# Combinatorics

Lecture Notes
Universität Leipzig

Summer 2024

Rainer Sinn
Joris Köfler

Version of July 1, 2024

# Contents

1 Introduction 5

2 Combinatorics – the art of counting 7

2.1 Generating Functions . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

3 Basics in commutative algebra 13

3.1 Noetherian rings and modules . . . . . . . . . . . . . . . . . . . . . . 13

3.2 Prime ideals and localization . . . . . . . . . . . . . . . . . . . . . . . 18

3.3 Primary decomposition . . . . . . . . . . . . . . . . . . . . . . . . . . 22

4 Monomial ideals 25

4.1 Basic properties . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 25

4.2 Algebraic operations . . . . . . . . . . . . . . . . . . . . . . . . . . . 26

4.3 Primary decomposition and associated primes . . . . . . . . . . . . . . 28

4.4 Squarefree monomial ideals and simplicial complexes . . . . . . . . . . 31

4.5 Graded modules and Hilbert functions . . . . . . . . . . . . . . . . . . 34

4.6 Free resolutions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 39

4.7 Face counting and Hilbert functions . . . . . . . . . . . . . . . . . . . 43

4.8 Alexander duality . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 45

5 Hochster's formula 47

5.1 Modules over the exterior algebra . . . . . . . . . . . . . . . . . . . . 47

5.2 Simplicial homology . . . . . . . . . . . . . . . . . . . . . . . . . . . . 49

5.3 Hochster's formula . . . . . . . . . . . . . . . . . . . . . . . . . . . . 50

# Chapter 1: Introduction

In this class, we will focus on combinatorics as the field of counting things. This is a vast area with many different methods and perspectives. After a brief introduction to some basic techniques, the main focus of the class is on Stanley-Reisner algebras/rings/ideals. This is an algebraic tool that can be used to prove properties of certain counts in the context of simplicial complexes. So essentially, we will introduce abstract simplicial complexes and study them with algebraic tools. They appear in nature in discrete geometry (e.g. the **boundary complex** of a simplicial polytope and more generally simplicial spheres) and algebraic topology (keyword **simplicial homology**), among other fields of mathematics.

One main point of Stanley-Reisner theory is to connect counts for simplicial complexes with algebraic invariants in the language of modules over polynomial rings. We will see Betti numbers and graded algebras. Abstract algebra is therefore a prerequisite, basics in commutative algebra are very useful, and familiarity with computer algebra systems (e.g. Macaulay2 or singular, the latter available in OSCAR) helps with computing examples.

The main sources for this course are the following.

## Bibliography

[A] M. Aigner. A Course in Enumeration. *Graduate Texts in Mathematics*, Springer, 2007.

[HH] J. Herzog, T. Hibi. Monomial Ideals. *Graduate Texts in Mathematics*, Springer, 2011.

[MS] E. Miller, B. Sturmfels. Combinatorial Commutative Algebra. *Graduate Texts in Mathematics*, Springer, 2005.

# Chapter 2: Combinatorics – the art of counting

**Note that the class starts in the third week. First meeting is on April 15!**

In *Enumerative Combinatorics* – also known as the art of counting – the goal is to systematically count the number of elements in a (countable) family of finite sets defined by combinatorial conditions. As a basic example, we might be interested to count the number of all 2-element subsets of the set $[n] = \{1, 2, \dots, n\}$ of all positive integers up to $n$ for any $n \in \mathbb{N}$. (Of course, the answer would be $\binom{n}{2}$.) Formally, we have an infinite family $S_n$ of finite sets indexed by a typically infinite set $I$ (for example, $n \in \mathbb{N}$) and we record the cardinality of $S_n$ in a **counting function** $f\colon I \longrightarrow \mathbb{N}_0$, $f(i) = |S_i|$. The index set $I$ might also live in $\mathbb{N} \times \mathbb{N}$, for instance. In this first chapter, we introduce some basic ways to give answers to such questions. The notion of a generating function is the main point. This chapter is based on [A]. There are many more examples and interesting results in that book.

## 2.1. Generating Functions

The idea of generating functions is very simple but surprising useful. We give a short introduction based on [A, Sections 2 and 3].

***Definition.*** A function $f\colon \mathbb{Z}_{\geq 0} \longrightarrow \mathbb{C}$ can be encoded in terms of a formal power series called the **generating function** of $f$ defined simply as

$$F(z) = \sum_{i=0}^{\infty} f(i) z^i.$$

This is a formal power series in the sense that we consider it as an algebraic object in the ring $\mathbb{C}[[z]]$ of power series as opposed to an analytic object (essentially, we are not concerned with matters of convergence). The algebraic operations are defined as usual, namely

$$\textstyle\sum_{i=0}^{\infty} a_i z^i + \sum_{j=0}^{\infty} b_j z^j = \sum_{i=0}^{\infty} (a_i + b_i) z^i \text{ and}$$
$$\textstyle\sum_{i=0}^{\infty} a_i z^i \cdot \sum_{j=0}^{\infty} b_j z^j = \sum_{k=0}^{\infty} \left( \sum_{i+j=k} a_i b_j \right) z^k.$$

Simple rational functions correspond to power series (by taking their Taylor expansion around 0). We might use the following with convention $\binom{m}{i} = 0$ for

$i > m$.

$$\begin{aligned}
\frac{1}{1-z} &= \sum_{i=0}^{\infty} z^i \\
\frac{1}{1+z} &= \sum_{i=0}^{\infty} (-1)^i z^i \\
\frac{1}{1-z^2} &= \sum_{i=0}^{\infty} z^{2i} \\
(1+z)^m &= \sum_{i=0}^{\infty} \binom{m}{i} z^i \\
\frac{1}{(1-z)^m} &= \sum_{i=0}^{\infty} \binom{m+i-1}{i} z^i \\
\frac{z^m}{(1-z)^{m+1}} &= \sum_{i=0}^{\infty} \binom{i}{m} z^i
\end{aligned}$$

***2.1.1 Exercise.*** Verify the expansions of rational functions as formal power series listed above.

***2.1.2 Exercise.*** What are the units of the ring $\mathbb{C}[[z]]$ of formal power series (with respect to the above product)?
*Hint:* If you know what a discrete valuation ring is, this should lead you to the answer. Otherwise, analysis courses often give the answer as well (in which case you want to think of the power series as a convergent power series for intuition).

***2.1.3 Exercise.*** Let $A$ and $B$ be two formal power series in $\mathbb{C}[[z]]$. Show that we get a well-defined series $A(B(z))$ if

(1) $A$ is a polynomial, or
(2) the constant term of $B$ is 0.

Furthermore, suppose that $A = \sum a_i z^i$ with $a_0 = 0$. Show that there exists a unique series $B = \sum b_j z^j$ with $b_0 = 0$ and $A(B(z)) = B(A(z)) = z$ if and only if $a_1 \neq 0$.

We might use the following series from analysis.

$$\begin{aligned}
\exp(z) &= \sum_{k=0}^{\infty} \frac{1}{k!} z^k \\
\log(1+z) &= \sum_{k=0}^{\infty} \frac{(-1)^{k+1}}{k} z^k \\
-\log(1-z) &= \sum_{k=0}^{\infty} \frac{1}{k} z^k
\end{aligned}$$

Sometimes it is useful to consider weights in addition to the counting function $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}$ (called $Q$-series in [A, Section 2.2]). Here is the primary example.

***Definition.*** For a function $f\colon \mathbb{Z}_{\geq 0} \longrightarrow \mathbb{C}$, the **exponential generating function** is defined as

$$\widehat{F}(z) = \sum_{k=0}^{\infty} \frac{1}{k!} f(k) z^k.$$

As an example of the usefulness of exponential generating functions, prove the binomial inversion formula.

***2.1.4 Exercise.*** Let $\widehat{A}(z) = \sum (a_i/i!) \cdot z^i$ and $\widehat{B}(z) = \sum (b_i/i!) \cdot z^i$ be two exponential generating functions for counting functions $a, b\colon \mathbb{Z}_{\geq 0} \longrightarrow \mathbb{C}$. First, show that the equality $\widehat{B}(z) = \widehat{A}(z)\exp(z)$ is equivalent to

$$b_n = \sum_{k=0}^{n} \binom{n}{k} a_k$$

for all $n$. From this, derive the *binomial inversion formula* which says that the following two identities are equivalent:

$$\begin{aligned} b_n &= \sum_{k=0}^{n} \binom{n}{k} a_k \text{ for all } n \in \mathbb{Z}_{\geq 0} \\ a_n &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k \text{ for all } n \in \mathbb{Z}_{\geq 0}. \end{aligned}$$

We will also consider the derivative of a formal power series as a formal, linear operation.

***Definition.*** The **formal derivative** of $F(z) = \sum_{i=0}^{\infty} a_i z^i \in \mathbb{C}[[z]]$, denoted $F'(z)$ is defined as

$$F'(z) = \sum_{i=0}^{\infty} (i+1) a_{i+1} z^i.$$

***2.1.5 Exercise.*** Show that familiar rules for derivatives also hold for formal derivatives of formal power series, i.e. show $(F+G)' = F' + G'$, $(FG)' = F'G + FG'$, $(F^{-1})' = -F'/F^2$, and $F(G(z))' = F'(G(z))G'(z)$, whenever the expressions are defined.

The formal derivative can be used to derive recursion formulas, for instance.

***2.1.6 Example.*** Set $A(z) = \sum_{i=0}^{\infty} \binom{2i}{i} z^i$ and $a_i = \binom{2i}{i}$. By definition of binomial coefficients, we have

$$a_i = \binom{2i}{i} = \frac{2i(2i-1)}{i^2} a_{i-1}$$

so that $ia_i = 4ia_{i-1} - 2a_i$. This is equivalent to the formal identity

$$F' = 4(zF)' - 2F = 4zF' + 2F.$$

Now we use some tricks. First, we rewrite the identity as $F = \frac{1}{2}(1-4z)F'$. Second, we solve this using logarithms, namely

$$(\log(F))' = \frac{F'}{F} = \frac{2}{1-4z} = -\frac{1}{2}\left(\log(1-4z)\right)'.$$

Integrating this identity (which we can again do formally, termwise), we get $\log(F) = -\frac{1}{2}\log(1-4z)$ – we don't have to worry about constant terms. Using the usual logarithmic exponential rule (exercise: this applies also in the setup of formal power series), we finally see

$$F(z) = \sum_{i=0}^{\infty} \binom{2i}{i} = \frac{1}{\sqrt{1-4z}}.$$

Exercise: Show, by Taylor expansion on the right hand side (or better yet of the identity $F^2 = 1/(1-4z)$), that this implies for all $n \geq 1$ the identity

$$\sum_{k=0}^{n} \binom{2k}{k}\binom{2(n-k)}{n-k} = 4^n.$$

***2.1.7 Exercise.*** Find the unique sequence $(a_n)_{n\geq 0}$ of real numbers such that

$$\sum_{k=0}^{n} a_k a_{n-k} = 1$$

for all $n \geq 0$.

Another basic application of generating functions is to recursively defined sequences. The main result is the following.

***2.1.8 Theorem.*** *Let $c_1, \ldots, c_d$ be a sequence of complex numbers for some integer $d \geq 1$ with $c_d \neq 0$ and set $c(z) = 1+c_1z+\ldots+c_dz^d \in \mathbb{C}[z]$. Denote by $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$ the distinct roots of the reciprocal polynomial $c^R(z) = z^d c(\frac{1}{z})$ (in some order) so that*

$$c(z) = (1-\alpha_1 z)^{d_1} \cdots (1-\alpha_k z)^{d_k}$$

*for multiplicities $d_i \in \mathbb{N}$. Let $f\colon \mathbb{Z}_{\geq 0} \longrightarrow \mathbb{C}$ be a function. The following statements are equivalent.*

*(1) The function $f$ satisfies the recurrence*

$$f(n+d) + c_1 f(n+d-1) + \ldots + c_d f(n) = 0$$

*of order $d$ for all $n \geq 0$.*

*(2) The corresponding generating function is a rational function, namely there is a polynomial $p \in \mathbb{C}[z]$ of degree less than $d$ such that*

$$F(z) = \sum_{i=0}^{\infty} f(i) z^i = \frac{p(z)}{c(z)}.$$

*(3) There are polynomials $p_i \in \mathbb{C}[z]$ of degree less than $d_i$ ($i \in [k]$) such that*

$$f(n) = \sum_{i=1}^{k} p_i(n)\alpha_i^n.$$

*Proof.* The following sketches the main steps in the proof. See [A, Theorem 3.1] for full details. The proof is based on linear algebra, comparing vector spaces of dimension $d$ over $\mathbb{C}$. We set

$$\begin{aligned}
V_1 &= \{f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}\colon f(n+d) + c_1 f(n+d-1) + \ldots + c_d f(n) = 0 \text{ for all } n \geq 0\} \\
V_2 &= \{f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}\colon \sum_{i=0}^{\infty} f(i) z^i = \frac{p(z)}{c(z)} \text{ for some } p \in \mathbb{C}[z]_{d-1}\} \\
V_3 &= \{f\colon \mathbb{Z}_{\geq 0} \to \mathbb{C}\colon f(n) = \sum_{i=1}^{k} p_i(n) \alpha_i^n \text{ for some } p_i \in \mathbb{C}[z]_{d_i-1}\}
\end{aligned}$$

with each vector space corresponding to one statement of the theorem. The first observation is that all three vector spaces have dimension $d$ over $\mathbb{C}$. In the first case, we have $d$ initial conditions; in the second, the polynomial $p$ has $d$ coefficients; and in the third, the polynomials $p_i$ have $d$ coefficients in total. Therefore, it suffices to prove inclusions of these vector spaces to conclude equality and therefore the theorem. The inclusion $V_2 \subset V_1$ is direct by comparing coefficients of the formal power series $c(z) \sum_{i=0}^{\infty} f(i) z^i = p(z)$; so we have $V_1 = V_2$. Finally, to show $V_1 = V_2 \subset V_3$, we use partial fraction decomposition of the rational function $p(z)/c(z)$ to obtain the polynomials $p_i$. Since the polynomials $(1 - \alpha_i z)^{d_i}$ divide $c(z)$, we can write

$$\frac{p(z)}{c(z)} = \sum_{i=1}^{k} \frac{g_i(z)}{(1-\alpha_i z)^{d_i}}.$$

Now we need to work a bit and manipulate this algebraically. The important result is the equality

$$\frac{g_i(z)}{(1-\alpha_i z)^{d_i}} = \sum_{n=0}^{\infty} \left( \sum_{j=0}^{d_i-1} \alpha_i^{-j} \cdot g_{i,j} \cdot \binom{n+d_i-j-1}{d_i-1} \right) \alpha_i^n z^n$$

where $g_i = \sum_{j=0}^{d_i-1} g_{i,j} z^j$. Comparing coefficients, we can read off the polynomials $p_i(n) = \sum_{j=0}^{d_i-1} \alpha_i^{-j} \cdot g_{i,j} \cdot \binom{n+d_i-j-1}{d_i-1}$ with the property that $f(n) = \sum_{i=1}^{k} p_i(n) \alpha_i^n$ as claimed in (3). ■

***2.1.9 Exercise.*** Use the above result to give a closed formula for the $n$th Fibonacci number defined by the recurrence $F_n = F_{n-1} + F_{n-2}$ $(n \geq 2)$ of order 2 with initial conditions $F_0 = 0$ and $F_1 = 1$. (The golden ratio should appear in your computations.) What happens if we change the initial conditions? For instance, can you quickly adapt the solution to $F_0 = 10$ and $F_1 = -5$?

# Chapter 3: Basics in commutative algebra

## 3.1. Noetherian rings and modules

In this section, we discuss some basics in abstract and commutative algebra. A ring $R$ for us here is a commutative ring with unit which means that $(R, +)$ is an abelian group, $(R, \cdot)$ is associative, commutative, and has a neutral element $1 \in R$, and addition and multiplication are distributive. We will assume that $0 \neq 1$ (so the neutral element for addition and multiplication are distinct). Most commonly, we will work with polynomial rings $R = [x_1, \ldots, x_n]$. Another good example to keep in mind is $R = \mathbb{Z}$.

***3.1.1 Exercise.*** Show that a ring $R$ with $0 = 1$ is $R = \{0\}$.

***Definition.*** Let $R$ be a ring. A subset $I \subset R$ is an **ideal** of $R$ if is is non-empty and satisfies $I + I \subset I$ and $R \cdot I \subset I$.

***3.1.2 Exercise.*** Show that every ideal is an abelian group with respect to addition (inherited from $R$).

***3.1.3 Proposition.*** *The intersection of ideals of a ring is again an ideal. In particular, for any set $M \subset R$, there is a unique smallest ideal containing $M$ which we denote by $\langle M \rangle = \bigcap_{I \supset M} I$. We have*

$$\langle M \rangle = \left\{ \sum_{i=1}^{r} f_i g_i \mid r \in \mathbb{N}, f_i \in R, g_i \in M \right\}.$$

*Proof.* Exercise. ■

***3.1.4 Theorem.*** *Let $k$ be a field and $R = k[x]$ be the polynomial ring over $k$ in one variable $x$. Then every ideal of $R$ is generated by one element.*

*Proof.* This follows from polynomial division with remainder. In other words, the ring $R$ is **Euclidean**. Let $I \subset R$ be an ideal, $I \neq \{0\}$. Then there is a unique monic polynomial $f \in I$ of smallest degree (so with leading coefficient 1). Indeed, let $f$ be any monic polynomial of smallest degree and pick $g \in I$. By polynomial division, we can write

$$g = q \cdot f + r$$

with $0 \leq \deg(r) < \deg(f)$ or $r = 0$. Since the degree of $f$ is minimal over all elements in $I$ and $r = g - q \cdot f \in I$, we must have $r = 0$ so that $f$ divides $g$. ■

***3.1.5 Exercise.*** Let $k$ be a field and $f, g \in k[t]$ be polynomials. (You can also start with $R = \mathbb{Z}$ – the arguments are similar.) Show that $\langle f \rangle + \langle g \rangle = \langle \gcd(f, g) \rangle$ (using the Euclidean algorithm). Also show that $\langle f \rangle \cap \langle g \rangle = \langle \operatorname{lcm}(f, g) \rangle$. Use this to find an example such that $\langle fg \rangle \subsetneq \langle f \rangle \cap \langle g \rangle$.

***Definition.*** A **module** $M$ over a ring $R$ (or $R$-**module**) is an abelian group $(M, +)$ together with a scalar multiplication $R \times M \longrightarrow M$, $(a, m) \mapsto a \cdot m$ satisfying the distributive laws $a(x + y) = ax + ay$ and $(a + b)x = ax + bx$, the associative law $(ab)x = a(bx)$, and the normalization $1x = x$.

***3.1.6 Example.*** (1) For any ring $R$ and any $n \in \mathbb{N}$, the $n$-fold direct product $R^n$ is an $R$-module with componentwise scalar multiplication (analogous to the vector space $k^n$ of column vectors for a field $k$).

(2) Any ideal of a ring $R$ is an $R$-module. In fact, the ideals of $R$ are exactly the $R$-modules contained in $R$.

(3) The $\mathbb{Z}$-modules are precisely the abelian groups.

(4) The trivial module over any ring $R$ is $M = \{0\}$.

***Definition.*** A **submodule** of an $R$-module $M$ is a subgroup $U \subset M$ that is closed under scalar multiplication.

***3.1.7 Exercise.*** Show that a subset $U \subset M$ of an $R$-module $M$ is a submodule if and only if $U \neq \emptyset$, $U + U \subset U$, and $R \cdot U \subset U$.

***3.1.8 Proposition.*** *Let M be an R-module. For any submodules U and V of M, the set*

$$(U \colon V) = \{a \in R \mid aV \subset U\}$$

*is an ideal of R.*

*Proof.* Exercise. ∎

***3.1.9 Exercise.*** What is $(U \colon V)$ if $R = k$ is a field and $M$ is a (say finite-dimensional) vector space over $k$?

***Definition.*** The **annihilator** of an $R$-module $M$ is the ideal

$$\operatorname{Ann}(M) = (\{0\} : M) = \{a \in R \mid ax = 0 \text{ for all } x \in M\}.$$

***3.1.10 Exercise.*** Let $R$ be a ring and $I \subset R$ an ideal. Show that $M = R/I$ is an $R$-module (with scalar multiplication $(a, \overline{x}) \mapsto \overline{ax}$) and compute the annihilator of $M$. (For simplicity, it might be good to start with $R = \mathbb{Z}$ and $I = \langle m \rangle$.)

***3.1.11 Exercise.*** Let $R$ be a ring and $M$ be an $R$-module. Show the following claims.

(1) For any ideal $I \subset R$ contained in $\operatorname{Ann}(M)$, the module $M$ is an $R/I$-module with scalar multiplication $\overline{a}x = ax$.

(2) The annihilator of $M$ as an $R/\operatorname{Ann}(M)$-module is $\{0\}$.

(3) For any submodules $U$ and $V$ of $M$, we have

$$\operatorname{Ann}(U + V) = \operatorname{Ann}(U) \cap \operatorname{Ann}(V).$$

(4) For any submodules $U$ and $V$ of $M$, we have

$$(U\colon V) = \operatorname{Ann}\left((U+V)/U\right).$$

***Definition.*** An $R$-module $M$ is called **noetherian** if every ascending chain of submodules $M_0 \subset M_1 \subset M_2 \subset \ldots$ stabilizes, i.e. there exists some $n \in \mathbb{N}$ such that $M_n = M_{n+k}$ for all $k \in \mathbb{N}$. A ring $R$ is called **noetherian** if it is noetherian as an $R$-module.

***3.1.12 Exercise.*** Show that a ring is noetherian if and only if every ideal is finitely generated. More generally, an $R$-module is noetherian if and only if it is finitely generated.

***Definition.*** A **(homo-)morphism** $\varphi\colon M \longrightarrow N$ of $R$-modules (sometimes also called $R$-**linear map**) is a map satisfying $\varphi(ax+by) = a\varphi(x) + b\varphi(y)$ for all $a, b \in R$ and $x, y \in M$. The **image** $\operatorname{im}(\varphi)$ of $\varphi$ is the set $\{\varphi(x) \mid x \in M\}$. The **kernel** of $\varphi$ is the set $\{x \in M \mid \varphi(x) = 0\}$.

***3.1.13 Exercise.*** Both image and kernel of any homomorphism of $R$-modules are $R$-modules.

***Definition.*** Let $I \subset \mathbb{Z}$ be an interval (meaning $I = [a,b] \cap \mathbb{Z}$ for some integers $a < b$). A **sequence** of $R$-modules is a family $(M_i)_{i\in I}$ of $R$-modules together with $R$-module homomorphisms $\varphi_i\colon M_{i-1} \longrightarrow M_i$ for all $i \in I$ such that $i-1 \in I$. The sequence is **exact at position** $i \in I$ (with $i-1, i+1 \in I$) if the image of $\varphi_i$ and the kernel of $\varphi_{i+1}$ are equal, i.e.

$$\operatorname{im}(\varphi_i) = \ker(\varphi_{i+1}) \subset M_i.$$

A sequence is **exact** if it is exact in every position. A **short exact sequence** is an exact sequence of the form

$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0.$$

***3.1.14 Example.*** (1) The sequence $0 \longrightarrow N \longrightarrow M$ is exact at $N$ if and only if the map $N \longrightarrow M$ is injective.

(2) The sequence $M \longrightarrow P \longrightarrow 0$ is exact at $P$ if and only if the map $M \longrightarrow P$ is surjective.

(3) So the sequence $0 \longrightarrow N \longrightarrow M \longrightarrow 0$ is exact at $M$ if and only if the map $N \longrightarrow M$ is an isomorphism.

***3.1.15 Proposition.*** *Given a short exact sequence*

$$0 \longrightarrow N \xrightarrow{\varphi} M \xrightarrow{\psi} P \longrightarrow 0$$

*of $R$-modules, we have that $M$ is noetherian if and only if both $N$ and $P$ are noetherian.*

*Proof.* If $M$ is noetherian, then a direct argument shows that $N$ and $P$ are noetherian. Indeed, any ascending chain $N_0 \subset N_1 \subset \ldots \subset N$ of submodules of $N$ gives the ascending chain $\varphi(N_0) \subset \varphi(N_1) \subset \dots$ in $M$, which stabilizes by noetherianity of $M$. This implies that the original chain of submodules also stabilizes showing that $N$ is noetherian. Any ascending chain $P_0 \subset P_1 \subset \dots \subset P$ of submodules of $P$ again gives the ascending chain $\psi^{-1}(P_0) \subset \psi^{-1}(P_1) \subset \dots \subset M$ of submodules of $M$, which stabilizes. This shows again that the original chain also stabilizes and that $P$ is noetherian.

Conversely, let $M_0 \subset M_1 \subset M_2 \subset \dots$ be an ascending chain of submodules of $M$. Then we get ascending chains in both $N$ and $P$, namely $\varphi^{-1}(M_0) \subset \varphi^{-1}(M_1) \subset \dots \subset N$ and $\psi(M_0) \subset \psi(M_1) \subset \dots \subset P$. By noetherianity of $N$ and $P$, both chains eventually stabilize. So we can choose an $n \in \mathbb{N}$ such that for any $k > n$ we have $\varphi^{-1}(M_k) = \varphi^{-1}(M_n)$ and $\psi(M_k) = \psi(M_n)$. We show that this implies $M_k = M_n$ proving the claim. Pick $x \in M_k \supset M_n$. Then $\psi(x) \in \psi(M_k) = \psi(M_n)$ so that there exists a $y \in M_n$ with $\psi(x) = \psi(y)$. So the element $x - y \in M_k$ is in the kernel of $\psi$, which is the image of $\varphi$. So there is an element $z \in \varphi^{-1}(M_k) = \varphi^{-1}(M_n)$ with $\varphi(z) = x - y$. Finally,

$$x = (x - y) + y = \varphi(z) + y$$

shows that $x \in M_n$ and therefore $M_k = M_n$. ■

***3.1.16 Corollary.*** *Every submodule and every quotient module of a noetherian module is noetherian.*

*Proof.* Exercise: write the correct short exact sequence. ■

***3.1.17 Theorem*** (Hilbert's basis theorem). *The polynomial ring $R[t]$ over a noetherian ring $R$ is noetherian. In particular, the polynomial ring $k[x_1, \dots, x_n]$ over a field is noetherian.*

*Proof.* Let $I$ be an ideal of $R[t]$ and set

$$J = \{\mathrm{LC}(f) \mid f \in I\}$$

where $\mathrm{LC}(f)$ is the leading coefficient of $f$. This set $J$ is an ideal of $R$ and therefore finitely generated by assumption, say $J = \langle a_1, \dots, a_m \rangle$. For each $i \in [m]$ pick a polynomial $f_i \in I$ with $\mathrm{LC}(f_i) = a_i$ and set $I' = \langle f_1, \dots, f_m \rangle \subset I$. Let $d$ be the largest degree of the $f_i$.

We first show that any polynomial $f \in I$ of degree $k \geq d$ can be written as $f = g + h$ for a polynomial $h \in I'$ and a polynomial $g$ of degree less than $d$. Write $f = \sum_{i=0}^{k} b_i t^i$. Then there are $u_j \in R$ such that $b_k = \sum_{j=1}^{m} u_j a_j \in J$. This identity implies that the polynomial

$$f - \sum_{j=1}^{m} u_j f_j t^{k - \deg(f_j)} \in I$$

has degree less than $k$. Iterating this process, we get a representation $f = g + h$ as claimed, i.e. $h \in I'$ and $\deg(g) < d$.

Set $M = R[t]_{<d}$ to be the $R$-submodule of $R[t]$ generated by the monomials

$1, t, \ldots, t^{d-1}$. The above argument shows that, as $R$-modules, we have

$$I = (I \cap M) + I'.$$

As a finitely generated module over a noetherian ring, the module $M$ is noetherian by Corollary 3.1.16 so that $I \cap M$ is finitely generated (as an $R$-module). If $g_1, \ldots, g_n$ generate $I \cap M$, then $I$ is finitely generated, namely

$$I = \langle f_1, \ldots, f_m, g_1, \ldots, g_n \rangle.$$

■

***3.1.18 Corollary.*** *For any noetherian ring $R$ and any $n \in \mathbb{N}$ the polynomial ring $R[x_1, \ldots, x_n]$ is noetherian. In particular, $S = k[x_1, \ldots, x_n]$ is noetherian for any field $k$.*

*Proof.* By induction on $n$, using Theorem 3.1.4 as the base case for the second sentence $S$. ■

Let us look at some notions from linear algebra in this more general contexts of $R$-modules. Note that finitely generated modules over fields are finite-dimensional vector spaces. So let $R$ be a ring and $M$ an $R$-module. Let $\mathcal{F} = (x_i)_{i \in I}$ be some family of elements $x_i \in M$. An $R$-**linear relation** in $\mathcal{F}$ is an identity

$$a_1 x_{i_1} + a_2 x_{i_2} + \ldots + a_k x_{i_k} = 0$$

for some $k \in \mathbb{N}$ and $a_1, \ldots, a_k \in R$ and distinct elements $i_1, \ldots, i_k \in I$. An $R$-linear relation is called **non-trivial** if at least one coefficient $a_j$ is not 0. The family $\mathcal{F}$ of elements of $M$ is $R$-**linearly independent** if there is no non-trivial $R$-linear relation in $\mathcal{F}$.

***Definition.*** Let $M$ be an $R$-module $M$. A family $\mathcal{F} = (x_i)_{i \in I}$ of elements in $M$ is called a **basis** of $M$ if it is a linearly independent generating set. The module $M$ is called **free** if it has a basis.

***3.1.19 Example.***

1. Vector spaces over a field $k$ are free $k$-modules (assuming Zorn's Lemma; otherwise, at least all finite-dimensional vector spaces are free $k$-modules).
2. For every ring $R$ and every $n \in \mathbb{N}$, the $R$-module $R^n$ is a free $R$-module with basis $e_1, \ldots, e_n$.
3. The $\mathbb{Z}$-module $\mathbb{Z}/m$ is not free for any $m \in \mathbb{Z}$, $m \neq 0$.

***3.1.20 Exercise.*** Find a minimal generating set of $\mathbb{Z}$ as a $\mathbb{Z}$-module that is not a basis.

We will see free modules later in the context of Betti numbers. As far as $R$-module homomorphisms go, free modules behave much like vector spaces. In particular, the following result holds.

***3.1.21 Theorem.*** *Let $M$ be a free $R$-module with basis $(x_i)_{i \in I}$. Let $N$ be an $R$-module and choose a family $(y_i)_{i \in I}$ of elements in $N$. There is a unique $R$-module homomorphism $\varphi\colon M \to N$ satisfying $\varphi(x_i) = y_i$ for all $i \in I$. If $(y_i)_{i \in I}$ is a basis of $N$, then $\varphi$ is an isomorphism.*

*Proof.* Every $x \in M$ has a unique representation $x = \sum_{i \in I} a_i x_i$ as a (finite!) $R$-linear combination of the basis elements of $M$. Hence, we must have $\varphi(x) = \sum_{i \in I} a_i y_i$. This map is $R$-linear and hence uniquely determined by $\varphi(x_i) = y_i$.

If $(y_i)_{i \in I}$ is a basis of $N$, the inverse of $\varphi$ is the map $\psi \colon N \longrightarrow M$ determined by $\psi(y_i) = x_i$. ■

***3.1.22 Exercise.*** Let $M$ be an $R$-module and $n \in \mathbb{N}$. Show that the following are equivalent.

(1) $M$ can be generated by (at most) $n$ elements.

(2) There is a surjective $R$-module homomorphism $R^n \longrightarrow M$.

(3) $M$ is isomorphic to a quotient module of $R^n$.

(For this exercise, we assume homomorphism and isomorphism theorems, as well as the quotient construction, that is not explicitly explained in these lecture notes.)

***3.1.23 Exercise.*** Show that the module $\mathrm{Hom}_R(M, R)$ of $R$-module homomorphisms from $M$ to $R$ is free for every free $R$-module $M$.
*Hint:* dual basis

## 3.2. Prime ideals and localization

Localization is an important technique in ring theory generalizing the construction of the fraction field. We will see it here to show some basic results involving prime ideals.

***Definition.*** An ideal $I$ of a ring $R$ is **prime** if $I \neq R$ and for all $a, b \in R$ with $a \cdot b \in I$ we have $a \in I$ or $b \in I$.

***3.2.1 Exercise.*** Show that a principal ideal $\langle a \rangle \subset R$ is prime if and only if the element $a$ is prime. (Recall that an element $a \in R$ is prime if for all $b, c \in R$ such that $a$ is a divisor of $b \cdot c$ it follows that $a$ divides $b$ or $c$.)

***3.2.2 Exercise.*** An ideal $I$ of $R$ is prime if and only if the quotient ring $R/I$ is a domain, i.e. it has no non-trivial zero divisors. (Recall, an element $a \in R$ is called a **zero divisor** if there exists a $b \neq 0$ such that $a \cdot b = 0$. The trivial zero divisor is 0.)

***Definition.*** A set $S \subset R$ in a ring $R$ is called **multiplicative** if $1 \in S$ and for all $s_1, s_2 \in S$ we also have $s_1 s_2 \in S$.

***3.2.3 Example.*** If $P \subset R$ is a prime ideal, then $S = R \setminus P$ is multiplicative.

If $R$ is a domain and $S \subset R$ is multiplicative with $0 \notin S$, then the set

$$R[S^{-1}] = \left\{ \frac{a}{s} \,\middle|\, s \in S \right\} \subset \mathrm{Quot}(R)$$

is a subring of the fraction field of $R$. In particular, the elements of $S$ are invertible in $R[S^{-1}]$.

***3.2.4 Example.*** (1) In $\mathbb{Z}$ the set $S$ of all odd numbers is multiplicative. The ring $\mathbb{Z}[S^{-1}]$ is the subset of $\mathbb{Q}$ of all fractions that can be written with an odd denominator. Similarly, the set $T$ of all even numbers is multiplicative. So the ring $\mathbb{Z}[T^{-1}]$ contains all fractions that can be written with an even denominator.

(2) In any ring $R$ and any element $s \in R$, the set $S = \{1, s, s^2, s^3, \ldots\}$ of all powers of $s$ is a multiplicative set.

***Definition.*** Let $M$ be an $R$-module and $S \subset R$ a multiplicative set. On $M \times S$ we define the relation

$$(x_1, s_1) \sim (x_2, s_2) \qquad \Longleftrightarrow \qquad \exists t \in S \colon t(s_2 x_1 - s_1 x_2) = 0.$$

(The $t$ in this definition is only relevant for rings that have nontrivial zero divisors.)

***3.2.5 Proposition.*** *Let $R$ be a ring and $S \subset R$ be a multiplicative set.*

(1) *The relation $\sim$ is an equivalence relation. Writing $\frac{x}{s}$ (or $x/s$) for the equivalence class of $(x, s)$ and $M[S^{-1}]$ for the set of these equivalence classes, we define*

$$\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st} \text{ and } a \cdot \frac{x}{t} = \frac{ax}{t}.$$

*This makes $M[S^{-1}]$ into an $R$-Modul, called the **localization** of $M$ with respect to $S$.*

(2) *The $R$-module $R[S^{-1}]$ with multiplication*

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

*is a ring with unit $\frac{1}{1}$ and zero element $\frac{0}{1}$, called the **localization** of $R$ with respect to $S$. For any $R$-module $M$, the $R$-module $M[S^{-1}]$ becomes a $R[S^{-1}]$-module via*

$$\frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st}.$$

*Proof.* This is mostly direct. The main point is to show that addition (and scalar multiplication) are well-defined. For addition. suppose $\frac{x}{s} = \frac{x'}{s'} \in M[S^{-1}]$ so that $u(s'x - sx') = 0$ for some $u \in S$. For $\frac{y}{t} \in M[S^{-1}]$ we then have

$$\frac{tx' + s'y}{s't} = \frac{tux' + s'uy}{s'tu} = \frac{stux' + ss'uy}{ss'tu} = \frac{s'tux + ss'uy}{ss'tu} = \frac{tux + suy}{stu} = \frac{tx + sy}{st}.$$

Therefore, whenever we want to compute $\frac{x}{s} + \frac{y}{t}$, we can first find a common denominator and replace $\frac{x}{s}$ by $\frac{xt}{st}$ and $\frac{y}{t}$ by $\frac{ys}{st}$. Then associativity of addition in $M[S^{-1}]$ follows from associativity in $M$. To see that $M[S^{-1}]$ is still an abelian group, note

$$\frac{0}{1} + \frac{x}{s} = \frac{x}{s} \quad \text{und} \quad \frac{x}{s} + \frac{-x}{s} = \frac{0}{s} = \frac{0}{1}$$

for all $\frac{x}{s} \in M[S^{-1}]$. Associativity (and normalization) of scalar multiplication as well as the distributive laws follow in the same vein. The remaining details (and a proof of claim (2)) are left as an exercise. ■

Localization of an $R$-module $M$ with respect to $S \subset R$ comes with an $R$-linear map

$$\lambda_S\colon M \longrightarrow M[S^{-1}],\ x \mapsto \frac{x}{1}.$$

For $M = R$ the map $\lambda_S\colon R \longrightarrow R[S^{-1}]$ is also a ring homomorphism. By construction, the elements of $S$ become units in $R[S^{-1}]$. Indeed, we have

$$\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1}$$

in $R[S^{-1}]$.

In general, $\lambda_S(x) = 0/1$ for $x \in M$ if and only if there is a $t \in S$ with $tx = 0$. So $\lambda_S$ is injective if and only if no element of $S$ annihilates any element of $M \setminus \{0\}$. In particular, $\lambda_S\colon R \longrightarrow R[S^{-1}]$ is injective if and only if $S$ does not contain any zero divisors. We usually will not distinguish between $a$ and $\frac{a}{1}$ not between $s^{-1}$ and $\frac{1}{s}$ even if $R$ is not a subring of $R[S^{-1}]$.

***3.2.6 Exercise.*** What is $R[S^{-1}]$ if $0 \in S$?

***3.2.7 Exercise.*** Show that a ring $R$ is a domain if and only if the set $S = R \setminus \{0\}$ is multiplicative. In this case, $R[S^{-1}]$ is equal to $\mathrm{Quot}(R)$.

***3.2.8 Lemma.*** *Let $S \subset R$ be a multiplicative set. For any ideal $I$ of $R$, the set*

$$I[S^{-1}] = \left\{\frac{a}{s} \mid a \in I, s \in S\right\}$$

*is an ideal of $R[S^{-1}]$. Any ideal of $R[S^{-1}]$ is of this form for a suitable ideal $I$ of $R$.*

*Proof.* That $I[S^{-1}]$ is an ideal of $R$ is direct from the fact that addition and multiplication of $R[S^{-1}]$ are well-defined. If $J \subset R[S^{-1}]$ is an ideal, then $I = \lambda_S^{-1}(J) \subset R$ is an ideal of $R$ and we have $J = I[S^{-1}]$. ■

***3.2.9 Theorem.*** *Let $P \subset R$ be a prime ideal and $S \subset R$ be a multiplicative set. If $P \cap S = \emptyset$, then the ideal $P[S^{-1}]$ is a prime ideal of $R[S^{-1}]$. Conversely, every prime ideal of $R[S^{-1}]$ is of the form $P[S^{-1}]$ of a prime ideal $P$ of $R$ with $P \cap S = \emptyset$.*

Let $S \subset R$ be multiplicative and $U \subset M$ be an $R$-submodule of an $R$-module $M$. We can argue directly that $U[S^{-1}]$ is a submodule of $M[S^{-1}]$. More generally, any $R$-linear map $\varphi\colon M \longrightarrow N$ induces an $R[S^{-1}]$-linear map

$$\varphi_S\colon M[S^{-1}] \to N[S^{-1}],\ \frac{x}{s} \mapsto \frac{\varphi(x)}{s}.$$

We have $(\varphi \circ \psi)_S = \varphi_S \circ \psi_S$ and $(\mathrm{id}_M)_S = \mathrm{id}_{M[S^{-1}]}$. (Put differently, $M \mapsto M[S^{-1}]$ and $\varphi \mapsto \varphi_S$ gives a functor from the category of$R$-modules to the category of $R[S^{-1}]$-modules.) The next result is about properties of these assignments.

***3.2.10 Theorem.*** *For any multiplicative set $S \subset R$ of a ring $R$ localization is an exact functor. Concretely, this means that for all exact sequences*

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \longrightarrow \cdots$$

*of $R$-modules the induced sequence*

$$\cdots \longrightarrow M_{i-1}[S^{-1}] \xrightarrow{\varphi_{i,S}} M_i[S^{-1}] \xrightarrow{\varphi_{i+1,S}} M_{i+1}[S^{-1}] \longrightarrow \cdots$$

*of $R[S^{-1}]$-modules is also exact.*

*Proof.* We have to show $\operatorname{im}(\varphi_{i,S}) = \ker(\varphi_{i+1,S})$ for each position $i$. For $x/s \in M_{i-1}[S^{-1}]$ we have $\varphi_{i+1,S}(\varphi_{i,S}(x/s)) = \varphi_{i+1}(\varphi_i(x))/s = 0/s$. This shows the inclusion $\operatorname{im}(\varphi_{i,S}) \subset \ker(\varphi_{i+1,S})$. So let $y/s \in M_i[S^{-1}]$ such that $\varphi_{i+1,S}(y/s) = 0$. Then there is a $t \in S$ with $t\varphi_{i+1}(y) = 0$, so that $\varphi_{i+1}(ty) = 0$. Since we have $\ker(\varphi_{i+1}) = \operatorname{im}(\varphi_i)$ there is an $x \in M_{i-1}$ with $\varphi_i(x) = ty$. Then $y/s = ty/st = \varphi_i(x)/st = \varphi_{i,S}(x/st)$ showing the other inclusion $\ker(\varphi_{i+1,S}) \subset \operatorname{im}(\varphi_{i,S})$. ■

***3.2.11 Exercise.*** Show that a sequence $\cdots \longrightarrow M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \longrightarrow \cdots$ is exact if and only if the sequences $0 \longrightarrow \ker(\varphi_{i+1}) \longrightarrow M_i \longrightarrow \operatorname{im}(\varphi_{i+1}) \longrightarrow 0$ are exact for all $i$ (for which they make sense).

There are some useful, concrete consequences of this general statement. For instance, it implies that localization commutes with intersection or taking a quotient.

***3.2.12 Corollary.*** *Let $S \subset R$ be a multiplicative set.*

(1) *For any submodule $U$ of any $R$-module $M$ we have*

$$(M/U)[S^{-1}] \cong M[S^{-1}]/U[S^{-1}].$$

(2) *For any family $(U_i)_{i\in I}$ of submodules of any $R$-module $M$ we have*

$$\bigcap_{i\in I}(U_i[S^{-1}]) = \left(\bigcap\nolimits_{i\in I} U_i\right)[S^{-1}].$$

*Proof.* Exercise: find helpful exact sequences for the two claims. ■

We next look at ideals of the localization $R[S^{-1}]$ and their relation to ideals of $R$.

***3.2.13 Proposition.*** (1) *For any ideal $J$ in $R[S^{-1}]$ we have $J = \left(\lambda_S^{-1}(J)\right)[S^{-1}]$. The map $J \mapsto \lambda_S^{-1}(J)$ is an injection from the set of ideals in $R[S^{-1}]$ to the set of ideals in $R$.*

(2) *The map $Q \mapsto \lambda_S^{-1}(Q)$ induces a bijection between the set of prime ideals in $R[S^{-1}]$ and the set of prime ideals $P$ of $R$ such that $P \cap S = \emptyset$. The inverse map is $P \mapsto P[S^{-1}]$. This bijection preservers inclusions and intersections.*

*Proof.* Exercise. A useful fact is the statement that the preimage $\varphi^{-1}(Q)$ of any prime ideal $Q \subset S$ and any ring homomorphism $\varphi\colon R \longrightarrow S$ is a prime ideal of $R$. (Why is that true?) Also, remember that the elements of $S \subset R$ become units in $R[S^{-1}]$ (for claim (2)). ■

Combining the previous two statements, we get the following special case (for $R$-modules $U$ that are ideals of $R$).

***3.2.14 Corollary.*** *Let $I \subset R$ be an ideal and $S$ a multiplicative set. There is a canonical isomorphism*

$$(R/I)\big[\overline{S}^{-1}\big] \cong R[S^{-1}]/I[S^{-1}]$$

*where we write $\overline{S} = \{s + I \mid s \in S\} \subset R/I$.* ■

For any prime ideal $P$ of $R$ the set $R \setminus P$ is a multiplicative set. We use the short notation

$$R_P = R[(R \setminus P)^{-1}]$$

for the **localization of $R$ with respect to $P$**. By the discussion above, the rings obtained in this way have the following special property (by Proposition 3.2.13).

***Definition.*** A ring is called **local** if it has a unique maximal ideal.

In fact, Proposition 3.2.13 implies the following result.

***3.2.15 Corollary.*** *For any prime ideal $P \subset R$ of $R$, the set of prime ideals of $R_P$ is in bijection with the prime ideals of $R$ that are contained in $P$. In particular, $R_P$ is a local ring with maximal ideal $PR_P$.* ■

We record just two important observations about local rings (for now...).

***3.2.16 Lemma.*** *Let $R$ be a local ring with maximal ideal $\mathfrak{m}$. We have $R \setminus \mathfrak{m} = R^*$, which means that the units of $R$ are exactly those elements that are not contained in the maximal ideal $\mathfrak{m}$.*

*Proof.* The proof is based on the simple observation that an element $a \in R$ is a unit if and only if $\langle a \rangle = R$ (and the fact that every proper ideal is contained in a maximal ideal by Zorn's Lemma). ■

For domains $R$ (in particular polynomial rings over fields), the localizations $R_P$ are naturally contained in the field $\mathrm{Quot}(R)$ (by Theorem 3.2.10). We can recover $R$ from its localizations in the following sense.

***3.2.17 Lemma.*** *Let $R$ be a domain. For any prime ideal $P$ of $R$ the local ring $R_P$ is a subring of* $\mathrm{Quot}(R)$ *and we have*

$$R \quad = \bigcap_{\substack{\mathfrak{m} \subset R \\ \textit{maximales Ideal}}} R_{\mathfrak{m}}.$$

*Proof.* The inclusion $R \subset \bigcap R_{\mathfrak{m}}$ is direct by exactness of localization. For $x \in \mathrm{Quot}(R) \setminus R$ set $I = \{s \in R \mid sx \in R\}$. Then $I$ is an ideal of $R$ with $1 \notin I$. By Zorn's Lemma, $I$ is contained in a maximal ideal $\mathfrak{m}$ of $R$. We must have $x \notin R_{\mathfrak{m}}$. Indeed, if $x = a/b$ in $\mathrm{Quot}(R)$ for $a, b \in R$, then $bx = a \in R$, which means $b \in I \subset \mathfrak{m}$. ■

## 3.3. Primary decomposition

***Definition.*** An ideal $I$ of $R$ is called **primary** if $I \neq R$ and for all $a, b \in R$ with $a \cdot b \in I$ we have $a \in I$ or there is a $k \in \mathbb{N}$ with $b^k \in I$.

***3.3.1 Example.*** (1) Every prime ideal of every ring is primary.

(2) In $\mathbb{Z}$, the ideals $\langle p^k \rangle$ for any prime $p \in \mathbb{Z}$ and any $k \in \mathbb{N}$ are primary.

***3.3.2 Exercise.*** (1) Show that an ideal $I$ is primary if and only if for all $a, b \in R$ with $a \cdot b \in I$ we have $a \in I$ or $b \in I$ or there is a $k \in \mathbb{N}$ such that both $a^k$ and $b^k$ are in $I$.

(2) Show that an ideal $I$ is primary if and only if every zero divisor of $R/I$ is nilpotent.

***3.3.3 Exercise.*** If $I$ is a primary ideal of $R$, then its radical ideal

$$\sqrt{I} = \{a \in R \mid \exists\, k \in \mathbb{N} \colon a^k \in I\}$$

is a prime ideal of $R$. (We usually say that $I$ is $P$-primary for $P = \sqrt{I}$. e.g. $\langle p^k \rangle$ is $\langle p \rangle$-primary (or just $p$-primary) in $\mathbb{Z}$ for any $k \in \mathbb{N}$.)

***3.3.4 Example.*** The converse of the claim in the above exercise is not true: if the radical of an ideal is prime, it does not need to be primary. Here is a standard example: Let $R = k[x, y, z]/\langle xy - z^2 \rangle$ for a field $k$ and consider $P = \langle \overline{x}, \overline{z} \rangle \subset R$ and $I = \langle \overline{x}^2, \overline{xy}, \overline{xz} \rangle = P^2 \subset R$ so that $\sqrt{I} = P$ by construction. The point is that $I$ is not primary. To see this, take $\overline{xy} = \overline{z}^2 \in I$; since $\overline{y}^k \notin I$ for any $k \in \mathbb{N}$ it follows that $I$ is not primary. (A primary decomposition of $I$ actually is $I = \langle \overline{x} \rangle \cap \langle \overline{x}^2, \overline{xz}, \overline{y} \rangle$.)

The example shows even more strongly that a power of a prime ideal does not need to be primary in general. (In $\mathbb{Z}$, for example, this statement is true.)

More generally, we consider primary ideals associated to $R$-modules in the following sense.

***Definition.*** Let $R$ be a ring and $M$ be an $R$-module. We call a prime ideal $P \subset R$ **associated** to $M$ (or an **associated prime ideal**) if there exists an element $x \in M$ such that $P = \operatorname{Ann}(x)$, that is

$$P = \{a \in R \mid ax = 0 \in M\}.$$

We write $\operatorname{Ass}(M)$ for the set of associated prime ideals.

A prime ideal $P \subset R$ is a **minimal prime ideal** of $M$ if the module $M_P$ is non-trivial and $M_Q = \{0\}$ for each prime ideal $Q \subset R$ properly contained in $P$.

***3.3.5 Exercise.*** Let $I \subset R$ be an ideal. Show that a prime ideal $P \subset R$ is a minimal prime ideal of the $R$-module $R/I$ if and only if $I \subset P$ and there is no prime ideal $Q$ properly contained in $P$ with $I \subset Q$.

If $R$ is noetherian and $M$ is finitely generated (as an $R$-module), then every minimal prime of $M$ is actually an associated prime as well. This statement requires proof (see standard textbooks in commutative algebra, e.g. Matsumura's textbook). Here is a somewhat related statement.

***3.3.6 Exercise.*** An ideal $I \subset R$ of a noetherian ring $R$ is $P$-primary if and only if $\operatorname{Ass}(R/I) = \{P\}$. (We will often write $\operatorname{Ass}(I)$ instead of $\operatorname{Ass}(R/I)$.)

# Chapter 4: Monomial ideals

## 4.1. Basic properties

Let $k$ be a field and write $S = k[x_1, \dots, x_n]$ for the polynomial ring over $K$ (in $n$ variables). The set

$$\operatorname{Mon}(S) = \{x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \mid \alpha \in \mathbb{Z}^n_{\geq 0}\}$$

of **monomials** in $S$ is a basis of $S$ as a $k$-vector space. For a polynomial

$$f = \sum_{u \in \operatorname{Mon}(S)} a_u \cdot u \in S$$

the set $\operatorname{supp}(f) = \{u \in \operatorname{Mon}(S) \mid a_u \neq 0\}$ is the **support** of $f$.

***Definition.*** An ideal $I \subset S$ is a **monomial ideal** if $I$ can be generated by monomials.

***4.1.1 Exercise.*** What is the monomial ideal $\langle t^4, t^7 \rangle \subset k[t]$? It should be a principal ideal since $k[t]$ is a principal ideal domain.

***4.1.2 Proposition.*** *Let $I \subset S$ be a monomial ideal. The set $N$ of monomials contained in $I$ is a $k$-basis of the vector space $I$.*

*Proof.* Exercise. ■

This result has direct, nice consequences. First is an equivalent characterization of monomial ideals.

***4.1.3 Corollary.*** *Let $I \subset S$ be an ideal. The following are equivalent.*

(1) *$I$ is a monomial ideal.*
(2) *For every polynomial $f \in S$ we have $f \in I$ if and only if $\operatorname{supp}(f) \subset I$.* ■

The second is about the quotient as a $k$-vector space.

***4.1.4 Corollary.*** *Let $I \subset S$ be a monomial ideal. The residue classes of all monomials that are not contained in $I$ form a basis of the $k$-vector space $S/I$.* ■

The membership problem for monomials in monomial ideals given by a monomial generating sets is simple.

***4.1.5 Proposition.*** *Let $\{u_1, \dots, u_m\} \subset \mathrm{Mon}(S)$ be a monomial set of generators for a monomial ideal $I \subset S$. Then a monomial $v \in \mathrm{Mon}(S)$ is in $I$ if and only if there exists a monomial $w \in \mathrm{Mon}(S)$ and an $i \in [m]$ such that $v = wu_i$.*

*Proof.* Exercise. ■

This implies that a monomial ideal has a distinguished generating set.

***4.1.6 Proposition.*** *Each monomial ideal of S has a unique minimal set of monomial generators. Concretely, let G be the set of monomials in I which are minimal with respect to divisibility. Then G is the unique minimal set of monomial generators for I.*

*Proof.* Exercise using the previous result on membership test. ■

## *4.2. Algebraic operations*

To recall some results from commutative algebra, we discuss standard algebraic operations of ideals in the special case of monomial ideals $I \subset S$. For a monomial ideal $I \subset S$, write $G(I)$ for the minimal monomial generating set in Proposition 4.1.6.

***4.2.1 Exercise.*** Let $I, J \subset S$ be monomial ideals. Show that $G(I + J) \subset G(I \cup J)$ and $G(IJ) \subset G(I)G(J)$. Conclude that the sum as well as the product of monomial ideals are monomial ideals.

For two monomials $u, v \in \mathrm{Mon}(S)$, write $\mathrm{gcd}(u, v)$ for the greatest common divisor of $u$ and $v$; write $\mathrm{lcm}(u, v)$ for the least common multiple of $u$ and $v$.

***4.2.2 Proposition.*** *Let $I, J \subset S$ be monomial ideals. The intersection $I \cap J$ is a monomial ideal generated by $\{\mathrm{lcm}(u, v) \mid u \in G(I), v \in G(J)\}$.*

*Proof.* For any $f \in I \cap J$, we have $\mathrm{supp}(f) \subset I \cap J$ by Corollary 4.1.3. This equivalence then also shows that $I \cap J$ is actually a monomial ideal.

Now let $w \in \mathrm{supp}(f)$ for $f \in I \cap J$ be a monomial occurring in $f$. Then there is a monomial $u \in G(I)$ dividing $w$ and a monomial $v \in G(J)$ dividing $w$. This implies that $\mathrm{lcm}(u, v)$ divides $w$. ■

***4.2.3 Exercise.*** Is $G(I \cap J) = \{\mathrm{lcm}(u, v) \mid u \in G(I), v \in G(J)\}$ for monomial ideals $I, J \subset S$?

***Definition.*** For ideals $I, J \subset S$, the **colon ideal** is defined as

$$I : J = \{f \in S \mid f \cdot J \subset I\}.$$

***4.2.4 Proposition.*** *For two monomial ideals $I, J \subset S$, the colon ideal $I : J$ is also a monomial ideal. We have*

$$I : J = \bigcap_{v \in G(J)} I : \langle v \rangle$$

*and $\{u/\mathrm{gcd}(u, v) \mid u \in G(I)\}$ is a monomial generating set of $I : \langle v \rangle$.*

*Proof.* Again, we can show that $I\colon J$ is a monomial ideal by using Corollary 4.1.3. The essential point this time is that $\operatorname{supp}(f)v = \operatorname{supp}(fv) \subset I$ for any polynomial $f \in I$ and monomial $v \in G(J)$.

The presentation $I\colon J = \bigcap_{v\in G(J)} I\colon \langle v\rangle$ is direct. The monomial set of generators for $I\colon \langle v\rangle$ is an elementary argument about greatest common divisors. These are left as an exercise. ■

***Definition.*** Let $\mathfrak{m} = \langle x_1,\ldots,x_n\rangle \subset S$ the homogeneous maximal ideal of $S$. The **saturation** of an ideal $I \subset S$ is

$$I\colon \mathfrak{m}^\infty = \bigcup_{k=1}^{\infty} I\colon \mathfrak{m}^k.$$

***4.2.5 Exercise.*** Show that $I\colon \mathfrak{m}^\infty$ is a monomial ideal for every monomial ideal $I \subset S$.

***Definition.*** The **radical** of an ideal $I \subset S$ is the ideal

$$\sqrt{I} = \{f \in S \mid f^k \in I \text{ for some } k \in \mathbb{N}\}.$$

***4.2.6 Proposition.*** *The radial ideal of a monomial ideal is again a monomial ideal.*

*Proof.* We use induction and some basis convex geometry for the proof of this statement. Let $f \in \sqrt{I}$ be a polynomial such that $f^k \in I$. Let us list $\operatorname{supp}(f) = \{x^{\alpha_1},\ldots,x^{\alpha_r}\}$. After relabelling, we can assume that $\alpha_1$ is a vertex of the convex hull of the set $\{\alpha_1,\ldots,\alpha_r\} \subset \mathbb{R}^n$, which means that $\alpha_1$ is not in the convex hull of $\alpha_2,\ldots,\alpha_r$. Suppose we could write

$$(x^{\alpha_1})^k = (x^{\alpha_1})^{k_1}(x^{\alpha_2})^{k_2}\cdot\ldots\cdot(x^{\alpha_r})^{k_r}$$

with $k = k_1+k_2+\ldots+k_r$ and $k_1 < k$. This implies that $\alpha_1$ is a convex combination of $\alpha_2,\ldots,\alpha_r$, namely

$$\alpha_1 = \sum_{i=2}^{r} \frac{k_i}{k-k_1}\alpha_i \text{ with } \sum_{i=2}^{r}\frac{k_i}{k-k_1} = 1.$$

This is a contradiction to the choice of $\alpha_1$ as a vertex of the convex hull of $\operatorname{supp}(f)$. What this means for $f^k$ is that the monomial $x^{k\alpha_1}$ cannot cancel with other terms in $f^k$. Differently put, we have $x^{k\alpha_1} \in \operatorname{supp}(f^k) \subset I$. This shows, using Corollary 4.1.3, $x^{\alpha_1} \in \sqrt{I}$ and hence $f - a_{\alpha_1}x^{\alpha_1} \in \sqrt{I}$. So we can proceed by induction on the number of elements of $\operatorname{supp}(f)$ to show $\operatorname{supp}(f) \subset \sqrt{I}$. The claim then follows from Corollary 4.1.3. ■

***Definition.*** A monomial $x^\alpha \in \operatorname{Mon}(S)$ is called **squarefree** if $\alpha \in \{0,1\}^n$. For $u = x^\alpha \in \operatorname{Mon}(S)$, we write

$$\sqrt{u} = \prod_{i\colon \alpha_i\neq 0} x_i.$$

***4.2.7 Example.*** The notation $\sqrt{u}$ for a monomial has nothing to do with a square root. For instance, we have $\sqrt{x_1^3x_2x_5^7} = x_1x_2x_5$.

***4.2.8 Proposition.*** *For a monomial ideal $I$, the set $\{\sqrt{u} \mid u \in G(I)\}$ is a generating set for the radical $\sqrt{I}$. In particular, a monomial ideal is radical if and only if it has a generating set of squarefree monomials.*

*Proof.* Exercise (using the previous result Proposition 4.2.6). ■

Based on this characterization of monomial radical ideals, we use the following term.

***Definition.*** A monomial ideal is called **squarefree** if it is radical.

## *4.3. Primary decomposition and associated primes*

Here are some general facts from commutative algebra that we will now revisit for monomial ideals. Every ideal $I \subset S$ has a **primary decomposition**

$$I = \bigcap_{i=1}^{m} Q_i$$

for primary ideals $Q_i \subset S$. Such a decomposition is called **irredundant** (or **minimal**) if no ideal in the intersection on the right can be dropped. An ideal $Q \subset S$ is **primary** if for all $a, b \in S$ the condition $ab \in Q$ implies $a \in Q$ or $b \in \sqrt{Q}$. The following statements are correct and can be found in standard textbooks on commutative algebra (e.g. Atiyah, Macdonald): The radical of a primary ideal is prime. The prime ideals $P_i = \sqrt{Q_i}$ in an irredundant primary decomposition of $I$ are unique. The primary ideals $Q_i$ in a primary decomposition of $I$ with the property that the corresponding prime ideal $P_i = \sqrt{Q_i}$ is minimal among these prime ideals are unique.

The following statement shows that every monomial ideal has a primary decomposition into monomial ideals, as we will see throughout this section.

***4.3.1 Theorem.*** *Let $I \subset S$ be a monomial ideal. The ideal $I$ is the intersection $I = \bigcap_{i=1}^{m} Q_i$ of ideals $Q_i$ generated by powers of variables; so each $Q_i$ is of the form $\langle x_{i_1}^{a_1}, \ldots, x_{i_k}^{a_k} \rangle$. There is one unique irredundant representation of this form.*

*Proof.* We first prove existence constructively. Let $G(I) = \{u_1, \ldots, u_r\} \subset \mathrm{Mon}(S)$ be the minimal monomial generating set of $I$ (see Proposition 4.1.6). If $u_1$ is not a power of a variable, then we can write $u_1 = v \cdot w$ for coprime monomials $v, w \in \mathrm{Mon}(S)$. For the ideal $I$ we get $I = I_1 \cap I_2$ for $I_1 = \langle v, u_2, \ldots, u_r \rangle$ and $I_2 = \langle w, u_2, \ldots, u_r \rangle$ (Check!). This shows the existence of an irredundant representation $I = \bigcap_{i=1}^{m} Q_i$ as claimed.

To show uniqueness, suppose $\bigcap_{i=1}^{r} Q_i = \bigcap_{j=1}^{s} Q'_j$. It suffices to show for every $i \in [r]$ that there is some $j \in [s]$ with $Q'_j \subset Q_i$. By symmetry and the fact that both representations are irredundant, we get $r = s$ and $\{Q_1, \ldots, Q_r\} = \{Q'_1, \ldots, Q'_s\}$.

To simplify notation, fix $i \in [r]$ and assume $Q_i = \langle x_1^{a_1}, \ldots, x_k^{a_k} \rangle$. If $Q'_j \not\subset Q_i$, there is a monomial $x_{\ell_j}^{b_j} \in Q'_j \setminus Q_i$. So we have $\ell_j \notin [k]$ or $b_j < a_j$. So in case that

$Q'_j \not\subset Q_i$ for any $j \in [s]$, set

$$u = \operatorname{lcm}\{x_{\ell_1}^{b_1}, \dots, x_{\ell_s}^{b_s}\}.$$

This monomial is in $\bigcap_{j=1}^{s} Q'_j$ by construction and hence in $Q_i$. So $x_i^{a_i}$ divides $u$ for some $i \in [r]$ which is a contradiction. ■

***Definition.*** We call a monomial ideal $I \subset S$ **irreducible** if it cannot be written as the intersection of two other monomial ideals. Otherwise, it is called **reducible**.

***4.3.2 Exercise.*** Find examples for both reducible as well as irreducible monomial ideals.

Use Theorem 4.3.1 to show the following characterization of irreducible monomial ideals.

***4.3.3 Corollary.*** *A monomial ideal is irreducible if and only if it can be generated by monomials that are all powers of variables.* ■

***4.3.4 Example.*** Consider the monomial ideal

$$I = \langle x_1^2x_2, x_1^2x_3^2, x_2^2, x_2x_3^2\rangle \subset k[x_1, x_2, x_3].$$

Following the algorithm in the proof of Theorem 4.3.1, we get

$$\begin{aligned} I &= \langle x_1^2, x_1^2x_3^2, x_2^2, x_2x_3^2\rangle \cap \langle x_2, x_1^2x_3^2, x_2^2, x_2x_3^2\rangle = \langle x_1^2, x_2^2, x_2x_3^2\rangle \cap \langle x_2, x_1^2x_3^2\rangle \\ &= \big(\langle x_1^2, x_2^2, x_2\rangle \cap \langle x_1^2, x_2^2, x_3^2\rangle\big) \cap \big(\langle x_2, x_1^2\rangle \cap \langle x_2, x_3^2\rangle\big) \\ &= \langle x_1^2, x_2^2, x_3^2\rangle \cap \langle x_1^2, x_2\rangle \cap \langle x_2, x_3^2\rangle \end{aligned}$$

***4.3.5 Exercise.*** Use the algorithm in the proof of Theorem 4.3.1 to decompose the monomial ideal $I = \langle x_1x_3, x_2x_4, x_3x_4, x_2x_3\rangle \subset k[x_1, x_2, x_3, x_4]$.

Following the algorithm in the proof of Theorem 4.3.1 for squarefree monomial ideals, we get the following statement.

***4.3.6 Corollary.*** *A squarefree monomial ideal is the intersection of monomial prime ideals.* ■

***Definition.*** A **minimal prime ideal** (or just **minimal prime**) of an ideal $I$ in a ring $R$ is a prime ideal $P$ with $I \subset P$ such that there is no prime ideal $Q$ satisfying $I \subset Q \subsetneq P$. We write $\operatorname{Min}(I)$ for the set of minimal primes of $I$.

***4.3.7 Lemma.*** *If an ideal I has an irredundant presentation $I = P_1 \cap P_2 \cap \ldots \cap P_m$ for prime ideals $P_i$, then $\operatorname{Min}(I) = \{P_1, P_2, \dots, P_m\}$.*

*Proof.* If $P$ is a minimal prime of $I$, then $P_1 \cdot P_2 \cdot \ldots \cdot P_m \subset I \subset P$ implies that $P_i \subset P$ for some $i$. The minimality of $P$ implies $P_i = P$ so that $P \in \operatorname{Min}(I)$.

To show that every $P_i$ is indeed minimial, we use localization, which commutes with intersection. This means that

$$IR_{P_i} = (P_1 \cap \ldots \cap P_m)R_{P_i} = P_iR_{P_i}.$$

If $P_i$ were not a minimal prime ideal, say $I \subset Q \subsetneq P_i$, then $IR_{P_i}$ would be contained in $QR_{P_i}$, which would be a proper subset of $P_iR_{P_i}$, contradiction. ■

This gives us the primary decomposition of radical monomial ideals.

***4.3.8 Corollary.*** *Every minimal prime of a squarefree monomial ideal $I \subset S$ is a monomial ideal so that $I$ is the intersection of monomial prime ideals*

$$I = \bigcap_{P \in \operatorname{Min}(I)} P.$$

*Proof.* Combine the previous two results Corollary 4.3.6 and Lemma 4.3.7. ■

More generally, every monomial ideal has a primary decomposition into monomial ideals. We show this based on Theorem 4.3.1.

***4.3.9 Proposition.*** *The irreducible ideal $\langle x_{i_1}^{a_1}, \dots, x_{i_k}^{a_k} \rangle$ is primary with radical $\langle x_{i_1}, \dots, x_{i_k} \rangle$.*

*Proof.* Set $Q = \langle x_{i_1}^{a_1}, \dots, x_{i_k}^{a_k} \rangle$ and $P = \langle x_{i_1}, \dots, x_{i_k} \rangle$. We have $Q \subset P$ and also $P^m \subset Q$ for $m = \sum_{i=1}^k a_i$. So $P$ is the only minimal prime ideal of $Q$. This implies $\sqrt{Q} = P$. What is left is to show that $Q$ is primary. If the product $uv$ is in $Q$ for two monomials $u, v \in \operatorname{Mon}(S)$, then $x_{i_j}^{a_j}$ divides $uv$ for some $j \in [k]$. If $x_{i_j}^{a_j}$ divides $u$, then $u \in Q$. Otherwise, $v$ must be divisible by $x_{i_j}$ so that $v^k \in Q$ for some sufficiently large $k$. To check the definition more generally, suppose $f \cdot g \in Q$ for some polynomials $f, g \in Q$. Since $Q$ is a monomial ideal, we have $u \cdot v \in Q$ for all $u \in \operatorname{supp}(f)$ and all $v \in \operatorname{supp}(g)$ with $uv \in \operatorname{supp}(fg)$. If $f \notin Q$, then we can assume that $u \notin Q$ for all $u \in \operatorname{supp}(f)$ (by replacing $f$ by $f - \sum_{u \in \operatorname{supp}(f) \cap Q} a_u u$). Then recursion on the monomials in $\operatorname{supp}(g)$ shows that each monomial in $\operatorname{supp}(g)$ is divisible by one of the variables $x_{i_j}$, which implies that $g^k \in Q$ for some sufficiently large $k \in \mathbb{N}$. ■

Now we know that every monomial ideal is the intersection of irreducible monomial ideals by Theorem 4.3.1 and that irreducible monomial ideals are primary by Proposition 4.3.9. This shows primary decomposition of monomial ideals into monomial ideals.

***4.3.10 Example.*** Following the algorithm in the proof of Theorem 4.3.1 for the monomial ideal

$$I = \langle x_1^3, x_2^3, x_1^2x_3^2, x_1x_2x_3^2, x_2^2x_3^2 \rangle \subset k[x_1, x_2, x_3]$$

we get the irredundant presentation as the intersection of irreducible monomial ideals $I = \langle x_1^3, x_2^3, x_3^2 \rangle \cap \langle x_1^2, x_2 \rangle \cap \langle x_1, x_2^2 \rangle$. The two ideals $\langle x_1^2, x_2 \rangle$ and $\langle x_1, x_2^2 \rangle$ have the same radical (so that $\operatorname{Ass}(\langle x_1^2, x_2 \rangle) = \{\langle x_1, x_2 \rangle\} = \operatorname{Ass}(\langle x_1, x_2^2 \rangle)$). The irredundant primary decomposition is therefore

$$I = \langle x_1^3, x_2^3, x_3^2 \rangle \cap \langle x_1^2, x_1x_2, x_2^2 \rangle.$$

The primary decomposition obtained in this way, using the algorithm in the proof of Theorem 4.3.1 and then coarsening it to an irredundant primary decomposition, is unique and called the **standard primary decomposition**. It is in general not the only one.

***4.3.11 Exercise.*** Find a monomial ideal with at least two primary decompositions. Determine the standard one and show that there is at least one more. (Recall that the primary ideals associated to minimal primes are always unique; the example needs embedded components for this to have a chance to work.)

Here are a few consequences for primary decompositions of monomial ideals.

***4.3.12 Corollary.*** *The associated prime ideals of a monomial ideal are also monomial ideals.* ■

***4.3.13 Corollary.*** *For any monomial ideal $I \subset S$ and any associated prime $P \in \mathrm{Ass}(I)$ there exists a monomial $u \in S$ such that $P = I \colon \langle u \rangle$.*

*Proof.* We use here that for every associated prime ideal $P \in \mathrm{Ass}(I)$ there exists an element $f \in S$ such that $P = I \colon \langle f \rangle$. That we can choose $f$ to be a monomial now follows from the irreducibility of monomial prime ideals as follows. For each variable $x_i \in P$ we have $x_i f \in I$ because $P = I \colon \langle f \rangle$. Since $I$ is a monomial ideal, this implies that $x_i u \in I$ for all $u \in \mathrm{supp}(f)$. In terms of colon ideals, this says

$$P = I \colon \langle f \rangle \subset \bigcap_{u \in \mathrm{supp}(f)} I \colon \langle u \rangle.$$

Conversely, for $g \in \bigcap_{u \in \mathrm{supp}(f)} I \colon \langle u \rangle$ we have $ug \in I$ for all $u \in \mathrm{supp}(f)$ and hence $fg \in I$ meaning $g \in I \colon \langle f \rangle = P$. Overall, we have $P = \bigcap_{u \in \mathrm{supp}(f)} I \colon \langle u \rangle$. Since $P$ is an irreducible ideal, the claim follows. ■

## 4.4. Squarefree monomial ideals and simplicial complexes

***Definition.*** A **simplicial complex** on the set $[n] = \{1, 2, \ldots, n\} \subset \mathbb{N}$ is a collection $\Delta$ of subset of $[n]$ such that for every $F \in \Delta$ and $F' \subset F$ we have $F' \in \Delta$. The ground set $[n]$ is called the **vertex set** of $\Delta$. The elements $F \in \Delta$ are called the **faces** of the simplicial complex.

In some sources the additional property $\{i\} \in \Delta$ for all $i \in [n]$ is required for a simplicial complex. This property naturally holds for many classes of examples, especially geometric examples.

***4.4.1 Example.*** (1) A central class of examples are **triangulations** (in algebraic topology, for instance). A basic version is given by triangulations of a convex polytope (e.g. in the plane).

(2) From a graph $G = ([n], E)$ we can construct the **clique complex** of $G$. This is the simplicial complex $\Delta$ on $[n]$ with faces $F \subset [n]$ such that the induced graph $(F, E|_F)$ is a complete graph (aka clique).

(Draw pictures for these examples!)

***Definition.*** The **dimension** (occasionally also rank) $\dim(F)$ of a face $F$ of a simplicial complex $\Delta$ is the number $|F| - 1 \in \mathbb{N}_0$. The dimension $\dim(\Delta)$ of $\Delta$ is the largest dimension of any face of $\Delta$. Faces of dimension 1 are called **edges** of $\Delta$; faces of dimension 0 are called **vertices**. A **facet** of $\Delta$ is an inclusion maximal element of $\Delta \subset 2^{[n]}$. We write $\mathcal{F}(\Delta)$ for the set of facets of $\Delta$.

A simplicial complex is called **pure** if all facets have the same dimension (or equivalently the same number of elements).

A simplicial complex $\Delta$ on $[n]$ is uniquely determined by its facets. Given the facets $F_1, \ldots, F_k$ of $\Delta$ we can directly reconstruct

$$\Delta = \{F \subset [n] \mid \exists\, j \in [k] \colon F \subset F_j\}.$$

More generally, given elements $G_1, \ldots, G_m \in \Delta$, we write $\langle G_1, \ldots, G_m \rangle$ for the simplicial complex of subset of the $G_j$, i.e.

$$\langle G_1, \ldots, G_m \rangle = \{G \subset [n] \mid \exists\, j \in [m] \colon G \subset G_j\}.$$

***Definition.*** A **non-face** of a simplicial complex on $[n]$ is a subset $F \subset [n]$ such that $F \notin \Delta$. We write $\mathcal{N}(\Delta)$ for the set of minimal non-faces (with respect to inclusion in $2^{[n]}$).

***4.4.2 Example.*** For $\Delta \subset 2^{[5]}$ with $\mathcal{F}(\Delta) = \{\{1,2,4\}, \{1,2,5\}, \{2,3\}, \{3,4\}\}$ we have $\dim(\Delta) = 2$ and $\mathcal{N}(\Delta) = \{\{1,3\}, \{3,5\}, \{4,5\}, \{2,3,5\}\}$.

The primary combinatorial data that we are interested in here is the number faces organized by dimension.

***Definition.*** Let $\Delta$ be a simplicial complex on $[n]$ of dimension $d$. We write $f_i(\Delta)$ for the number of $i$-dimensional faces of $\Delta$. The $f$-**vector** of $\Delta$ is the sequence

$$f(\Delta) = (f_0(\Delta), f_1(\Delta), \ldots, f_d(\Delta)).$$

We set $f_{-1} = 1$.

In algebraic topology, triangulations are used to give a definition of the **Euler characteristic** $\chi(X)$ of a topological space $X$. It is, by definition, the alternating sum of the entries of the $f$-vector.

***4.4.3 Example.*** Let $\Delta = 2^{[n]}$ be the trivial simplicial complex. Topologically, this is the ball of dimension $n$, so it is homotopy equivalent to a point. The $f$-vector of $\Delta$ is given by $f_i(\Delta) = \binom{n}{i+1}$ for $i = 0, 1, \ldots, n-1$. It follows that the Euler characteristic $\chi(\Delta)$ of $\Delta$ is 1 because

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} = (1-1)^n = 0.$$

For the Euler characteristic of the sphere of dimension $n-2$, we take the simplicial complex $\Delta'$ on $[n]$ whose facets are the subsets with $n-1$ elements. In other words, $\mathcal{N}(\Delta') = \{[n]\}$. The Euler characteristic $\chi(\Delta')$ of $\Delta'$ can be determined the same way. Now, however, we have to distinguish whether $n$ is even or odd

$$\chi(\Delta') = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ 2 & \text{if } n \text{ is even.} \end{cases}$$

***Definition.*** Let $\Delta$ be a simplicial complex on $[n]$ and let $S = k[x_1, \dots, x_n]$ be a polynomial ring in $n$ variables over a field $k$. For each subset $F \subset [n]$ we write

$$x_F = \prod_{i \in F} x_i$$

for the monomial corresponding to the indicator function of $F$. We define the **Stanley-Reisner ideal** of $\Delta$ to be

$$I_\Delta = \langle x_F \mid F \in \mathcal{N}(\Delta) \rangle$$

the ideal generated by the monomials corresponding to the minimal non-faces of $\Delta$. The **Stanley-Reisner ring** of $\Delta$ is the quotient $S/I_\Delta$.

***4.4.4 Exercise.*** Show the following statements. For every non-face $F$ of $\Delta$ we have $x_F \in I_\Delta$. For every face $F$ of $\Delta$ we have $x_F \notin I_\Delta$.

In fact we have the following result.

***4.4.5 Proposition.*** *The monomials $u = x^\alpha \in \mathrm{Mon}(S)$ such that $\{i \in [n] \mid \alpha_i \neq 0\} \in \Delta$ are a basis of the $K$-vector space $S/I_\Delta$.*

*Proof.* By Corollary 4.1.4 it suffices to show that $u = x^\alpha \notin I_\Delta$ if and only if $F_u = \{i \in [n] \mid \alpha_i \neq 0\} \in \Delta$. We show this by contraposition. So first, let $u = x^\alpha \in \mathrm{Mon}(S)$ be a monomial such that $F_u \notin \Delta$. Then we have $u \in I_\Delta$ because $u$ is then divisible by a monomial $x_F$ for a non-face $F$ of $\Delta$. Indeed, if $F_u \notin \Delta$ it contains a minimal non-face $F \in \mathcal{N}(\Delta)$; then $u$ is a multiple of $x_F$. Conversely, if $u \in \mathrm{Mon}(S)$ is in $I_\Delta$, then it is a multiple of a generator of $I_\Delta$ by Proposition 4.1.5. By definition, the generators of $I_\Delta$ are the monomials $x_F$ for $F \in \mathcal{N}(\Delta)$ so that we have $u = v \cdot x_F$ for some minimal non-face $F \in \mathcal{N}(\Delta)$. This implies $F \subset F_u$ and therefore $F_u \notin \Delta$. ■

To wrap up this introductory section to monomial ideals, we collect some exercises to recall some important points.

***4.4.6 Exercise.***

(1) Let $I \subset S$ be a monomial ideal. Show that $S/I$ is a finite-dimensional vector space if and only if for all $i \in [n]$ there is an $a_i \in \mathbb{N}$ with $x_i^{a_i} \in I$.

(2) Compute the dimension of the $k$-vector space $S/I$ for $I = \langle x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n} \rangle$ as a function of the $a_i \in \mathbb{N}$.

(3) Write $P_F = \langle x_i \mid i \in F \rangle$ for any subset $F \subset [n]$. For any $d \in [n]$ find the minimal monomial generating set $G(I)$ for

$$I = \bigcap_{F\,:\,|F|=d} P_F.$$

(4) Fix an integer $d \in \mathbb{N}$ and let $I_d \subset S$ be the ideal generated by all monomials $x^\alpha$ with $\sum_{i=1}^n \alpha_i = d$ and $\alpha_i < d$ for all $i$. Find the radical $\sqrt{I_d}$ of $I_d$.

(5) Find the standard primary decomposition of the ideals $I_d \subset k[x_1, x_2, x_3]$ defined in the previous problem for $n = 3$.

## 4.5. Graded modules and Hilbert functions

***Definition.*** Let $k$ be a field and $R = \bigoplus_{i \geq 0} R_i$ a graded $k$-algebra. Elements of $R_i$ are called **homogeneous elements** of degree $i$. We call $R$ **standard graded** if $R$ is a finitely generated $k$-algebra and there is a generating set of elements of degree 1.

***4.5.1 Example.*** The polynomial ring $R = k[x_1, \dots, x_n]$ with the usual grading $\deg\colon k[x_1, \dots, x_n] \to \mathbb{Z}_{\geq 0}$, $\deg(x_i) = 1$ for $i = 1, 2, \dots, n$ is a standard graded $k$-algebra.

A module $M$ over a graded $k$-algebra $R$ is an $R$-module $M$ with a decomposition $M = \bigoplus_{j \in \mathbb{Z}} M_j$ as $k$-vector spaces such that $f M_j \subset M_{j+d}$ for every homogeneous element $f \in R_d$. Here is an example. Write $S = k[x_1, \dots, x_n]$ for the polynomial ring with its standard degree grading. Recall that an ideal $I \subset S$ is **homogeneous** if it is a graded $S$-module, i.e. $I = \bigoplus_{i \geq 0} I_d$, where $I_d = I \cap S_d$. Equivalently, an ideal is homogeneous if it has a generating set of homogeneous polynomials.

***4.5.2 Proposition.*** *Every standard graded $k$-algebra $R$ is isomorphic to the quotient $k[x_1, \dots, x_n]/I$ of a suitable polynomial ring modulo a homogeneous ideal $I \subset k[x_1, \dots, x_n]$.* ■

***Definition.*** The **Hilbert function** of a finitely generated graded module $M$ over a standard graded $k$-algebra $R$ is the (numerical) function $H(M, -)\colon \mathbb{Z} \to \mathbb{Z}$, $i \mapsto \dim_k(M_i)$, where $\dim_k(M_j)$ is the dimension of the $j$th graded piece of $M$ as a $k$-vector space. The generating (formal Laurent) series of the Hilbert function

$$H_M(t) = \sum_{i \in \mathbb{Z}} H(M, i) t^i \in k((t))$$

is called the **Hilbert series** of $M$.

***4.5.3 Exercise.*** Show that the dimension $\dim_k(M_i)$ is finite for every finitely generated graded module $M$ over a standard graded algebra $k$ and every $i \in \mathbb{Z}$.

***4.5.4 Example.*** The Hilbert function of $S = k[x_1, \dots, x_n]$ is

$$H(S, d) = \binom{n + d - 1}{d} = \binom{n + d - 1}{n - 1}.$$

This implies that (actually is equivalent to) the Hilbert series of $S$ is

$$H_S(t) = \frac{1}{(1 - t)^n}.$$

***Definition.*** Let $R$ be a ring. Then, we define the **Krull dimension** of $R$ as the supremum of the length of all ascending chains of prime ideals ordered by inclusion. For an $R$-module $M$ we define its **Krull dimension** by setting

$$\dim M = \dim\left(\frac{R}{\operatorname{Ann}(M)}\right).$$

***4.5.5 Example.*** (1) The Krull dimension of any field is 0, as it only contains two distinct ideals only one of which is prime.

(2) The Krull dimenson of $\mathbb{C}[t]$ equals one, as all of the prime ideals are of the form $\langle t-a\rangle$ for $a \in \mathbb{C}$. Hence, $\langle 0\rangle \subset \langle t-a\rangle \subset \langle t-b\rangle$ if and only if $a = b$.

(3) Let $M$ be a faithful $\mathbb{C}[t]$ module, that is $\operatorname{Ann}(M) = \{0\}$. Then, its Krull dimension is 1, as $\mathbb{C}[t]/\operatorname{Ann}(M) \simeq \mathbb{C}[t]$.

***4.5.6 Exercise.*** (1) What is the Krull dimension of $\mathbb{Z}$? What is the Krull dimension of any principal ideal domain? What is the dimension of $\mathbb{Z}[t]$?

(2) Let $M$ be a $R$ module of dimension $d$, and $y$ of degree one in $R$ such that it is not contained in any minimal prime in $\operatorname{Ass}(M)$. What is the dimension of $M/yM$? Hint: Use Krulls principal ideal theorem.

(3) Let $M$, and $y \in R$ as above. What is $Ann(M)$, when we consider $M$ as a $k[y]$ module? What is the dimension of $M$?

Now we go on a slight tangent, by introducing a very handy tool to study dimensions of monomial ideals.

***4.5.7 Proposition.*** *Let $I \subset S$ be a proper monomial ideal, then the set of monomials of $S$ not lying in $I$ can be written as a finite (but not necessarily disjoint) union of translates of coordinate subspaces of $\mathbb{N}^n$.*

***4.5.8 Proposition.*** *Let $I$ be a proper monomial ideal in $S$. Then, for all $i \in \mathbb{N}$, the number of monomials not in $I$ of total degree $\leq i$ equals $H(S/I, i)$. In particular, the Krull dimension of $S/I$ is the dimension of the largest subspace of monomials not in the ideal $I$.*

***4.5.9 Example.*** Let $I = \langle x^2y^5, x^4y^3\rangle \subset k[x,y]$. Then, we can read off from Figure 4.1, that the set $C(I)$ of monomials not contained in $I$ can be written as

$$\begin{aligned} C(I) =&[e_1] \cup (e_2 + [e_1]) \cup (2e_2 + [e_1]) \cup [e_2] \cup (e_1 + [e_2]) \\ &\cup [(3,4)] \cup [(3,3)] \cup [(2,4)] \cup [(2,3)], \end{aligned}$$

where $[-]$ denotes the $\mathbb{Z}$ span.

Now lets turn to one of Hilbert's most famous theorems.

***4.5.10 Theorem*** (Hilbert). *Let $k$ be a field, $R$ a standard graded $k$-algebra and $M$ a nonzero, finitely generated, graded $R$-module of (Krull) dimension $d$. Then,*

*(1) there exists a Laurent-polynomial $\mathrm{Q}_M(t) \in \mathbb{Z}(t)$ with $\mathrm{Q}_M(1) > 0$ such that*

$$\mathrm{H}_M(t) = \frac{\mathrm{Q}_M(t)}{(1-t)^d}.$$

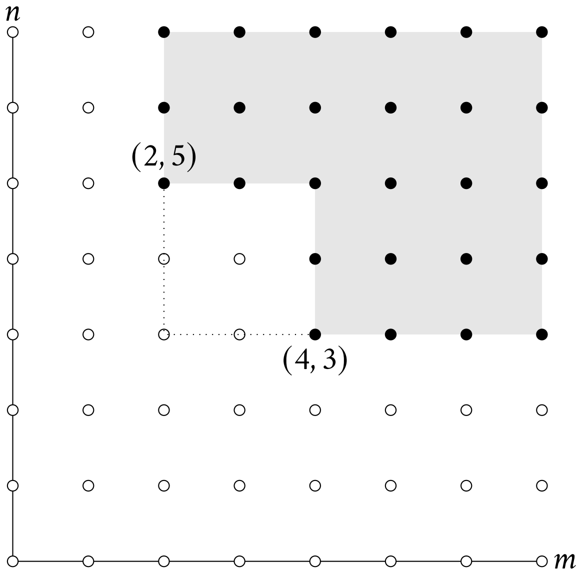

Figure 4.1: Visualisation of monomials under the identification of $(m,n) \leftrightarrow x^m y^n$. Black lattice points in the grey shaded area correspond to monomials in $I$, white points to those which do not lie in $I$.

(2) *there exists a polynomial* $\mathrm{P}_M(x) \in \mathbb{Q}[x]$ *of degree* $d-1$ *(called the Hilbert polynomial of* $M$*) such that*

$$\mathrm{H}(M,i) = \mathrm{P}_M(i)$$

*for all* $i > \deg \mathrm{Q}_M(t) - d$.

*Proof.* Notice that we can switch to an infinite field by extending $k$. We proceed by induction. If $d = \dim(M) = 0$, then $M_i = 0$ for large $i$, and the claims become trivial.

So, let $d > 0$. Now we choose a degree one element $y$ in $R$ such that it does not belong to any minimal prime in $\mathrm{Ass}(M)$. This means that the multiplication map $y : M_{i-1} \longrightarrow M_i$ is injective for $i$ large enough. By $M(-1)$ let us denote the module with its grading shifted by $-1$, further let $\mathrm{Ann}(y) = \{m \in M \mid ym = 0 \in M\}$.

Then, the exact sequence

$$0 \longrightarrow \mathrm{Ann}(y)(-1) \longrightarrow M(-1) \xrightarrow{y} M \longrightarrow M/yM \longrightarrow 0$$

is graded such that we get the following exact sequence of $k$-vector spaces

$$0 \longrightarrow \mathrm{span}_k \mathrm{Ann}(y)_{i-1} \longrightarrow \mathrm{span}_k M_{i-1} \xrightarrow{y^*} \mathrm{span}_k M_i \longrightarrow \mathrm{span}_k (M/yM)_i \longrightarrow 0$$

for all $i \in \mathbb{N}$. Using the rank-nullity theorem this implies

$$0 = H_{M/yM}(t) - H_M(t) + tH_M(t) - H_{\mathrm{Ann}(y)(-1)}(t).$$

Therefore,

$$H_M(t) = \frac{H_{M/yM}(t) - H_{\mathrm{Ann}(y)(-1)}(t)}{1-t}.$$

Now, by our choice of $y$ and Krull's principal ideal theorem it follows that the dimension of $(M/yM)$ equals $d-1$, because $y$ is not contained in any of the minimal primes. Therefore, we can apply the induction hypothesis to $H_{M/yM}(t)$, so there exists a Laurent polynomial $Q_{M/yM}(t)$ which evaluates positively on 1, such that

$$H_{M/yM}(t) = \frac{Q_{M/yM}(t)}{(1-t)^{d-1}}.$$

Hence, we can define a Laurent polynomial $Q_M(t)$ by setting

$$H_M(t) = \frac{Q_{M/yM}(t)(1-t)^{d-1} - H_{\mathrm{Ann}(y)(-1)}(t)}{1-t} = \frac{Q_M(t)}{(1-t)^d}.$$

This also shows that $Q_M(1) > 0$ for $d > 1$, so it remains to consider the case where $d = 1$. Notice this condition holds if and only if the length of $\mathrm{Ann}(y)$ is smaller than the length of $M/yM$. To that end, first notice $M$ is a $k[y]$ module, and then recall from a previous exercise, that, as such, $M/yM$ has finite length, because $M$ is noetherian, implying that $M$ is finitely generated. Moreover, $M$ is a one dimensional module over $k[y]$, as $\mathrm{Ann}(M) \subset k[y]$ is empty, again by our choice of $y$. Then, we may apply the structure theorem for modules over PIDs, which gives us $M \simeq k[y]^r \oplus \bigoplus_{j=1}^{s} k[y]/\langle y^{a_j}\rangle$ where $a_j \in \mathbb{N}$, and $r > 0$ because $M$ is one dimensional. Finally, notice that the length of $\mathrm{Ann}(y)$ is precisely $s$, and that of $M/yM$ is $r+s$. This proves part (1).

For the second claim, we write $Q_M(t) = \sum_{i=r}^{s} h_i t^i$ where $h_i$ are integer coefficient polynomials. Then, using the properties of binomial coefficients, we get

$$H_M(t) = \frac{\sum_{i=r}^{s} h_i t^i}{(1-t)^d} = \sum_{i=r}^{s} h_i t^i \sum_{j\in\mathbb{N}} \binom{d+j-1}{d-1} t^j.$$

Hence,

$$H(M,i) = \sum_{j=r}^{s} h_j \binom{d+(i-j)-1}{d-1}.$$

Then, we simply set

$$P_M(x) = \sum_{j=r}^{s} h_j \binom{x+d-j-1}{d-1},$$

and notice that this polynomial has the correct properties; that is, it is of degree $d$ in $x$ and $H(M,i) = P_M(i)$ for $i > s-d$. This completes the proof. ■

Our next goal will be to discuss Macaulays theorem, but in order to do so we need a few more notions from commutative algebra.

***Definition.*** A **monomial ordering** $<$ on $S$ is a relation $<$ on $\mathbb{N}^n$, or equivalently, a relation on the set of monomials $x^\alpha$ , $\alpha \in \mathbb{N}^n$ , satisfying:

(1) $<$ is a total (or linear) ordering on $\mathbb{N}^n$.

(2) If $\alpha > \beta$ and $\gamma \in \mathbb{N}^n$ , then $\alpha + \gamma > \beta + \gamma$.

(3) $<$ is a well-ordering on $\mathbb{N}^n$. This means that every nonempty subset of $\mathbb{N}^n$ has a smallest element under $>$. In other words, if $A \subset \mathbb{N}^n$ is nonempty, then there is $\alpha \in A$ such that $\beta > \alpha$ for every $\beta \neq \alpha \in A$.

***4.5.11 Example.*** The standard monomial order is the **(graded) lexicographic ordering**. It is defined by setting $x^\alpha <_{\text{lex}} x^\beta$if either $|\alpha| < |\beta|$ or $|\alpha| = |\beta|$ and the left most entry of $\alpha - \beta$ is negative. So for example, when $S = k[x_1, x_2]$, $\alpha = (1,1)$ and $\beta = (1,2)$, then $x^\alpha <_{\text{lex}} x^\beta$. Grvlex ususally used for computations as it (almost all the times) reduces the time Buchbergers algorithm for computing Groebner bases takes to terminate.

***4.5.12 Exercise.*** Verify that $<_{\text{lex}}$ is indeed a monomial order. What is the smallest element?

***Definition.*** Let $<$ be a monomial order on $\text{Mon}(S)$ and $f \in S$. Then, we define the **initial monomial** of $f = \sum_{i=1}^s c_i x^{\alpha_i} \in S$ wrt. $<$ by

$$\text{in}_<(f) = \max_<\{x^{\alpha_i} \in \text{Mon}(S) \mid c_i \neq 0\}.$$

For an ideal $I \subset S$ we write $\text{in}_<(I)$ for the ideal generated by $\text{in}_<(g)$ for all $g \in I$.

It is important to note that for an ideal $I \subset S$ generated by $f_1, \dots f_r$ the initial ideal $\text{in}_<(I)$ does not necessarily equal $\langle \text{in}_<(f_1), \dots, \text{in}_<(f_r)\rangle$.

***4.5.13 Exercise.*** Can you find an ideal in a univariate polynomial ring which does not have this property? Find an ideal $I \subset \mathbb{R}[x,y]$ which does not have this property.

This motivates the following definition.

***Definition.*** Let $I$ be an ideal in $S$ and fix a monomial order $<$. We say a generating set $G = \{g_1, \dots, g_s\}$ for $I$ is a **Gröbner basis** of $I$ wrt. to the monomial order $<$ if $\text{in}_<(I) = \langle \text{in}_<(g_1), \dots, \text{in}_<(g_s)\rangle$.

Let us record a few important properties of Gröbner basis which we will need at a later point.

***4.5.14 Proposition.*** *Let $I$ be an ideal in $S$ and $<$ a monomial order.*

(1) *There exists a Gröbner basis for $I$.*

(2) *Polynomial division wrt. to a Gröbner basis $G$ is unique. In particular, a polynomial is contained in $I$ if and only if its remainder wrt. $G$ vanishes.*

***4.5.15 Exercise.*** Let $f = x^2y + xy^2 + y^2$. Then divide $f$ by the ordered tuple $(g_1, g_2)$ where $g_1 = xy - 1$ and $g_2 = y^2 - 1$, and compare that with the result when you divide $f$ by $(g_2, g_1)$.

***4.5.16 Theorem*** (Macaulay). *The set of monomials* $\text{Mon}(S) \setminus \text{in}_<(I)$ *form a $k$-basis of $S/I$.*

*Proof.* Let $G = \{g_1, \dots, g_r\}$ be a Gröbner basis of $I$, and let $f \in S$. Then, $f$ has a unique remainder $r$ with respect to $G$. The residue class of $f$ modulo $I$ is the same as that of $r$, and no monomial in the support of $r$ is divided by any of the monomials $\mathrm{in}_<(g_i)$, which follows from the division algorithm. This shows that $\mathrm{Mon}(S) \setminus \mathrm{Mon}(\mathrm{in}_<(I))$ is a system of generators of the $k$-vector space $S/I$. Assume there exists a set $\{u_1, \dots, u_s\} \subset \mathrm{Mon}(S)\setminus\mathrm{Mon}(\mathrm{in}_<(I))$ and $a_i \in k\setminus\{0\}$ such that $h = \sum_{i=1}^{s} a_i u_i \in I$. We may assume that $u_1 = \mathrm{in}_<(h)$. Then $u_1 = \mathrm{in}_<(h) \in \mathrm{Mon}(\mathrm{in}_<(I))$, a contradiction. ■

***4.5.17 Corollary.*** *Let $I \subset S$ be a graded ideal and $<$ a monomial order on $S$. Then $S/I$ and $S/\mathrm{in}_<(I)$ have the same Hilbert function, i.e. $H(S/I, i) = H(S/\mathrm{in}_<(I), i)$ for all $i$.*

***4.5.18 Corollary.*** *Let $G = \{g_1, \dots, g_r\}$ be a homogeneous system of generators of $I$, and let $J = \langle \mathrm{in}_<(g_1), \dots, \mathrm{in}_<(g_r)\rangle$. Then $G$ is a Gröbner basis of $I$ if and only if $S/I$ and $S/J$ have the same Hilbert function.*

*Proof.* If $G$ is a Gröbner basis then $J = I$. If it is not then, $J \subset \mathrm{in}_<(I)$, such that $H(S/J, i) > H(S/\mathrm{in}_<(I), i) = H(S/I, i)$ for all $i$. Hence, the Hilbert function will differ. ■

## 4.6. Free resolutions

We have seen earlier in this course that not all modules do come with a basis; those were precisely modules which are not free. The first goal of this section is therefore to remedy this shortcoming by introducing a series of free modules over any module - called free resolution. Secondly, we then want use these resolutions to find the Hilbert series of modules. However, before we start with the setup, it is important to note that description of free resolutions comes in two flavours. Those, where the finitely generated modules are over standard graded $k$-algebras and those where they are modules over local rings. Whereas the latter is the more general notion, the former is more applicable in our context. Hence, we choose here to introduce the notion over graded $k$-algebras and then explain how to move between them.

Let $M$ be a finitely generated standard graded $S$-module with homogeneous generators $m_1, \dots, m_r$ and $\deg(m_i) = a_i$ for $i \in [r]$. Further, let $F_0 = \bigoplus_{i=1}^{r} Se_i$ be a free module over $S$ of rank $r$. Then, there exists a surjective $S$-module homomorphism $F_0 \longrightarrow M$ with $e_i \mapsto m_i$. If we assign to $e_i$ the degree $a_i$ for $i \in [r]$, then $F_0$ becomes isomorphic to $\bigoplus_{i=1}^{r} S(-a_i)$ and we obtain the short exact sequence (SES)

$$0 \longrightarrow U \hookrightarrow \bigoplus_j S(-j)^{\beta_{0j}} \longrightarrow M \longrightarrow 0,$$

where $\beta_{0j} = |\{i \mid a_i = j\}|$, and $U = \ker\left(\bigoplus_j S(-j)^{\beta_{0j}} \to M\right)$ such that the sequence is exact indeed. (Note that the $\beta_{0j}$ simply collect all copies of $S$ whose degrees are shifted by $j$.) The module $U$ is a graded submodule of $F_0 = \bigoplus_j S(-j)^{\beta_{0j}}$.

Since $M$ was finitely, generated we know that $U$ is also finitely generated. Therefore, we can apply the same construction as above again to find a surjective homomorphism $\bigoplus_j S(-j)^{\beta_{1j}} \to U$. (Notice the power $\beta_{1j}$ here.) Composing this map with the inclusion map $U \hookrightarrow \bigoplus_j S(-j)^{\beta_{0j}}$ we obtain the exact sequence

$$\bigoplus_j S(-j)^{\beta_{1j}} \longrightarrow \bigoplus_j S(-j)^{\beta_{0j}} \longrightarrow M \longrightarrow 0$$

of graded $S$-modules. Proceeding in this way, and setting $F_i = \bigoplus_j S(-j)^{\beta_{ij}}$, we obtain a long exact sequence

$$\cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

of graded $S$-modules.

***Definition.*** Let $M$ be a finitely generated graded $S$-module as above and $F_i = \bigoplus_j S(-j)^{\beta_{ij}}$. Then, a long exact sequence

$$\mathbb{F} : \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

is called a **graded free $S$-resolution** of $M$. Moreover, the powers $\beta_{ij}$ are called **graded Betti numbers**, and the **$i$-th Betti number** $\beta_i$ is defined as $\beta_i = \sum_j \beta_{ij}$.

***4.6.1 Example.*** Consider $S$ as an module over itself. Then, $S^n \to S \to 0$ is a graded free $S$-resolution of $S$. However, so is $S^{n+1} \to S \to 0$. This shows that free resolutions are not at all unique.

***4.6.2 Exercise.*** (1) Let $M$ be as above. Is the sequence

$$\bigoplus_j S(-j)^{\beta_{1j}} \longrightarrow \bigoplus_j S(-j)^{\beta_{0j}} \longrightarrow M \longrightarrow 0$$

exact at every position?

(2) What does the $i$-th Betti number count?

We have seen that free resolutions are not unique. However, if, in each step, we choose the resolution minimally, the overall chain will be unique up to isomorphism, motivating the following definition.

***Definition.*** Let $M$ be a finitely generated $S$-module. Then, we call a set of homogeneous generators $m_1, \dots, m_r$ of $M$ **minimal** if no proper subset of it generates $M$. Moreover, a graded free S-resolution F of M is called **minimal free resolution** if for all $i$, the image of $F_{i+1} \to F_i$ is contained in $\mathfrak{m}F_i$, where $\mathfrak{m} = \langle x_1, \dots, x_n \rangle \subset S$.

For this definition to make sense we need the following statement, which asserts a relation between minimal generators and the containment condition in the submodules $\mathfrak{m}F_i$.

***4.6.3 Lemma.*** *Let $m_1, \dots, m_r$ be a homogeneous set of generators of the graded $S$-module $M$. Let $F_0 = \bigoplus_{i=1}^r Se_i$ and $\varepsilon : F_0 \to M$ be the surjective homomorphism with $e_i \mapsto m_i$ for $i \in [r]$. Then, the following conditions are equivalent:*

*(1)* *$m_1, \dots, m_r$ are minimal generators of $M$*

*(2)* $\ker(\varepsilon) \subseteq \mathfrak{m}F_0$*, where* $\mathfrak{m} = \langle x_1, \dots, x_n \rangle \subset S$

*Proof.* First, suppose $\ker(\varepsilon) \nsubseteq \mathfrak{m}F_0$. Then, there exists a homogeneous element $f = \sum_{i=1}^r f_i e_i \in \ker(\varepsilon)$ such that $f \notin \mathfrak{m}F_0$. Since elements in $\mathfrak{m}F_0$ are degree 1 or higher, at least one of the coefficients $f_i$ must be of degree 0, wlog. $\deg f_1 = 0$ and $f_1 \in K \setminus 0$. Therefore, it follows that

$$m_1 = f_1^{-1} f_2 m_2 + \cdots + f_1^{-1} f_r m_r,$$

but then $m_2, \dots, m_r$ would already generate $M$, contradicting our assumption.

For the converse, suppose that $\ker(\varepsilon) \subset \mathfrak{m}F_0$, further wlog. suppose that $m_1$ can be omitted, such that $m_2, \dots, m_r$ is a system of generators of $M$ as well. Then, we have $m_1 = \sum_{i=2}^r \widetilde{f_i} m_i$ for suitable homogeneous elements $\widetilde{f_i} \in S$. Next, we consider

$$f = e_1 - \sum_{i=2}^r \widetilde{f_i} e_i,$$

which is in $\in \ker(\varepsilon)$. However, since the coefficient of $e_1$ is of degree 0, we see that $f \notin \mathfrak{m}F_0$. Thus, contradicting our assumption. ■

***4.6.4 Corollary.*** *Every finitely generated standard graded $S$-module admits a minimal free resolution.*

As alluded to at the beginning of this section, we could have defined minimal free resolutions over local rings $(O, P)$. We can do this by saying that such a resolution is minimal if the images of the maps in the chain complex are contained in $P\widetilde{F_i}$, where the $\widetilde{F_i}$ are modules over $O$. Now, recall that every maximal ideal $\mathfrak{m}$ in a commutative ring $R$ with 1 is prime, hence the localization at $\mathfrak{m}$ yields a local ring $(R_\mathfrak{m}, \mathfrak{m}R_\mathfrak{m})$. Furthermore, for every $R$-module $M$, localization at $\mathfrak{m}$ yields a module over $R_\mathfrak{m}$. Now, since any standard graded $k$-algebra $R$ is isomorphic to a quotient of $S$, we know that $R$ does not contain a unique maximal ideal, however there is a unique **homogeneous** maximal ideal $\mathfrak{m} = \bigoplus_{i \geq 1} R_i$. So there is a canonical way of passing from a standard graded $k$-algebra to a local ring. Finally, notice, if we do so, $x \in \mathfrak{m}F_i$ if and only if $x \in (\mathfrak{m}S_\mathfrak{m})\widetilde{F_i}$, where $\widetilde{F_i} = (F_i)_\mathfrak{m}$. Then, upon combinations of these observations, we see that the definitions align.

To get a non-trivial but finite example of a minimal free resolution it is most convenient to introduce a few more notions.

***Definition.*** Let $\Delta$ be a simplicial complex with vertex set $[n]$. Then, we define the **reduced chain complex** of $\Delta$ over a field $k$ as the complex $\widetilde{C_\bullet}(\Delta; k)$ as

$$0 \longrightarrow k^{F_{n-1}(\Delta)} \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_{i+1}} k^{F_i(\Delta)} \xrightarrow{\partial_i} k^{F_{i-1}(\Delta)} \xrightarrow{\partial_{i-1}} \cdots \xrightarrow{\partial_0} k^{F_{-1}(\Delta)} \longrightarrow 0,$$

where $F_i(\Delta)$ denotes the set of faces of dimension $i$. Its **boundary maps** are defined by

$$\partial_i(e_\sigma) = \sum_{j \in \sigma} \operatorname{sign}(j, \sigma) e_{\sigma \setminus j},$$

where $\sigma \in \Delta$ and $\operatorname{sign}(j, \sigma) = (-1)^{r-1}$ when $j$ is the $r$-th element of $\sigma$.

***4.6.5 Exercise.*** Verify that this is indeed a chain complex. That is, show that $\operatorname{im}\partial_i \subset \ker \partial_{i-1}$ i.e. $\partial_{i-1}\circ\partial_i = 0$.

***4.6.6 Example.*** The reduced chain complex for the simplicial complex given by $\Delta \subset 2^{[5]}$ with $\mathcal{F}(\Delta) = \{\{1,2,3\},\{2,4\},\{3,4\},\{5\}\}$ is

$$0 \longrightarrow k \xrightarrow[\partial_2]{\begin{bmatrix}1\\-1\\1\\0\\0\end{bmatrix}} k^5 \xrightarrow[\partial_1]{\begin{bmatrix}-1&-1&0&0&0\\1&0&1&1&0\\0&1&1&0&-1\\0&0&0&1&1\\0&0&0&0&0\end{bmatrix}} k^5 \xrightarrow[\partial_0]{\begin{bmatrix}1&1&1&1&1\end{bmatrix}} k \longrightarrow 0,$$

with respect to the canonically ordered basis.

***Definition.*** The **Koszul complex** $\mathbb{K}_\bullet(n)$ is the complex of free modules over $S$ whose boundary maps are derived as follows:

(1) Start with the reduced chain complex of the simplicial complex consisting of all subsets $\sigma$ of $[n]$.

(2) For every face $\sigma \in F_i$ label the columns and rows of the boundary maps corresponding to $e_\sigma$ by $\sigma$.

(3) Renumber the homological degree such that the empty set $\varnothing$ sits in homological degree 0.

***4.6.7 Example.*** The Koszul complex for $n = 3$ is given as:

$$\mathbb{K}_\bullet(3):\quad 0 \longrightarrow S \xrightarrow{\begin{array}{c|c} & xyz\\ \hline xy & 1\\ xz & -1\\ yz & 1\end{array}} S^3 \xrightarrow{\begin{array}{c|ccc} & xy & xz & yz\\ \hline x & -1 & -1 & 0\\ y & 1 & 0 & -1\\ z & 0 & 1 & 1\end{array}} S^3 \xrightarrow{\begin{array}{c|ccc} & x & y & z\\ \hline 1 & 1 & 1 & 1\end{array}} S \longrightarrow 0$$

***4.6.8 Exercise.*** Write down the Koszul complex for $n = 4$.

***4.6.9 Proposition.*** *The Koszul complex $\mathbb{K}_\bullet(n)$ is a minimal free graded $S$-resolution of $S/\mathfrak{m}$ where $\mathfrak{m} = \langle x_1,\dots,x_n\rangle$.*

Now, let us apply everything we have learned about minimal resolutions to Hilbert series. To that end, let

$$\mathbb{F}: 0 \longrightarrow F_p \longrightarrow F_{p-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

be a graded minimal free $S$-resolution of $M$ with

$$F_i = \bigoplus_j S(-j)^{\beta_{ij}} = \bigoplus_{j=1}^{\beta_i} S(-d_{ij}),$$

where suitable $d_{ij} \in \mathbb{N}$. Recall, from the proof of Theorem 4.5.10 that the Hilbert function is additive on SES. More precisely, for the SES of $S$-modules from above

$$0 \longrightarrow U_{i+1} \hookrightarrow F_i \longrightarrow U_i \longrightarrow 0,$$

we get $H(F_0, i) = H(U_{i+1}, i) + H(U_i, i)$. Now notice that, closely following the construction detailed at the beginning of this section, we can extend $\mathbb{F}$ by diagonally inserting the SES from the display above. Next, we note that the shifted Hilbert series of $S$ is $H_{S(-j)}(t) = t^j/(1-t)^n$. Combining these two observations allows us to write down the Hilbert series of $M$ as follows

$$H_M(t) = \frac{R_M(t)}{(1-t)^n},$$

where $R_M(t) = \sum_{i=0}^{p}(-1)^i \sum_j \beta_{ij} t^j = \sum_{i=0}^{p}(-1)^i \sum_{j=1}^{\beta_i} t^{d_{ij}}$.

## 4.7. Face counting and Hilbert functions

We begin to study the relationship between the Hilbert function (or, more generally the Betti numbers) of a Stanley-Reisner ring and the enumerative combinatorics of the corresponding simplicial complex.

We saw in Theorem 4.5.10 that the Hilbert function of a finitely generated graded module $M$ over a standard graded algebra $R$ is a rational function

$$H_M(t) = \frac{Q_M(t)}{(1-t)^d}$$

where $Q_M(t)$ is a Laurent polynomial with integer coefficients, say $Q_M(t) = \sum_{i=r}^{s} h_i t^i$.

***Definition.*** We call the coefficient vector $(h_r, h_{r+1}, \dots, h_s)$ of $Q_M(t) \in \mathbb{Z}[t, t^{-1}]$ the $h$-**vector** of the graded module $M$.

The goal of this section is to relate the $h$-vector of the Stanley-Reisner algebra $K[\Delta] = S/I_\Delta$ with the $f$-vector of the simplicial complex $\Delta$. For this, we consider $K[\Delta]$ as a graded module $M$ over the standard graded algebra $S = K[x_1, \dots, x_n]$.

***4.7.1 Proposition.*** *Let $\Delta$ be a simplicial complex of dimension $d-1$ and write its $f$-vector as $(f_0, f_1, \dots, f_{d-1})$ (meaning that $f_i = f_i(\Delta)$ is the number of $i$-dimensional faces of $\Delta$). Then the Hilbert function of $K[\Delta]$ is*

$$H_{K[\Delta]}(t) = \frac{\sum_{i=0}^{d} f_{i-1} t^i (1-t)^{d-i}}{(1-t)^d}.$$

*Proof.* For a monomial $u = x^\alpha \in \mathrm{Mon}(S)$ we write $\mathrm{supp}(u) = \{i \in [n] : \alpha_i \neq 0\}$ for the set of variables that actually occur in the monomial $u$. By Proposition 4.4.5, the set $B$ of all $u \in \mathrm{Mon}(S)$ such that $\mathrm{supp}(u) \in \Delta$ is a $K$-basis of $K[\Delta]$. We partition this basis by the faces of $\Delta$ so that we can compute the Hilbert function $H_{K[\Delta]}$ in terms of the faces. So for any face $F \in \Delta$ we have

$$\{u \in \mathrm{Mon}(S) \mid \mathrm{supp}(u) = F\} = \{x_F \cdot v \mid v \in \mathrm{Mon}\left(K[\{x_i\}_{i \in F}]\right)\}.$$

As claimed, the basis $B$ of $K[\Delta]$ is the disjoint union of these sets

$$B = \bigsqcup_{F \in \Delta} \{u \in \mathrm{Mon}(S) \mid \mathrm{supp}(u) = F\}$$

so that the dimension of $K[\Delta]$ in dimension $t$ is the sum of the dimensions of $K[\{x_i\}_{i\in F}]_{t-|F|}$ over all faces $F$ of $\Delta$. Since $H_{K[\{x_i\}_{i\in F}]} = \frac{1}{(1-t)^{|F|}}$ and Hilbert functions are additive, we get the desired formula

$$H_{K[\Delta]}(t) = \sum_{F\in\Delta} \frac{t^{|F|}}{(1-t)^{|F|}} = \frac{\sum_{i=0}^{d} f_{i-1}t^i(1-t)^{d-i}}{(1-t)^d}.$$

■

***4.7.2 Corollary.*** *If $\Delta$ is a simplicial complex of dimension $d-1$, then the Stanley-Reisner ring $K[\Delta]$ has Krull dimension $d$.* ■

***4.7.3 Exercise.*** Give a direct proof of the inequality $\dim(K[\Delta]) \geq d$. Can you also prove the other inequality directly?

***Definition.*** The **multiplicity** $e(M)$ of a finitely generated graded module $M$ over a standard graded algebra $R$ is $Q_M(1)$ with the same notation $H_M(t) = Q_M(t)/(1-t)^d$ as before.

***4.7.4 Corollary.*** *Let $\Delta$ be a simplicial complex of dimension $d-1$. Its Euler characteristic is $\chi(\Delta) = (-1)^{d-1}h_d + 1$ and the multiplicity of the Stanley-Reisner ring is $e(K[\Delta]) = f_{d-1}$.*

***4.7.5 Exercise.*** Do the necessary computations for $H_{K[\Delta]}$ to prove the previous statement.

Our next goal is a result due to Macaulay characterizing the numerical functions $h\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ that are Hilbert functions of standard graded algebras.

***4.7.6 Lemma.*** *Fix a positive integer $j$. Any positive integer $a$ has a unique expansion*

$$a = \binom{a_j}{j} + \binom{a_{j-1}}{j-1} + \ldots + \binom{a_k}{k}$$

*where $a_j > a_{j-1} > \ldots > a_k \geq k \geq 1$.*

***4.7.7 Exercise.*** Suppose $j = 2$. Compute this expansion for $a = 5$ and $a = 12$.

*Proof.* Existence follows by induction: choose $a_j$ as large as possible with the property that $a \geq \binom{a_j}{j}$. Then we set $a' = a - \binom{a_j}{j}$ and continue inductively until we reach 0. The only subtlety is to show $a_j > a_{j-1}$ (exercise).

We show uniqueness by induction on $a$ showing that $a_j$ is indeed the largest integer such that $a \geq \binom{a_j}{j}$. For $a = 1$, this is clear. So let $a > 1$ and assume $\binom{a_j+1}{j} \leq a$. Then

$$a' = \sum_{i=k}^{j-1} \binom{a_i}{i} \geq \binom{a_j+1}{j} - \binom{a_j}{j} = \binom{a_j}{j-1} \geq \binom{a_{j-1}+1}{j-1}$$

which is in contradiction to the induction hypothesis. This implies the claim now by recursively applying this argument. ■

***Definition.*** We call the expansion of $a$ in Lemma 4.7.6 the **binomial expansion of** $a$ **with respect to** $j$. We define the integer

$$a^{\langle j\rangle} = \binom{a_j+1}{j+1} + \binom{a_{j-1}+1}{j} + \ldots + \binom{a_k+1}{k+1}.$$

***4.7.8 Exercise.*** Compute the integers $5^{\langle 2\rangle}$ and $12^{\langle 2\rangle}$.

***4.7.9 Exercise.*** Show that $a^{\langle j\rangle} \geq b^{\langle j\rangle}$ for any positive integer $j$ and any positive integers $a \geq b$.

With the binomial expansion, we can at least state Macaulay's Theorem.

***4.7.10 Theorem*** (Macaulay). *Let $h\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ be a function. The following statements are equivalent.*

(1) *$h$ is the Hilbert function $H_R$ of a standard graded $K$-algebra $R$.*

(2) *$h(0) = 1$ and $h(j+1) \leq h(j)^{\langle j\rangle}$ for all $j > 0$.*

## 4.8. Alexander duality

For a simplicial complex $\Delta \subset [n]$, we define its **Alexander dual** as

$$\Delta^\vee = \{[n] \setminus F \mid F \notin \Delta\} = \{F \subset [n] \mid [n] \setminus F \notin \Delta\}.$$

***4.8.1 Lemma.*** *The set $\Delta^\vee \subset [n]$ is a simplicial complex and we have*

$$(\Delta^\vee)^\vee = \Delta.$$

*Proof.* That $\Delta^\vee$ is itself a simplicial complex is direct: For any $F' \subset F$ and $F \in \Delta^\vee$ we have $[n] \setminus F \notin \Delta$ and $[n] \setminus F \notin \Delta$ and $[n] \setminus F \subset [n] \setminus F'$. Since $\Delta$ is a simplicial complex, this implies $F' \in \Delta^\vee$. Biduality $(\Delta^\vee)^\vee = \Delta$ is clear. ■

***4.8.2 Exercise.*** Check the following description of the set of faces of the Alexander dual complex $\Delta^\vee$.

$$\mathcal{F}(\Delta^\vee) = \{[n] \setminus F \mid F \in \mathcal{N}(\Delta)\}$$

Write $\overline{\Delta}$ for the simplicial complex generated by the complements of faces of $\Delta$, in symbols

$$\overline{\Delta} = \langle [n] \setminus F \mid F \in \mathcal{F}(\Delta)\rangle.$$

We use the notation

$$\begin{aligned} I_\Delta &= \langle x_F \mid F \in \mathcal{N}(\Delta)\rangle \text{ and} \\ I(\Delta) &= \langle x_F \mid F \in \mathcal{F}(\Delta)\rangle \end{aligned}$$

for the Stanley-Reisner ideal and the **facet ideal** of $\Delta$.

***4.8.3 Exercise.*** Compute the Alexander dual as well as the associated Stanley-Reisner ideals and facet ideals for the simplicial complex $\Delta \subset [5]$ with faces

$$\mathcal{F}(\Delta) = \langle \{1,2,3\}, \{2,3,4\}, \{3,5\}, \{4,5\}\rangle.$$

***4.8.4 Exercise.*** The Stanley-Reisner ideal of the Alexander dual of a simplicial complex $\Delta$ is the facet ideal of the simplicial complex $\overline{\Delta}$, i. e., we have $I_{\Delta^\vee} = I(\overline{\Delta})$.

***4.8.5 Exercise.*** Compute the standard primary decomposition of the Stanley-Reisner ideal $I_\Delta$ of a simplicial complex $\Delta$. Derive from this the minimal monomial generating set $G(I_{\Delta^\vee})$ for the Alexander dual.
*Hint:* It can be written in terms of the prime ideals $P_F = \langle x_i \mid i \in F \rangle$ for the faces $F$ of some associated simplicial complex.

# Chapter 5: Hochster's formula

The goal of this chapter is to show Hochster's formula relating Betti numbers of monomial ideals to the (co-)homology of the simplicial complex. This requires some abstract nonsense that we mostly summarize only briefly.

## 5.1. Modules over the exterior algebra

The basic setup in this section is the following. We fix a field $K$ and an $n$-dimensional vector space $V$ over $K$, usually $V = K^n$ with its standard basis $e_1, e_2, \ldots, e_n$. We write $E = \bigwedge V = \bigoplus_{i=0}^n \bigwedge^i V$ for the exterior algebra. Then $E$ is a standard graded (non-commutative) $K$-algebra with $E_1 = V$ and the relation $v \wedge v = 0$ for every $v \in V$.

***5.1.1 Exercise.*** The $K$-vector space $\bigwedge^k V$ is spanned by the vectors $e_F = e_{i_1} \wedge \ldots \wedge e_{i_k}$ for all $k$-element subsets $F = \{i_1, i_2, \ldots, i_k\} \subset [n]$ whose elements are ordered $i_1 < \ldots < i_k$. These basis vectors satisfy the relation

$$e_F \wedge e_G = \begin{cases} (-1)^\sigma(F,G) e_{F\cup G} & \text{if } F \cap G = \emptyset \\ 0 & \text{otherwise.} \end{cases}$$

where we write $\sigma(F, G)$ for the number of pairs $(i, j)$ with $i \in F$, $j \in G$, and $i > j$.

***Definition.*** A **graded $E$-module** is a finite-dimensional $K$-vector space $M$ satisfying the following properties.

(1) $M = \bigoplus_i M_i$ is a direct sum of $K$-vector spaces $M_i$.
(2) $M$ is a left and a right $E$-module.
(3) For all integers $i$ and $j$ and all $f \in E_i$ and $x \in M_j$ we have $fx \in M_{i+j}$ and $fx = (-1)^{ij} xf$.

***5.1.2 Example.*** $E = \bigwedge V$ is a graded $E$-module with respect to the usual decomposition $\bigwedge V = \bigoplus_i \bigwedge^i V$ as above.

Our primary examples of graded $E$-modules are quotients of $E$ by submodules associated to simplicial complexes.

***5.1.3 Construction.*** Let $\Delta \subset [n]$ be a simplicial complex. For every face $F \in \Delta$ we define the associated **monomial** $e_F = e_{i_1} \wedge \ldots \wedge e_{i_k}$ for $F = \{i_1, \ldots, i_k\}$ and $i_1 < \ldots < i_k$. Write $J_\Delta$ for the $E$-submodule of $E$ generated by the monomials $e_F$, $F \in \Delta$. Write $K\{\Delta\}$ for the quotient $E/J_\Delta$. We call this $E$-module the **exterior face ring** of $\Delta$.

***5.1.4 Exercise.*** Show that $J_\Delta$ is a graded ideal of $E$ so that the exterior face ring $K\{\Delta\}$ is a graded $K$-algebra. Moreover, show that the dimension of $K\{\Delta\}_i$ as a $K$-vector space is equal to $f_{i-1}(\Delta)$, the number of $(i-1)$-dimensional faces of $\Delta$ (for each $i$).

Next, we want to discuss duality of graded $E$-modules. The fact that $E$ is not commutative makes this more technical than we might be used to. We have to keep track of multiplication from left or right throughout the process. Let $M$ and $N$ be graded $E$-modules. We write

$$^*\mathrm{Hom}_E(M,N) = \bigoplus_i \mathrm{Hom}_E(M,N)_i,$$

where $\mathrm{Hom}_E(M,N)_i$ is the set of all homogeneous $E$-module homomorphisms $\varphi\colon M \longrightarrow N$ of degree $i$. We make this set into an $E$-module with multiplication defined as follows. For any $f \in E$ and any $\varphi \in {}^*\mathrm{Hom}_E(M,N)$ define $(f\varphi)(x) = \varphi(xf)$ and $(\varphi f)(x) = \varphi(x)f$ for all $x \in M$.

***5.1.5 Exercise.*** Show that this definition satisfies property (3) in the definition of a graded $E$-module.

We set $M^\vee = {}^*\mathrm{Hom}_E(M,E)$ and $M^* = {}^*\mathrm{Hom}_K(M,K(-n))$, where $K(-n)$ is the $E$-module $M$ with $M_n = K$ and $M_j = \{0\}$ for $j \neq n$ – this is the $E$-module obtained from the $E$-module $K$ by shifting the grading. In other words, $(M^*)_j$ is isomorphic to $\mathrm{Hom}_K(M_{n-j},K)$ for all $j$. Here, $M^*$ is a graded $E$-module with left multiplication defined by $(f\varphi)(x) = \varphi(xf)$ for all $x \in M$, as before, abd right multiplication defined by $\varphi f = (-1)^{ij} f\varphi$ for any $\varphi \in (M^*)_j$ and any $f \in E_i$ (so that property (3) holds by definition).

***5.1.6 Exercise.*** What is $E^\vee$?

***5.1.7 Construction.*** Let $M$ be a graded $E$-module. For $\varphi \in M^\vee$, we define $\varphi_F\colon M \longrightarrow K(-n)$ for any $F \subset [n]$ as follows. For $x \in M$ we have $\varphi(x) = \sum_{F\subset[n]} \varphi_F(x)e_F$ with $\varphi_F(x) \in K$ for all $F \subset [n]$ because $\varphi$ is a map from $M$ to $E$. Since $\varphi$ is in particular a linear map of $K$-vector spaces, each $\varphi_F$ is a $K$-linear map $\varphi_F\colon M \longrightarrow K(-n)$.

***5.1.8 Theorem.*** *The map $M^\vee \longrightarrow M^*$, $\varphi \mapsto \varphi_{[n]}$, is a functorial isomophism of graded $E$-modules.*

*Proof.* This is mostly abstract nonsense and some elementary computations in linear algebra using the above definitions of module structures. ■

***5.1.9 Corollary.*** *(1) The functor $M \mapsto M^\vee$ is contravariant and exact.*

*(2) We have $(M^\vee)^\vee \cong M$ and $\dim_K(M) = \dim_K(M^\vee)$ for all graded $E$-modules $M$.* ■

***5.1.10 Proposition.*** *Let $\Delta \subset [n]$ be a simplicial complex. The following identities of graded $E$-modules hold.*

*(1)* $0 \colon_E J_\Delta = J_{\Delta^\vee}$;

(2) $K\{\Delta\}^\vee = J_{\Delta^\vee}$ *and* $(J_\Delta)^\vee = K\{\Delta^\vee\}$.

*Proof.* The first claim is elementary, using that $0\colon_E J_\Delta$ is again a monomial ideal, from $e_F \in 0\colon_E J_\Delta$ if and only if $F \cap G \neq \emptyset$ for all $G \notin \Delta$.

The second claim follows from dualizing the exact sequence

$$0 \to J_\Delta \to E \to K\{\Delta\} \to 0$$

defining the exterior face ring $K\{\Delta\}$ to obtain the exact sequence

$$0 \to K\{\Delta\}^\vee \to E^\vee \to (J_\Delta)^\vee \to 0.$$

Identifying $K\{\Delta\}$ and $0\colon_E J_\Delta$ and using the first claim then gives the second claim. ■

## 5.2. Simplicial homology

Originally homology has been introduced as a tool, informally speaking, to measure the number of holes in the boundary of manifolds. Our exposure here is more abstractly formulated in the language of modules over the exterior algebra.

Let $M$ be a graded $E$-module and fix $v \in V = E_1$. We write $(M, v)$ for the complex

$$\ldots \xrightarrow{v} M_{i-1} \xrightarrow{v} M_i \xrightarrow{v} M_{i+1} \xrightarrow{v} \ldots$$

of finitely generated $K$-vector spaces, where each map is given by (left-)multiplication with $v$. The $i$**th homology** of this complex, denoted by $H_i(M, v)$, is defined to be

$$H_i(M, v) = \ker(M_i \xrightarrow{v} M_{i+1})/\operatorname{im}(M_{i-1} \xrightarrow{v} M_i).$$

***5.2.1 Exercise.*** Why is $(M, v)$ a complex?

***5.2.2 Exercise.*** Show that we get for every short exact sequence $0 \to N \to M \to P \to 0$ of graded $E$-modules a long exact sequence of in homology, namely

$$\cdots \to H_i(N, v) \to H_i(M, v) \to H_i(P, v) \to H_{i+1}(N, v) \to \ldots$$

by constructing the **connecting morphisms** $H_i(P, v) \to H_{i+1}(N, v)$.

To define the $i$-th cohomology, we take the dual complex $(M, v)^*$

$$\ldots \xrightarrow{v^*} \operatorname{Hom}_K(M_{i+1}, K) \xrightarrow{v^*} \operatorname{Hom}_K(M_i, K) \xrightarrow{v^*} \operatorname{Hom}_K(M_{i-1}, K) \xrightarrow{v^*} \ldots$$

and take its $i$-th homology so that

$$H^i(M, v) = \ker(M_i^* \xrightarrow{v^*} M_{i-1}^*)/\operatorname{im}(M_{i+1}^* \xrightarrow{v^*} M_i^*),$$

where we used the notation $M_i^* = \operatorname{Hom}_K(M_i, K)$. Thus, we call $H^i(M, v)$ the $i$**-th cohomology** of $(M, v)$.

***5.2.3 Exercise.*** Show that $\mathrm{Hom}_K(H^i(M,v),K)$ is (functorially) isomorphic to $H_i(M,v)$. Dually, the same statement holds for $\mathrm{Hom}_K(H_i(M,v),K)$ and $H^i(M,v)$.

***5.2.4 Proposition.*** *Let $M$ be a graded $E$-module. Then there is an isomorphism from $H^i(M^\vee,v)$ to $H_{n-i}(M,v)$ for all $i \in [n]$.*

*Proof.* The main argument is that the following diagram of maps given in the above Theorem 5.1.8 is commutative.

$$\begin{tikzcd}
(M^\vee)_{i-1} \arrow[r, "\alpha_{i-1}"] \arrow[d, "v"'] & \mathrm{Hom}_K(M_{n-i+1},K) \arrow[d, "(-1)^{n-i}v^*"] \\
(M^\vee)_i \arrow[r, "\alpha_i"'] & \mathrm{Hom}_K(M_{n-i},K)
\end{tikzcd}$$

■

***Definition.*** Let $\Delta \subset [n]$ be a simplicial complex and set $e = \sum_{i=1}^n e_i \in V$. We define the $i$-th **reduced simplicial homology** of $\Delta$ with values in $K$ as $\widetilde{H}_i(\Delta;K) = H_{i+1}(K\{\Delta\},e)$ and the $i$-th **reduced simplicial cohomology** of $\Delta$ with values in $K$ as $\widetilde{H}^i(\Delta;K) = H^{i+1}(K\{\Delta\},e)$.

***5.2.5 Exercise.*** Show that there are functorial isomorphisms from $\widetilde{H}_i(\Delta;K)$ to $\mathrm{Hom}_K\left(\widetilde{H}^i(\Delta;K),K\right)$ and dually from $\widetilde{H}^i(\Delta;K)$ to $\mathrm{Hom}_K\left(\widetilde{H}_i(\Delta;K),K\right)$. In particular, it follows that $\widetilde{H}_i(\Delta;K)$ has the same dimension as a $K$-vector space as $\widetilde{H}^i(\Delta;K)$.

***5.2.6 Proposition*** (Alexander duality). *Let $\Delta \subset [n]$ be a simplicial complex. For each $i \in [n]$ there is a functorial isomorphism*

$$\widetilde{H}^{i-2}(\Delta^\vee;K) \cong \widetilde{H}_{n-i-1}(\Delta;K).$$

*Proof.* This follows essentially from Proposition 5.2.4 and Exercise 5.2.3. ■

## *5.3. Hochster's formula*

First, we have to fix some notation. For $a \in \mathbb{Z}^n$ the numbers

$$\beta_{i,a}(I_\Delta) = \dim_K H_i(K\{\mathbb{K}^a(I_\Delta)\};e)$$

are called the **multigraded** or $\mathbb{Z}^n$**-graded Betti numbers** of $I_\Delta$. An element $a \in \mathbb{Z}^n$ is called **squarefree** if $a$ has only the integers 0 and 1 as possible entries. We set $\mathrm{supp}(a) = \{i \mid a_i \neq 0\}$. Moreover, let $\Delta \subset 2^{[n]}$ be a simplicial complex and $W = \mathrm{supp}(a)$, then we define the restriction of a simplicial complex by

$$\Delta_W = \{F \subseteq [n] \mid F \subseteq W\}.$$

Finally, let

$$\mathbb{K}^a(I_\Delta) = \{F \subset [n] \mid x^{a-\varepsilon(F)} \in I_\Delta\}$$

be the **upper Koszul simplicial complex** of $I_\Delta$ in degree $a$, where , where $\varepsilon(F) \in \{0,1\}^n$ such that $\operatorname{supp}(\varepsilon(F)) = F$.

***5.3.1 Exercise.*** Show that $\Delta_W$ and $\mathbb{K}^a(I_\Delta)$ are simplical complexes.

Now we can state the fundamental theorem of Hochster, which gives a very useful description of the $\mathbb{Z}^n$-graded Betti numbers of a Stanley–Reisner ideal.

***5.3.2 Theorem*** (Hochster). *Let $\Delta$ be a simplicial complex and $a \in \mathbb{Z}^n$. Then we have:*

*(a) $H_i(K\{\mathbb{K}^a(I_\Delta)\}; e) = 0$ if $a$ is not squarefree;*

*(b) if $a$ is squarefree and $W = \operatorname{supp}(a)$, then*

$$H_i(K\{\mathbb{K}^a(I_\Delta)\}; e) \cong \widetilde{H}^{|W|-i-2}(\Delta_W; K) \quad \textit{for all } i$$

*Proof.* We start with a bit of setup. For $F \subseteq [n]$, $F = \{j_0 < j_1 < \cdots < j_i\}$, we set $e_F = e_{j_0} \wedge e_{j_1} \wedge \cdots \wedge e_{j_i}$. Then, the elements $e_F$ with $F \subseteq [n]$ and $|F| = i$ form a basis of the free $S$-module $\mathbb{K}_i(n)$; the $i$-th homology part of the Koszul complex. Then, in $i$-th homology of the corresponding chain complex, the vector space $C_i(\mathbb{K}^a(I_\Delta); K)$, has a basis given by

$$x^b e_F, \quad b + \varepsilon(F) = a, \quad \operatorname{supp}(b) \not\subseteq \Delta.$$

Next, define the following simplicial complex

$$\Delta_a = \{F \subseteq [n] : F \subseteq \operatorname{supp}(a) \wedge \operatorname{supp}(a \setminus \varepsilon(F)) \notin \Delta\}.$$

Further, let $\widetilde{C}_\bullet(\Delta_a; K)[-1]$ be the reduced chain complex of $\Delta_a$ shifted by $-1$ in homological degree, that is $\widetilde{C}_i(\Delta_a; K)[-1] = \widetilde{C}_{i-1}(\Delta_a; K)$. Then we obtain an isomorphism of complexes

$$\alpha : \widetilde{C}_\bullet(\Delta_a; K)[-1] \longrightarrow C_\bullet(\mathbb{K}^a(I_\Delta); K)$$

where each

$$\alpha_i : \widetilde{C}_{i-1}(\Delta_a; K) \to C_i(\mathbb{K}^a(I_\Delta); K), \quad F = [j_0, j_1, \ldots, j_{i-2}] \mapsto x^{a-\varepsilon(F)} e_F$$

is a vector space isomorphism. Note that we can think of $\mathbb{K}^a(I_\Delta)$ as an $E = \bigwedge K^n$-module via its exterior face ring $K\{\mathbb{K}^a(I_\Delta)\}$. This induces an isomorphism in homology

$$\widetilde{H}_{i-1}(\Delta_a; K) \cong H_i(K\{\mathbb{K}^a(I_\Delta)\}; e),$$

where $e = \sum_{j=1}^{|F|} e_j$, and again to emphasise $W = \operatorname{supp}(a)$. We begin with the proof of $(a)$: Suppose $a$ is not squarefree. Then there exists $j$ such that $a_j > 1$. We define $a(r) = (a_1, \ldots, a_j + r, \ldots, a_n)$ for $r \geq 0$. Since $\Delta_a$ depends only on the support of $a$ we get $\Delta_a = \Delta_{a(r)}$ for all $r \geq 0$. Moreover, $H_i(K\{\mathbb{K}^a(r)(I_\Delta)\}; e)$, has only finitely many nonzero graded components there exists $r \gg 0$ such that $H_i(K\{\mathbb{K}^{a(r)}(I_\Delta)\}; e)_, = 0$. Thus, by the isomorphism above, we have

$$H_i(K\{\mathbb{K}^a(I_\Delta)\}; e), \cong \widetilde{H}_{i-1}(\Delta_a; K) = \widetilde{H}_{i-1}(\Delta_{a(r)}; K) \cong H_i(K\{\mathbb{K}^{a(r)}(I_\Delta)\}; e) = 0.$$

It remains to prove $(b)$. Let $a \in \mathbb{Z}^n$ squarefree with $W = \operatorname{supp}(a)$. Then $F \in \Delta_a$ if and only if $F \subseteq W$ and $W \setminus F \not\subseteq \Delta_a$. This is equivalent to saying that $(\Delta_W)^\vee = \Delta_a$. Thus, it follows by Alexander duality, i.e. Proposition 5.2.6, that

$$H_i(K\{\mathbb{K}^a(I_\Delta\}; e) \cong \widetilde{H}_{i-1}((\Delta_W)^\vee; K) \cong \widetilde{H}^{|W|-i-2}(\Delta_W; K),$$

as desired. ■