sense that it uses the cell decomposition of a cross-section of the cone D. By local duality one can then immediately derive Danilov's and Stanley's description of the canonical module as the ideal generated by the monomials corresponding to interior points of D.

As a combinatorial application of commutative algebra we include the main theorem on the Ehrhart function $E(P,n)$ of a rational convex polytope, including the reciprocity law. For the study of $E(P,n)$ one readily constructs a normal semigroup R ring with Hilbert function $E(P,n)$, so that results on $E(P,n)$ are special cases of theorems of Hilbert functions. In geometric language, if P is the polytope associated with a very ample line bundle L on a projective toric variety X, then R is the canonical ring

$$R = \bigoplus_{n=0}^{\infty} H^0(X, L^n).$$

For the reader's convenience we briefly sketch the theory of graded rings in Section 1; it is basic for every algebraic approach to the subject. Section 2 contains an outline of the main results on Hilbert functions and polynomials; they form the bridge between commutative algebra and combinatorics. We refer to Bruns and Herzog [1] for a detailed treatment.

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 $R = K[x_1, \dots, x_n]$ for suitable elements $x_1, \dots, x_n \in \bigcup_{i>0} R_i$. 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.* If a graded K-algebra is generated by elements of degree 1, then we call it a *homogeneous* 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 graded R-module is an R-module that as a K-vector space is a direct sum $M = \bigoplus_{i \in \mathbb{Z}} M_i$ 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. 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 $M_i/(U \cap M_i)$. The annihilator of a graded module is a graded ideal. If $\mathfrak{a}$ is a graded ideal in R, then $R/\mathfrak{a}$ is a graded K-algebra in a natural way.

A homomorphism $\varphi\colon M \to N$ 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 $\varphi\colon M \to N$. The graded modules form an Abelian category whose morphisms are the homogeneous homomorphisms.

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.

Theorem 1.1. *Let K be a field and R a graded K-algebra. Then there exist homogeneous elements $x_1, \dots, x_d$ (necessarily $d = \dim R$, the Krull dimension of R) such that*

(a) *$x_1, \dots, x_d$ are algebraically independent over K, and*
(b) *R is a finite $K[x_1, \dots, x_d]$-module.*

If R is a homogeneous K-algebra and K is infinite, then $x_1, \dots, x_d$ can be chosen to be of degree 1.

If $x_1, \dots, x_d$ satisfy the conditions (a) and (b), then we say that $K[x_1, \dots, x_d]$ is a *Noether normalization* of R, and $x_1, \dots, x_d$ is a *homogeneous system of parameters.*

Graded resolutions. Suppose that M is a finitely generated graded R-module, and choose a minimal homogeneous system $z_1, \dots, z_m$ of generators. Let F_0 be the free R-module of rank m over R; we grade it by setting $\deg e_i = \deg z_i$ for the elements e_i of a basis or F. The kernel of the homogeneous map $\varphi_0\colon F_0 \to M$, $e_i \mapsto z_i$, is again a finitely generated graded module with a minimal homogeneous system $y_1, \dots, y_p$ of generators. Therefore we have a presentation $F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0$ in which all the entries of a matrix representing φ_1 are homogeneous elements in $\mathfrak{m}$. 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 $z_1, \dots, z_m$ are uniquely determined (up to a permutation): exactly $\dim_K(M/\mathfrak{m}M)_i$ among the z_j have degree i. Iterating this construction one finds a *minimal graded free resolution of M*; it is uniquely determined up to an isomorphism of complexes of graded R-modules.

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

Theorem 1.2. *Let $R = K[X_1, \dots, X_n]$, and M a finite graded R-module. Then M has a minimal finite free resolution*

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

with $p = \operatorname{projdim} M = \operatorname{projdim} M_{\mathfrak{m}} \le n$.

In the summands $R(-j)^{\beta_{ij}}$ 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 i-th graded Betti numbers β_{ij} are uniquely determined by M.

Since a graded R-module 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: a graded R-module M has an injective resolution $0 \to I^0 \to I^1 \to \cdots \to I^n \to \cdots$ in the category of graded R-modules. This fact is important for graded local cohomology.

Graded Cohen–Macaulay rings and modules. A fundamental notion of commutative algebra is 'depth'. We need it only for graded rings R and finitely generated modules M. One says that $x_1, \dots, x_s \in R$ is an *M-sequence* if x_i is a not a zero-divisor of $M/(x_1, \dots, x_{i-1})M$ for $i = 1, \dots, s$ and if furthermore $M \neq (x_1, \dots, x_s)M$. The *depth of M* is the length of a maximal M-sequence contained in $\mathfrak{m}$. One can show that all the maximal M-sequences in $\mathfrak{m}$ have the same length, that there exists a maximal M-sequence consisting of homogeneous elements, and that $\operatorname{depth} M \le \dim M$. (Here

$\dim M = \dim R/\operatorname{Ann} M$ is the Krull dimension of M.) The *Auslander–Buchsbaum equation* connects depth and projective dimension:

$$\operatorname{depth} M + \operatorname{projdim} M = \operatorname{depth} R \qquad \text{if } \operatorname{projdim} M < \infty.$$

If R itself is a finite S-module, then $\operatorname{depth}_S M = \operatorname{depth}_R M$.

One calls M a *Cohen–Macaulay R-module* if $\operatorname{depth} M = \dim M$, and M is a *maximal* Cohen–Macaulay module, if $\operatorname{depth} M = \dim R$. The Cohen–Macaulay property has a down-to earth characterization in terms of a Noether normalization:

Proposition 1.3. *Let R be a graded K-algebra, and $M \neq 0$ a finitely generated graded R-module. Then the following are equivalent:*

(a) *M is Cohen–Macaulay;*
(b) *M is a free module over a Noether normalization of $R/\operatorname{Ann} M$.*

In particular, R is Cohen–Macaulay if and only if it is a free module over any of its Noether normalizations.

The elements $x_1, \dots, x_s$ form a maximal M-sequence for a Cohen–Macaulay R-module M if and only if their residue classes generate a Noether normalization of $R/\operatorname{Ann} M$.

The canonical module of a graded Cohen–Macaulay K-algebra. We introduce the canonical module via a Noether normalization. Therefore we must first define it for the polynomial ring $S = K[X_1, \dots, X_n]$ where $\deg X_i = a_i$: we set

$$\omega_S = S(-\textstyle\sum a_i).$$

(A good representative for ω_S is the principal ideal generated by $X_1 \cdots X_n$; it is isomorphic to ω_S as a graded module.) That this choice is very reasonable is indicated by the following theorem.

Theorem 1.4. *Let R be a Cohen–Macaulay graded K-algebra of dimension d and $S \subset R$ a Noether normalization.*

(a) *Then, with respect to its natural R-module structure, $\omega = \operatorname{Hom}_S(R, \omega_S)$*
  (i) *is a maximal Cohen–Macaulay R-module;*
  (ii) *it has finite injective dimension;*
  (iii) *$\operatorname{Ext}^j_R(K,\omega)_i = 0$ if $j \neq d$ or $j \neq 0$, and $\operatorname{Ext}^d_R(K,\omega)_0 = K$;*
  (iv) *$\operatorname{Hom}_R(\operatorname{Hom}_R(M,\omega),\omega) \cong M$ for all (graded) maximal Cohen–Macaulay R-modules, in particular $\operatorname{End}_R(\omega) \cong R$;*
  (v) *$\operatorname{rank}_R \omega = 1$ if R is an integral domain.*

(b) *If a graded R-module C satisfies the conditions* (i), (ii), *and* (iii), *then $C \cong \omega$.*

Part (b) shows that ω is independent of the choice of S, and therefore we may call it the *canonical module* ω_R *of* R. For (ii) one should note that $\operatorname{Ext}^j_R(M,N)$ is a graded R-module whenever M and N are graded and M is finitely generated; this holds since M has a graded free resolution by finitely generated free modules.

If ω_R is a free R-module, then R is called a *Gorenstein ring.* In this case we necessarily have $\omega_R \cong R(a)$. The number a will be identified below.

Local cohomology. What has been said above indicates that the theory of local rings has a graded counterpart (which, in a sense, is even simpler). This analogy includes local cohomology. 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 $f\colon M \to N$ 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 1.5. 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 a (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. We can even localize with respect to $\mathfrak{m}$: for all (graded) R-modules one has

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

One can use this isomorphism in order to reduce assertions about graded local cohomology to 'local' local cohomology, for example *Grothendieck's vanishing theorem.*

Theorem 1.6. *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* $H^d_{\mathfrak{m}}(M) \neq 0$.

Since injective resolutions are very hard to grasp, it is difficult to understand local cohomology from its definition. Therefore, in order to effectively use it for a specific ring R, one must find a complex that, in addition to 'computing' local cohomology, reflects the structure of R.

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 1.7. *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*

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

Here $M^\vee = \bigoplus_{i\in\mathbb Z}\operatorname{Hom}_K(M_{-i},K)$ denotes the *graded K-dual* of M; $M^\vee$ has a natural R-module structure. Behind 1.7 there is the fact that $R^\vee$ is the (graded) injective hull of K as an R-module.

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 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 the formal power series $H_M(t)=\sum_{n\in\mathbb Z}H(M,n)t^n$ 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 K. Furthermore the homological properties of M are stable under such extensions; see [1].

Suppose that S is the polynomial ring $K[X_1,\dots,X_d]$ 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.

Theorem 2.2. *Let R be a graded K-algebra, and $M\neq 0$ a finite graded R-module of dimension d. Then there exist positive integers $a_1,\dots,a_d$, 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 $S\cong K[X_1,\dots,X_d]$. By Hilbert's syzygy theorem M has a graded free resolution $F_\bullet$ with graded Betti numbers β_{ij}. We choose $Q(t)=\sum_{i=1}^p(-1)^i(\sum_j\beta_{ij}t^j)$, and indeed $H_M(t)=Q(t)H_S(t)$ by the additivity of the Hilbert function. 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 occurring in Theorem 2.2 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, $i = 0, \dots, g-1$, such that for all $n \in \mathbb{Z}$ one has $P(n) = P_i(n)$ where $n = mg + i$ with $0 \le i \le g-1$.

Theorem 2.3 (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 unique 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 $H_M(t)$.)*

Definition 2.4. (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 2.3, we have $a(R) < 0$ if and only the equation $P_R(n) = H(R,n)$ holds for all $n \ge 0$. At least in the Cohen–Macaulay case the a-invariant has a satisfactory homological interpretation:

Proposition 2.5. *Let R be a graded Cohen–Macaulay K-algebra of dimension d. Then*

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

In particular, if R is Gorenstein, then $\omega_R = R(a(R))$ (and conversely).

Homogeneous K-algebras. The exponents a_i in the denominator of $H_M(t)$ are the degrees of the elements generating a Noether normalization of $R/(\operatorname{Ann} M)$. As pointed out above, we may freely assume that K is infinite; by 1.1 we can then choose a system of parameters among the 1-forms, if R is a homogeneous K-algebra.

Theorem 2.6. *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*

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

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

Theorem 2.7. *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*

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

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

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

Theorem 2.8 (Stanley). *Let R be a d-dimensional Cohen–Macaulay graded K-algebra. Then $H_{\omega_R}(t) = (-1)^d H_R(t^{-1})$.*

The theorem follows quickly from the description $\omega_R = \operatorname{Hom}_S(R, \omega_S)$ for a Noether normalization S of R. Since R is a direct sum of shifted copies of S, it is in fact sufficient to do the case $R = S$ for which the equation boils down to the identity

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

3. 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

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

is a well-defined K-algebra. In the following we write X^z for $X_1^{z_1} \cdots X_n^{z_n}$. 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 $c_1, \dots, c_m \in \mathbb{Q}^n$ such that D is the set of non-negative linear combinations of $c_1, \dots, c_m$. Then $K[C]$ looks much more promising.

Theorem 3.1. *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 $\mathbb{Z}C$ 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 description of D that is equivalent to being finitely generated: D is the intersection of finitely many vector half-spaces,

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

here $\langle \_, \_ \rangle$ is the scalar product. If D is rational, then the a_i can be chosen in $\mathbb{Q}^n$, and vice 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 $K[C_i] \cong K[X_1^{\pm 1}, \dots, X_{n-1}^{\pm 1}, X^n]$ 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.

Theorem 3.2. *Let C be an affine semigroup. Then the following are equivalent:*
(a) *$K[C]$ is a normal domain;*
(b) *C is a normal semigroup, i.e. if $mz \in C$ for some $z \in \mathbb{Z}C$ and $m > 0$, then $z \in C$;*
(c) *$C = D \cap \mathbb{Z}^n$ as above.*

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

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

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 $H_1^0 \cap \dots \cap H_m^0$.

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 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 3.3. (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 want to apply the theory of graded rings as developed above to $K[C]$; this makes only sense if the grading on $K[C]$ is compatible with the semigroup structure of C. 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 3.4. *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 3.4 are satisfied, then C or D are called *positive.* Positive cones have *cross-sections* T.

Proposition 3.5. *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 3.3 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 $B^i = \{x \in \mathbb{R}^i \colon \|x\| \leq 1\}$ onto the closure $\bar{e}$ of e which maps the open ball $U^i = \{x \in \mathbb{R}^i \colon \|x\| < 1\}$ 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 $\dim \Gamma = \max\{i \colon \Gamma^i \neq \emptyset\}$. 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 as in (v) above.

Lemma 3.6. *Let Γ be a cell complex. Then there exists an incidence function on Γ.*

For a proof see Massey [10] where the incidence numbers $\varepsilon(e, e')$ appear as topological data determined by orientations of the cells. 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

$$\tilde{\mathcal{C}}(\Gamma) \colon 0 \to \mathcal{C}_{d-1} \xrightarrow{\partial} \mathcal{C}_{d-2} \to \cdots \to \mathcal{C}_0 \xrightarrow{\partial} \mathcal{C}_{-1} \to 0$$

where

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

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

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

Theorem 3.7. *Let Γ be a cell complex. Then $\tilde{H}_i(\Gamma) = \tilde{H}_i(|\Gamma|)$ for all $i \geq 0$ (and $\tilde{H}_{-1}(\Gamma) = 0$).*

We use 3.7 via the following corollary:

Corollary 3.8. *Let Γ be a cell complex such that $|\Gamma|$ is homeomorphic to a closed ball B^n. Then $\tilde{H}_i(\Gamma) = 0$ 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 cell 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

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

that is, we form the ring of fractions of R whose denominators are the monomials in $\{X^z : z \in C \cap F\}$. 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

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

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

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

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

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

is a complex. That $L^{\bullet}$ is exactly what we want, is shown by the next theorem.

Theorem 3.9. *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 exponent vectors z generate the cone D.

Next we need that $L^{\bullet} \otimes \_$ is an exact functor; this follows from the fact that $L^{\bullet}$ is a complex of flat R-modules.

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 heart of the proof is that

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

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

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 component $(L^\bullet)_z$. 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 3.10. *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 $\mathcal{S} = \{F \in \mathcal{F}\colon F$ 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.*

Lemma 3.11. *$(R_F)_z \neq 0$ (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 3.12. (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 $\mathcal{S} = \{F \cap T\colon F \in \mathcal{F}(D)$ visible from $z\}$. Then*

(i) $(L^\bullet)_z \cong \operatorname{Hom}_{\mathbb{Z}}\Big((\tilde{\mathcal{C}}(\mathcal{F})/\tilde{\mathcal{C}}(\mathcal{S}))(-1),\ K\Big)$,
(ii) $\tilde{H}_i(\mathcal{F}) = \tilde{H}_i(\mathcal{S}) = 0$ *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 $F = D$. The rest requires a careful discussion based on 3.10 and 3.11.

Theorem 3.13. (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 $i = 0, \dots, d-1$ by 3.9 and 3.12. Therefore depth $R = d$ by 1.6, 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 3.14. *$K[C]$ is Gorenstein if and only if there exists* $c \in \operatorname{relint} C$ *with* $\operatorname{relint} C = c + C$.

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

We define the cone $D \subset \mathbb{R}^{n+1}$ by $D = \mathbb{R}_+\{(p,1)\colon p \in P\}$. 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 finitely 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 $c = (c_1, \dots, c_{d+1})$ 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 3.15 (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*

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

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 2.3 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 3.13 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 2.8. The second equation results from $\sum_{m \geq 1} E(P, -m) t^m = -E_P(t^{-1})$.

The quasi-polynomial q in 3.15 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

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

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. In particular the Ehrhart quasi-polynomial of P is a polynomial and therefore called the *Ehrhart polynomial*. Furthermore $k[C]$ has a well-defined multiplicity.

Theorem 3.16. *Let $P \subset \mathbb{R}^n$ be an n-dimensional integral polytope, and let $k[C]$ the normal semigroup ring constructed above. Then*

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

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

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

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 $\operatorname{vol} P$. On the other hand, it is also given by $e(k[C])/n!$.

The fact that $K[C]$ is Cohen–Macaulay and contains its graded canonical module implies restrictions for the coefficients of the numerator polynomial of the Ehrhart series of P, the so-called h-vector; see Stanley [12] and Hibi [6].

References

1. W. Bruns and J. Herzog. *Cohen–Macaulay rings.* Cambridge University Press, 1993.
2. V. I. Danilov. The geometry of toric varieties. *Russian Math. Surveys* **33** (1978), 97–154.
3. E. Ehrhart. *Polynômes arithméthiques et méthode des polyédres en combinatoire.* Birkhäuser, 1977.
4. S. Goto and K. Watanabe. On graded rings, I. *J. Math. Soc. Japan* **30** (1978), 179–213.
5. S. Goto and K. Watanabe. On graded rings, II ($\mathbb{Z}^n$-graded rings). *Tokyo J. Math.* **1** (1978), 237–261.
6. T. Hibi. Ehrhart polynomials of convex polytopes, h-vectors of simplicial complexes, and non-singular 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.
7. T. Hibi. *Algebraic combinatorics on convex polytopes.* Carslaw Publications, 1992.
8. M. Hochster. Rings of invariants of tori, Cohen–Macaulay rings generated by monomials, and polytopes. *Ann. of Math.* **96** (1972), 318–337.
9. 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.
10. W. S. Massey. *Singular homology theory.* Springer, 1980.
11. U. Schäfer and P. Schenzel. Dualizing complexes and affine semigroup rings. *Trans. Amer. Math. Soc.* **322** (1990), 561–582.
12. R. P. Stanley. Hilbert functions of graded algebras. *Adv. in Math.* **28** (1978), 57–83.
13. R. P. Stanley. *Combinatorics and commutative algebra.* Birkhäuser, 1983.
14. R. P. Stanley. On the Hilbert function of a graded Cohen–Macaulay domain. *J. Pure Applied Algebra* **73** (1991), 307–314.

Universität Osnabrück, FB Mathematik/Informatik, 49069 Osnabrück, Germany
E-mail address: Winfried.Bruns@mathematik.uni-osnabrueck.de