Utrecht University

# Hilbert's Syzygy Theorem

## Thesis Mathematics BSc

---

---

*Student:*
Rodin Salman
6009549
*Date:*
18 juni 2021

*Supervisor:*
Dr. Martijn Kool

# Contents

# 1 Introduction

At the end of the 19th century Hilbert published his famous syzygy theorem, which ensures the existence of a finite free resolution. Hilbert at the time studied free resolutions because he wanted to find an explicit description of his so called Hilbert function, which roughly speaking gives us information about the structure of a module.

In 1964 Bruno Buchberger introduced the theory of Gröbner bases, named after his thesis advisor Wolfgang Gröbner. Since then Gröbner bases have proved to be very useful tools, especially in computational algebra. A few decades later German mathematician Frank-Olaf Schreyer used these Gröbner bases to give a new proof for the syzygy theorem.

We will use the first chapter to introduce the necessary background material. In the second chapter we will present the proof Schreyer gave for the syzygy theorem. The last chapter will be dedicated to the motivation for studying resolution.

The first two chapters are mostly based on the book "Using Algebraic Geometry" by Cox, Little and O'Shea [1]. For the algorithms that we will discuss a nice presentation can be found in the book "An Introduction to Gröbner Bases" by Adams and Loustaunau [4]. The last part of the proof of the syzygy theorem will be based on the proof given in this book. It also contains most of the results in the first two chapters. The book "Commutative Algebra" by Eisenbud [2] contains most of the results in the first three chapters and also a short history of Gröbner bases in chapter 15. The book "A Singular Introduction To Commutative Algebra" by Greuel and Pfister [5] contains an introduction to computer algebra system Singular, which we will use in some of the examples.

For the last chapter the book "The Geometry of Syzygies" by Eisenbud [3], contains many of the results, examples and a motivation for the study of free resolutions. The book "Graded Syzygies" by Peeva [6] contains most of the results in the chapter. Theorem 4.17 is discussed on p. 100 in the book "Monomial Ideals" by Herzog and Hibi [9]. This book also contains most of the material discussed, in particular a good overview of the Taylor complex. A treatment of tensor powers and exterior powers of graded modules can be found on pages 40 and 182 in the text "Graded Rings and Graded Grothendieck Groups" by Hazrat [7]. The set of notes on homological algebra by Swanson [8] contains a nice treatment of Koszul complexes. Lastly a clear treatment of the graded version of Schreyer's method for constructing free resolutions can be found on pp. 70-71 in the book "Gröbner Bases in Commutative Algebra" by Ene and Herzog [11].

# 2 Theoretical Background

## 2.1 Module Theory Basics

In this section we will introduce some general results and definitions in module theory. Throughout this text rings are assumed to be commutative, and $\mathcal{R}$ will stand for a polynomial ring $k[x_1, \ldots, x_n]$ over a field $k$ unless otherwise stated.

**Definition 2.1.** An $\mathcal{R}$-module is said to be a free $\mathcal{R}$-module if it is isomorphic to a direct sum of $s$ copies of $\mathcal{R}$, that is:

$$M \simeq \oplus_{i=1}^{s} \mathcal{R} = \{(m_0, \ldots, m_s) | m_0, \ldots, m_s \in \mathcal{R}\}.$$

We will always denote $\oplus_{i=1}^{s} \mathcal{R}$ by $\mathcal{R}^s$. Alternatively, one could give the following definition: $M$ is a **free $\mathcal{R}$-module** if it has a module basis i.e. a subset $S \subset M$ that is $\mathcal{R}$-linearly independent and generates $M$.

**Definition 2.2.** A ring $\mathcal{N}$ is a **Noetherian** if every ideal in $\mathcal{N}$ is finitely generated.

Note that any field $k$ is Noetherian because the only ideals are 0 and the whole field.

We will now state of another famous theorem due to Hilbert.

**Theorem 2.3** (*Hilbert Basis Theorem*)**.** *If a ring $\mathcal{N}$ is Noetherian, then the polynomial ring $\mathcal{N}[x_1, \ldots, x_n]$ is Noetherian.*

It follows $\mathcal{R}$ is Noetherian. We can extend the definition for ring to a more general one for modules.

**Definition 2.4.** An $\mathcal{R}$-module $M$ is **Noetherian** if every submodule of $M$ is finitely generated.

Another result which will prove to be very useful later on is the following.

**Proposition 2.5.** *The free module $\mathcal{R}^s$ is Noetherian.*

This is a direct consequence of the following more general result.

**Proposition 2.6.** *If $\mathcal{N}$ is a Noetherian ring and $M$ is a finitely generated $\mathcal{N}$-module, then $M$ is Noetherian.*

The final result we will state in this section is an 1st isomorphism theorem for modules. Let $M$ and $M'$ be two $\mathcal{R}$-modules, and $\varphi : M \to M'$ an $\mathcal{R}$-module homomorphism. The map

$$\Phi : M/\ker\varphi \to \mathrm{im}(\varphi)$$

$$\Phi(m + \ker\varphi) = \varphi(m)$$

defines an $\mathcal{R}$-module isomorphism. Thus, $M/\ker\varphi \simeq \mathrm{im}(\varphi)$.

## 2.2 Syzygies, Orders and Gröbner Bases

In this section we will introduce the theory underlying the proof of the syzygy theorem, we will introduce syzygies, Gröbner bases and give some important results that we will be needing for the proof of the syzygy theorem.

**Definition 2.7.** The (first) **syzygy** module of an ordered s-tuple $(m_1, \ldots, m_s)$ of elements $m_i \in M$, is the set:

$$\text{Syz}(m_1, \ldots, m_s) = \{(a_1, \ldots, a_s)^T \in \mathcal{R}^n | a_1 m_1 + \ldots + a_s m_s = 0\}.$$

The s-tuples $(a_1, \ldots, a_s)$ are also said to be **relations** on $(m_1, \ldots, m_s)$.

We will now show that a syzygies module is indeed a module.

**Proposition 2.8.** *Let $(m_1, \ldots, m_s)$ be an ordered s-tuple of elements $m_i \in M$. The set*

$$Syz(m_1, \ldots, m_s)$$

*is an $\mathcal{R}$-submodule of $\mathcal{R}^s$*

*Proof.* Let $(a_1, \ldots, a_s)^T, (b_1, \ldots, b_s)^T \in \text{Syz}(m_1, \ldots m_s)$ and $c \in R$.
We have

$$ca_1 m_1 + \ldots ca_s m_s = 0, \text{ and}$$

$$b_1 m_1 + \ldots b_n m_s = 0.$$

Adding both equations we get

$$ca_1 m_1 + b_1 m_1 \ldots ca_s m_s + b_s m_s = (ca_1 + b_1) m_1 \ldots (ca_s + b_s) m_s = 0.$$

It follows that $(ca_1 + b_1, \ldots, ca_s + b_s) \in \text{Syz}(m_1, \ldots, m_s)$. Thus,
$\text{Syz}(m_1, \ldots, m_s) \subset \mathcal{R}^s$ is an $\mathcal{R}$-submodule of $\mathcal{R}^s$.

□

**Example 2.9.** Let $\mathcal{R} = \mathbb{Q}[x, y]$ and consider the ideal $I = \langle xy, x^2 \rangle \subset \mathcal{R}$. Then the syzygy module $\text{Syz}(xy, x^2)$ is generated by $(x, -y) \in \text{Syz}(xy, x^2)$. Later when we have developed more tools we will see a method for determining syzygies for more complicated sets.

We will use the shorthand notation $x^\alpha$, where $\alpha = (\alpha_1, \ldots, \alpha_n)$, for monomials $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$.

**Definition 2.10.** A **monomial order** on $\mathcal{R}$ is any relation $>$ on the set of monomials $x^\alpha \in \mathcal{R}$ satisfying:

1. $>$ is a total ordering relation i.e. $>$ is reflexive, transitive, antisymmetric and for each $f, g \in \mathcal{R}$ we have that either $x > y$, $x = y$ or $y > x$.;
2. $>$ is compatible with multiplication in $\mathcal{R}$, i.e. if $x^\alpha > x^\beta$, then for any monomial $x^\gamma$
$$x^\alpha x^\gamma = x^{\alpha+\gamma} > x^{\beta+\gamma} = x^\beta x^\gamma.$$
3. $>$ is a well-ordering i.e. let $\emptyset \neq S \subset \mathcal{R}$ be a collections of monomials, then there is an element $s_0 \in S$ such that for each $s \in S$, $s > s_0$.

We will now give the definitions for three well known monomial orders.

**Definition 2.11.** Let $x^\alpha, x^\beta \in \mathcal{R}$ and denote by $>_{lex}$ the **lexicographic order**. We say that $x^\alpha >_{lex} x^\beta$ if in the difference $\alpha - \beta \in Z^n$ the leftmost nonzero entry is positive.

**Definition 2.12.**

1. $x^\alpha >_{grlex} x^\beta$ if $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$, or if $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ and $x^\alpha >_{lex} x^\beta$.
2. $x^\alpha >_{grevlex} x^\beta$ if $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$, or if $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ and the rightmost nonzero entry in $\alpha - \beta \in \mathbb{Z}^n$ is negative.

Equip $\mathcal{R}$ with a monomial order $>$, and let $f \in \mathcal{R}$. Then we write $\mathrm{LT}_>(f)$ to denote the leading term in $f$. Now that we have introduced the notion of a monomial order on $\mathcal{R}$ we want to extend this notion to the more general case of monomials of free modules $\mathcal{R}^s$. But first we have to agree on the language we use. In the case of free modules monomials are elements $m \in \mathcal{R}^s$ of the form $x^\alpha e_i$, where $e_i$ is a standard basis vector for $\mathcal{R}^s$.

A monomial of the form $m = x^\alpha e_i$ is said to contain $e_i$, and for a pair of monomials $m = x^\alpha e_i$, $n = x^\beta e_j$, and coefficients $c_1, c_2 \in k$, with $c_2 \neq 0$ we say that the term $c_1 m$ is divisible by $c_2 n$ if and only if $i = j$ and $x^\beta$ divides $x^\alpha$. The resulting quotient is $\frac{c_1 x^\alpha}{c_2 x^\beta} \in \mathcal{R}$.

If $m$ and $n$ contain the same basis element $e_i$ the least common multiple denoted by $\mathrm{LCM}(m, n)$ is the least common multiple of $x^\alpha$ and $x^\beta$, multiplied by $e_i$. In the case that $m$ and $n$ do not contain the same basis vector we have $\mathrm{LMC}(m, n) = 0$.

Finally a submodule $M \subset \mathcal{R}^q$ is a monomial submodule if it is generated by a

collection of monomials. Now we can proceed to define the monomial order for submodules, but before we do we do, we prove the following proposition, which will be utilized in proof of Schreyer's theorem.

**Proposition 2.13.** *Let $M \subset \mathcal{R}^q$ be a monomial submodule generated by $\{m_1, \ldots, m_s\}$, let $\epsilon_1, \ldots, \epsilon_s$ denote the standard basis vectors for $\mathcal{R}^s$, and let $m_{i,j} = LCM(m_i, m_j)$. Then the syzygy module $Syz(m_1, \ldots, m_s)$ is generated by the syzygies*

$$\sigma_{i,j} = \frac{m_{i,j}}{m_i}\epsilon_i - \frac{m_{i,j}}{m_j}\epsilon_j, \quad \textit{for all} \quad 1 \leq i < j \leq s$$

*and $\sigma_{i,j} = 0$ unless $m_i$ and $m_j$ contain the same standard basis vector in $\mathcal{R}^q$.*

*Proof.* Let $(a_1, \ldots, a_s)^T \in \mathrm{Syz}(m_1, \ldots, m_s)$, and let $e_1, \ldots, e_q$ denote the standard basis vectors for $\mathcal{R}^q$. We have the following equation:

$$0 = a_1 m_1 + \ldots + a_s m_s = a_1 x^{\alpha_1} e_{\sigma(1)} + \ldots + a_s x^{\alpha_s} e_{\sigma(s)},$$

where $(\sigma(1), \ldots, \sigma(s))$ is a permutation of $(1, \ldots, s)$. In the above equation, by grouping together the terms with the same standard basis vectors $e_{\sigma(i)}$, we find that the syzygy $(a_1, \ldots, a_s)^T$ is the sum of syzygies on the monomials $m_i$ with the same standard basis vector. Without loss of generalization we continue our proof with one such subset $\{\tilde{m}_1, \ldots, \tilde{m}_t\} \subset \{m_1, \ldots, m_s\}$, with standard basis vector $e_k$, and a syzygy $(\tilde{a}_1, \ldots, \tilde{a}_t)^T \in \mathrm{Syz}(\tilde{m}_1, \ldots, \tilde{m}_t)$.
For this new pair we can write:

$$(*) \quad \tilde{a}_1 \tilde{m}_1 + \ldots + \tilde{a}_t \tilde{m}_t = 0$$

$$= (\tilde{a}_1 x^{\tilde{\alpha}_1} + \ldots + \tilde{a}_t x^{\tilde{\alpha}_t}) e_k = (\sum_{i=1}^{v_1} c_{1i} x^{\beta_{1i}} x^{\tilde{\alpha}_1} + \ldots + \sum_{i=1}^{v_t} c_{ti} x^{\beta_{ti}} x^{\tilde{\alpha}_t}) e_k$$

Now let us group together the terms such that $\tilde{\alpha}_i + \beta_{ix} = \tilde{\alpha}_j + \beta_{jy}$. We can write the equation $(*)$ in the following way:

$$((\tilde{c}_{11} x^{\tilde{\alpha}_1 + \tilde{\beta}_{11}} + \ldots + \tilde{c}_{1t} x^{\tilde{\alpha}_t + \tilde{\beta}_{1t}}) + \ldots + (\tilde{c}_{z1} x^{\tilde{\alpha}_1 + \tilde{\beta}_{z1}} + \ldots + \tilde{c}_{zt} x^{\tilde{\alpha}_t + \tilde{\beta}_{zt}})) e_k$$

$$= ((\tilde{c}_{11} + \ldots + \tilde{c}_{1t}) x^{\eta_1} + \ldots + (\tilde{c}_{z1} + \ldots + \tilde{c}_{zt}) x^{\eta_z}) e_k.$$

Notice that we can add terms with zero coefficient so that each of the sums contain $t$ terms. Also note that for the above equation to hold we must have $\sum_{j=1}^{t} \tilde{c}_{ij} = 0$ for every $i$. We can rewrite our syzygy as a sum of syzygies of the form

$$(\tilde{c}_{i1}x^{\eta_i-\tilde{\alpha}_1},\dots,\tilde{c}_{it}x^{\eta_i-\tilde{\alpha}_t}) \in \mathrm{Syz}(\tilde{m}_1,\dots,\tilde{m}_t),$$

Now let us continue our proof with one such syzygy $(u_1x^{\mu-\tilde{\alpha}_1},\dots,u_tx^{\mu-\tilde{\alpha}_t})^T \in \mathrm{Syz}(\tilde{m}_1,\dots,\tilde{m}_t)$. Let $\epsilon_1,\dots,\epsilon_t$ denote the standard basis vectors for $\mathcal{R}^t$, we can write the syzygy $(u_1x^{\mu-\tilde{\alpha}_1},\dots,u_tx^{\mu-\tilde{\alpha}_t})^T$ as the following sum:

$$(u_1x^{\mu-\tilde{\alpha}_1}\epsilon_1 - u_1x^{\mu-\tilde{\alpha}_2}\epsilon_2) + ((u_1+u_2)x^{\mu-\tilde{\alpha}_2}\epsilon_2 - (u_1+u_2)x^{\mu-\tilde{\alpha}_3}\epsilon_3)$$
$$+$$
$$\vdots$$
$$+$$
$$(\sum_{i=1}^{l} u_ix^{\mu-\tilde{\alpha}_l}\epsilon_l - \sum_{i=1}^{l} u_ix^{\mu-\tilde{\alpha}_{l+1}}\epsilon_{l+1}) + (\sum_{i=1}^{l+1} u_ix^{\mu-\tilde{\alpha}_{l+1}}\epsilon_{l+1} - \sum_{i=1}^{l+1} u_ix^{\mu-\tilde{\alpha}_{l+2}}\epsilon_{l+2})$$
$$+$$
$$\vdots$$
$$+$$
$$(\sum_{i=1}^{t-2} u_ix^{\mu-\tilde{\alpha}_{t-2}}\epsilon_{t-2} - \sum_{i=1}^{t-2} u_ix^{\mu-\tilde{\alpha}_{t-1}}\epsilon_{t-1}) + (\sum_{i=1}^{t-1} u_ix^{\mu-\tilde{\alpha}_{t-1}}\epsilon_{t-1} + u_tx^{\mu-\tilde{\alpha}_t}\epsilon_t).$$

Note that $u_t = -\sum_{i=1}^{t-1} u_i$.
Now let $\tilde{u} = \sum_{i=1}^{l} u_i$, and lets take a closer look at one of these differences:

$$\tilde{u}(x^{\mu-\tilde{\alpha}_l}\epsilon_l - x^{\mu-\tilde{\alpha}_{l+1}}\epsilon_{l+1}).$$

Note that $x^\mu$ is divisible by $x^{\tilde{\alpha}_i}$ for every $1 \le i \le t$, therefore we can write $x^\mu = \mathrm{LCM}(x^{\tilde{\alpha}_l}, x^{\tilde{\alpha}_{l+1}})x^{\mu_l}$. With this in mind we can rewrite our difference as

$$\tilde{u}x^{\mu_l}(\frac{\mathrm{LCM}(x^{\tilde{\alpha}_l}, x^{\tilde{\alpha}_{l+1}})}{x^{\tilde{\alpha}_l}}\epsilon_l - \frac{\mathrm{LCM}(x^{\tilde{\alpha}_l}, x^{\tilde{\alpha}_{l+1}})}{x^{\tilde{\alpha}_{l+1}}}\epsilon_{l+1})$$

$$= \tilde{u}x^{\mu_l}(\frac{\mathrm{LCM}(\tilde{m}_l, \tilde{m}_{l+1})}{\tilde{m}_l}\epsilon_l - \frac{\mathrm{LCM}(\tilde{m}_l, \tilde{m}_{l+1})}{\tilde{m}_{l+1}}\epsilon_{l+1}).$$

This concludes the proof of the proposition.

□

**Definition 2.14.** A **monomial ordering** on $\mathcal{R}^t$ is an ordening relation $>$ on the set of monomials $m \in \mathcal{R}^t$ satisfying:

1. $>$ is a total ordering relation i.e. $>$ is reflexive, transitive, antisymmetric and for every pair of monomials $m, n \in \mathcal{R}^t$, we have either $m > n$, $m = n$ or $n > m$.

2. $>$ is compatible with multiplication in $\mathcal{R}^t$, i.e. for every $m, n \in \mathcal{R}^t$ if $m > n$, then $x^\gamma m > x^\gamma n > n$ for every monomial $1 \neq x^\gamma \in \mathcal{R}$.;

3. $>$ is a well-ordering i.e. let $\emptyset \neq S \subset \mathcal{R}^t$ be a collection of monomials, then there is an element $s_0 \in S$ such that for each $s \in S$, $s > s_0$.

**Remark.** Instead of saying that a monomial order is a well-ordering some authors say that it is **Artinian**. Although we require that a monomial order is by definition Artinian, in our case, that is working over the ring $\mathcal{R}$, this is not necessary because it follows from the first two conditions and the fact that $\mathcal{R}^t$ is Noetherian. The argument is as follows: Let $\emptyset \neq S \subset \mathcal{R}^t$ be a collection of monomials, then since $\mathcal{R}^t$ is Noetherian the set generated by $S$ is finitely generated by a subset $U \subset S$. The finite set $U$ has a least element $u_0 \in U$, and by the second condition $u_0$ is also a least element in $S$ since every $s \in S$ is of the form $x^\alpha u$ for some $u \in U$ and $x^\alpha \in \mathcal{R}$.

Monomial orders on $\mathcal{R}$ can be extended to a monomial order on $\mathcal{R}^t$ using the so called TOP and POT extension. These extensions are defined as follows.

**Definition 2.15.**

Given an monomial order $>$ on $\mathcal{R}$, the TOP extension of $>$, denoted by $>_{\text{TOP}}$ is the monomial order on $\mathcal{R}^t$ such that

$$x^\alpha e_i >_{\text{TOP}} x^\beta e_j \text{ if } x^\alpha > x^\beta, \text{ or if } x^\alpha = x^\beta \text{ and } i < j.$$

The POT extension of $>$, denoted by $>_{\text{POT}}$ is the monomial order on $\mathcal{R}^t$ such that

$$x^\alpha e_i >_{\text{POT}} x^\beta e_j \text{ if } i < j, \text{ or if } i = j \text{ and } x^\alpha > x^\beta.$$

Let $>$ be a monomial order on $\mathcal{R}^t$ and $m \in \mathcal{R}^t$. We can write

$$m = \sum_{i=1}^{k} c_i m_i$$

where the $m_i$ are monomials, the $c_i \neq 0$ coefficients, and $m_1 > m_2 > \ldots > m_k$. We use the notation

$$\text{LC}_>(m) = c_1 \text{ for the leading coefficient of m,}$$

$$\mathrm{LM}_>(m) = m_1 \text{ for the leading monomial, and}$$

$$\mathrm{LT}_>(m) = c_1 m_1 \text{ for the leading term.}$$

In the above notation we will omit the ordering when it is obvious which one we are using, i.e. we write L-$(m)$ instead of L-$_>(m)$. Also, for any monomial order $>$ on $\mathcal{R}^t$ we assume that $e_1 > \ldots > e_t$.

Let $M$ be a submodule of $\mathcal{R}^t$, and let $>$ be a monomial ordering. Define $\mathrm{LT}_>(M) = \{\mathrm{LT}_>(m) | m \in M\}$, and for a subset $X$ of a module we use the notation $\langle X \rangle$ to mean the submodule generated by the set $X$. We have now set the stage to define the Gröbner basis for a submodule, our main tool for proving the syzygy theorem.

**Definition 2.16.** A finite collection $\mathcal{G} = \{g_1, \ldots, g_s\} \subset M$ is said to be a **Gröbner basis** for $M$ with respect to the order $>$ if

$$\langle \mathrm{LT}(M) \rangle = \langle \mathrm{LT}(g_1) \ldots \mathrm{LT}(g_s) \rangle.$$

A Gröbner basis $\{g_1, \ldots, g_s\}$ for $M$ such that $\mathrm{LT}(g_i)$ does not divide any of the terms in $g_j$, for $i \neq j$, is said to be a **reduced** Gröbner basis. If in addition the leading coefficients of all the Gröbner basis elements are equal to $1 \in k$ we say that the Gröbner basis is **monic**.
In the following theorem we state a generalization of division with remainder for the free module $\mathcal{R}^t$.

**Theorem 2.17** (*Division Algorithm in $\mathcal{R}^t$*)**.** *Equip $\mathcal{R}^t$ with any monomial ordering and let $F = f_1, \ldots, f_s \in \mathcal{R}^t$ be an ordered s-tuple. Then every $f \in \mathcal{R}^t$ can be written in the following form:*

$$f = a_1 f_1 + \ldots + a_s f_s + r,$$

*with $a_i \in \mathcal{R}$, $r \in \mathcal{R}^t$, $LT(a_i f_i) \leq LT(f)$ for all $i$, and $r = 0$ or $r$ is a $k-$linear combination of monomials which are not divisible by $LT(f_1), \ldots, LT(f_s)$. The term $r$ is said to be the remainder on division by $F$.*

Below we give a description of the algorithm.

We start with $a_1 := 0,\ a_2 := 0, \ldots a_s := 0,\ r := 0$ and $g := f$, and iterate the process described below each time updating the $a_i$, $r$ and $g$ so long as $g \neq 0$.
Choose the smallest $i$ such that $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(g)$, and proceed as follows:

$$a_i := a_i + \frac{\mathrm{LT}(g)}{\mathrm{LT}(f_i)}$$

$$g := g - \frac{\mathrm{LT}(g)}{\mathrm{LT}(f_i)} f_i.$$

If no such $i$ exists

$$r := r + \mathrm{LT}(g)$$

$$g := g - \mathrm{LT}(g).$$

Next we state two useful results for Gröbner bases.

**Proposition 2.18.** *Let $\mathcal{G}$ be a Gröbner basis for a submodule $M \subset \mathcal{R}^t$, and let $f \in \mathcal{R}^t$. Then*

1. *$f \in M$ if and only if the remainder on division by $\mathcal{G}$ is zero.*
2. *$M = \langle \mathcal{G} \rangle$.*

**Proposition 2.19.** *Let $M \subset \mathcal{R}^t$ be a submodule and $\mathcal{G}$ a Gröbner basis for $M$. Then two elements $[f]$ and $[g]$ in the quotient module $\mathcal{R}^t/M$ are equal if and only if the their remainder on division by $\mathcal{G}$ is equal*

*Proof.* Let $[f], [g] \in \mathcal{R}^t/M$. First note that the remainder of $f - g$ on division by $\mathcal{G}$ is equal to the difference of the remainder of $f$ and $g$ on division by $\mathcal{G}$. Now assume that $[f] = [g]$, then we must have that $f - g \in M$ and by the first part of the previous result that the remainder $f - g$ on division by $\mathcal{G}$ is zero. It follows that the remainders on division by $\mathcal{G}$ of $f$ and $g$ are equal. On the other hand, if the remainders of $f$ and $g$ are equal then, the remainder of their difference is 0. Using the previous result once more we have that $f - g \in M$, and thus $[f] = [g]$. □

The question remains: **how does one find Gröbner bases?**

Given a set of generators for some module one could try to produce a Gröbner basis by thinking hard of a set that satisfies the definition. Although this is possible, it seems like a difficult undertaking that requires a lot of trial and error.

Around the beginning to the middle of the 20th century, Austrian mathematician Wolfgang Gröbner was able to explicitly find bases for zero dimensional factor rings, for which he used ideas developed around the same time by British mathematician Francis Sowerby Macaulay.

It wasn't until 1964 when Buchberger suggested to his student Bruno Buchberger to compute such bases for his PhD thesis, when large steps where taken in the developement of the theory of Gröbner bases. In his thesis Buchberger introduced the concept of Gröbner bases together with the main theorem of Gröbner basis theory, which characterizes the bases using so called S-polynomials.
Based on this theorem Buchberger had developed an algorithm for calculating Gröbnerbases. In the following decades the ideas introduced by Buchberger had been further developed by himself and many others. We will now state the theorem and algorithm developed by Buchberger, for the module case.

The S-polynomials we mentioned are called S-vectors in the module setting, and are defined as follows.

**Definition 2.20.** Equip $\mathcal{R}^t$ with a monomial order, let $f, g \in \mathcal{R}^t$, and let $m = \mathrm{LCM}(\mathrm{LT}(f), \mathrm{LT}(g))$. The **S-vector**, $S(f,g) \in \mathcal{R}^t$ is given by the following equation:

$$S(f,g) = \frac{m}{\mathrm{LT}(f)} f - \frac{m}{\mathrm{LT}(g)} g.$$

Now we state the main theorem of Gröbner basis theory, also known as Buchberger's criterion.

**Theorem 2.21** (*Buchberger's Criterion*)**.** *A subset $\mathcal{G} = \{g_1, \ldots, g_s\} \subset \mathcal{R}^t$ is a Gröbner basis for $\langle \mathcal{G} \rangle$ if and only if the remainder of $S(g_i, g_j)$ on division by $\mathcal{G}$ is zero for all $i, j$.*

Using Buchberger's criterion we present the algorithm for calculating Gröbner bases of finitely generated submodules of $\mathcal{R}^t$.

**Theorem 2.22** (*Buchberger's Algorithm*)**.** *Let $F = \{f_1, \ldots, f_s\} \subset \mathcal{R}^t$, and $>$ a monomial order on $\mathcal{R}^t$. Then there exists a Gröbner basis $\mathcal{G}$ for $\langle F \rangle$ with respect to the monomial order $>$*

Below we give a description of the algorithm.

Let $\overline{S(f,g)}^{\mathcal{G}'}$ denote the remainder on division by $\mathcal{G}'$, using the division algorithm. We start with $\mathcal{G} = F$ and $\mathcal{S} := \{\{f_i, f_j\} \subset \mathcal{G} | f_i \neq f_j\}$, and iterate the process described below each time updating $\mathcal{G}$ and $\mathcal{S}$, so long as $\mathcal{S} \neq \emptyset$.

Choose an element $\{f_i, f_j\} \in \mathcal{S}$ and proceed as follows:

$$\mathcal{S} := \mathcal{S} \setminus \{\{f_i, f_j\}\}$$

$$r := \overline{S(f,g)}^{\mathcal{G}}.$$

If $r \neq 0$ then

$$\mathcal{S} := \mathcal{S} \cup \{\{f', r\} | f' \in \mathcal{G}\}$$

$$\mathcal{G} = \mathcal{G} \cup \{r\}.$$

In addition to being able to find a Gröbner basis when given a set of generators, given a Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_s\}$, one can produce a monic Gröbner basis following the general procedure outlined below.

1. First remove all the $g_i$ for which there exists some $g_j$ with $i \neq j$ such that $\mathrm{LT}(g_j)$ divides $g_i$, to obtain a new set $\mathcal{G}'$
2. Next, for each $g_i' \in \mathcal{G}'$ calculate $\overline{g_i}^{\mathcal{G}' \setminus g_i}$, the remainder on division by $\mathcal{G}' \setminus g_i$, and replace $g_i' \in \mathcal{G}'$ by $\overline{g_i}^{\mathcal{G}' \setminus g_i}$
3. Finally we divide each $\overline{g_i}^{\mathcal{G}' \setminus g_i}$ by $\mathrm{LC}(\overline{g_i}^{\mathcal{G}' \setminus g_i})$.

We will now give an example of a Gröbner basis for a submodule of $\mathcal{R}^t$. To do this we will use the computer algebra system Singular, which among other algorithms also implements Buchbergers algorithm to compute Gröbner bases.

**Example 2.23.** Let $M \subset \mathcal{R}^3$, where $\mathcal{R} = \mathbb{Q}[x_1, x_2, x_3, x_4]$ and we use the TOP extension of $>_{grevlex}$ . Suppose $M$ is the module generated by:

$$\begin{pmatrix} x_1 + x_2 \\ x_3 \\ x_1x_3 - x_4 \end{pmatrix}, \begin{pmatrix} x_1x_2x_3 - x_4 \\ x_2x_3 \\ x_1x_4 \end{pmatrix}, \begin{pmatrix} x_1^2 \\ x_2^2 \\ x_3^2 - x_4 \end{pmatrix} \in \mathcal{R}^3.$$

The set $\mathcal{G}$ defines a Gröbner basis for $M$

$$g_1 = \begin{pmatrix} x_1 + x_2 + x_3 \\ 0 \\ 0 \end{pmatrix}, g_2 = \begin{pmatrix} x_2^2 + 2x_2x_3 + x_3^2 \\ x_2^2 \\ x_3^2 - x_4 \end{pmatrix}, g_3 = \begin{pmatrix} x_2^2x_3 + x_2x_3^2 + x_4^2 \\ -x_2x_3 \\ -x_1x_4 \end{pmatrix},$$

$$g_4 = \begin{pmatrix} -x_2x_3^2 - x_3^3 + x_4^2 \\ x_1x_2x_3 + x_2x_3^2 - x_2x_3 \\ -x_3^3 + x_1^2x_4 + x_1x_2x_4 + x_1x_3x_4 - x_1x_4 + x_3x_4 \end{pmatrix},$$

$$g_5 = \begin{pmatrix} 0 \\ 0 \\ x_1x_3^3 + x_2x_3^3 + x_3^4 - x_1^2x_2x_4 - x_1x_2^2x_4 - x_1x_2x_3x_4 - x_1x_3x_4 - x_2x_3x_4 - x_3^2x_4 \end{pmatrix},$$

$$\mathcal{G} = \{g_1, g_2, g_3, g_4, g_5\} \subset \mathcal{R}^3.$$

Note that when we use the TOP extension of $>_{grlex}$ order instead of the extension of $>_{grevlex}$ we get

$$g_1 = \begin{pmatrix} x_1 + x_2 \\ x_3 \\ x_1x_3 - x_4 \end{pmatrix}, g_2 = \begin{pmatrix} x_1^2 \\ x_2^2 \\ x_3^2 - x_4 \end{pmatrix}, g_3 = \begin{pmatrix} x_1x_2x_3 - x_4^2 \\ x_2x_3 \\ x_1x_4 \end{pmatrix}, g_4 = \begin{pmatrix} x_1x_4^2 \\ x_2^3x_3 - x_1x_2x_3 \\ x_2x_3^3 - x_1^2x_4 - x_2x_3x_4 \end{pmatrix}$$

$$\mathcal{G} = \{g_1, g_2, g_3, g_4\}.$$

This indicates that the choice of order has a significant effect what Gröbner basis one obtains.

## 2.3 Presentations and Free Resolutions

In this section we introduce the free resolution, the main subject of the syzygy theorem.

**Definition 2.24.** A sequence of $\mathcal{R}$-modules $M_i$ and homomorphisms $\varphi_i$

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

is said to be exact at $M_i$ if $im(\varphi_{i+1}) = \ker \varphi_i$. The entire sequence is exact if it is exact each $M_i$.

We have the following three useful facts:

1. $\varphi : M \to N$ is surjective $\iff M \xrightarrow{\varphi} N \to 0$ is exact
2. $\varphi : M \to N$ is injective $\iff 0 \longrightarrow M \xrightarrow{\varphi} N$ is exact
3. $\varphi : M \to N$ is an isomorphism $\iff 0 \longrightarrow M \xrightarrow{\varphi} N \to 0$ is exact

**Proposition 2.25.** *For an $\mathcal{R}$-module $M$, choosing a generating set with t elements is equivalent to choosing a surjective homomorphism $\mathcal{R}^t \to M$, or equivalently an exact sequence $\mathcal{R}^t \xrightarrow{\varphi} M \longrightarrow 0$.*

*Proof.* First note that we can choose an element $m \in M$ by choosing a homomorphism $\varphi : \mathcal{R} \to M$ with $\varphi(1) = m$. This is the case because for all $g \in \mathcal{R}$

$$\varphi(g) = \varphi(g \cdot 1) = g\varphi(1) = gm.$$

This idea can be extended so that we can interpret choosing t elements in $M$ as choosing an $\mathcal{R}$-module homomorphism $\varphi : \mathcal{R}^t \to M$. Denote by

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_t = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

the standard basis of $\mathcal{R}^t$, and choose a set of generators $\{m_1, \ldots, m_t\} \subset M$. Extending the idea for the identification of one element, the choice of generators corresponds to choosing a homomorphism $\varphi : \mathcal{R}^t \to M$, with $\varphi(e_i) = m_i$ for all $i \in \{1, \ldots, t\}$. Since $\{m_1, \ldots, m_t\}$ is a generating set for $M$, we have that $\mathrm{im}(\varphi) = M$.

□

**Definition 2.26.** A **presentation** for an $\mathcal{R}$-module $M$ is a set of generators $m_1, \ldots, m_t$, for $M$ together with a set of generators for the syzygy module $\mathrm{Syz}(m_1, \ldots, m_t)$ of relations among $m_1, \ldots, m_t$.

**Proposition 2.27.** *A presentation for an $\mathcal{R}$-module $M$ is an exact sequence of the form*

$$\mathcal{R}^s \xrightarrow{\nu} \mathcal{R}^t \xrightarrow{\varphi} M \longrightarrow 0.$$

*Proof.* It follows from the previous proposition that a set of generators $m_1, \ldots, m_t$ for $M$ gives us an exact sequence

$$\mathcal{R}^t \xrightarrow{\varphi} M \longrightarrow 0$$

where $\varphi$ is the homomorphism mapping $(g_1, \ldots, g_t) \in \mathcal{R}^t$ to

$$\sum_{i=1}^{t} g_i \varphi(e_i) = \sum_{i=1}^{t} g_i m_i.$$

By definition we have that

$$\mathrm{Syz}(m_1, \ldots, m_t) = \ker(\varphi).$$

Let $a_1, \ldots, a_s$ denote the set of generators for the syzygy module $\mathrm{Syz}(m_1, \ldots, m_t)$, and apply the proposition again. We get a surjective homomorphism

$$\nu : \mathcal{R}^s \to \mathrm{Syz}(m_1, \ldots, m_t) (= \ker(\varphi)).$$

Also note that since $\nu$ is surjective $\mathrm{im}(\nu) = \ker(\varphi)$. It follows that the sequence

$$\mathcal{R}^s \xrightarrow{\nu} \mathcal{R}^t \xrightarrow{\varphi} M \longrightarrow 0$$

is exact. □

**Proposition 2.28.** *Every finitely generated $\mathcal{R}$-module $M$ has a presentation.*

*Proof.* Let $m_1, \ldots, m_s$ be a generating set for $M$. Then the Syzygy module $\mathrm{Syz}(m_1, \ldots, m_s)$ is a submodule of $\mathcal{R}^s$. Since $\mathcal{R}^s$ is Noetherian, it follows that $\mathrm{Syz}(m_1, \ldots, m_s)$ has a finite set of generators. Thus, $M$ has a presentation. □

**Definition 2.29.** A **free resolution** of $M$ is an exact sequence of the form

$$\ldots \longrightarrow M_2 \xrightarrow{\varphi_2} M_1 \xrightarrow{\varphi_1} M_0 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

Where all the $M_i$ are free $\mathcal{R}-$modules.

A resolution is said to be finite of length $s$ if for all $i > s$, $M_i = 0$ but $M_s \neq 0$.

**Example 2.30.** Consider the monomial ideal, $\langle x^2, xy\rangle \subset \mathcal{R} = \mathbb{Z}_{907}[x, y]$. We start with the following homomorphism,

$$\varphi_0 : \mathcal{R}^2 \to I, \text{ with } \varphi_0(e_1) = x^2 \text{ and } \varphi_0(e_2) = xy.$$

Since $\varphi_0$ is a surjective homomorphism we get the exact sequence:

$$\mathcal{R}^2 \xrightarrow{\varphi_0} I \longrightarrow 0.$$

Next we find that $(-y, x)^T$ is a set of generators for the syzygy module $\mathrm{Syz}(x^2, xy)$. Note that we have not yet developed the right tools for finding generators for syzygy modules. In the next chapter we will state and prove Schreyer's theorem which given a Gröbner basis for a submodule of $\mathcal{R}^t$ gives us an explicit way of finding a set of generators for the syzygy module of the Gröbner basis elements. This will allow us to tackle more difficult examples.

Now define $\varphi_1 : \mathcal{R} \to \mathcal{R}^2$, $\varphi_1(1) = (-y, x)^T$ since $\mathrm{im}(\varphi_1) = \ker(\varphi_0)$ we can extend our sequence to the following exact sequence:

$$\mathcal{R} \xrightarrow{\varphi_1} \mathcal{R}^2 \xrightarrow{\varphi_0} I \longrightarrow 0.$$

Note that $\mathrm{Syz}((-y, x)^T) = 0$. It follows that $I$ has a free resolution of length 2,

$$0 \longrightarrow \mathcal{R} \xrightarrow{\varphi_1} \mathcal{R}^2 \xrightarrow{\varphi_0} I \longrightarrow 0.$$

**Proposition 2.31.**

1. *In a finite free resolution*

$$0 \longrightarrow M_s \xrightarrow{\varphi_s} M_{s-1} \xrightarrow{\varphi_{s-1}} M_{s-2} \longrightarrow \ldots \longrightarrow M_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

   $\ker(\varphi_{s-1})$ *is a free module.*

2. *If $M$ has a free resolution in which* $\ker(\varphi_{s-1})$ *is a free module for some $s$, then $M$ has a finite free resolution of length $s$.*

*Proof.* Since we have a finite free resolution, the sequence is exact at each $i$. In particular if we isolate the partial sequence

$$0 \longrightarrow M_s \xrightarrow{\varphi_s} M_{s-1},$$

this is an exact sequence. As we noted before for a sequence of this type being exact is equivalent to $\varphi_s : M_s \to M_{s-1}$ being injective. This gives us an isomorphism $\varphi_s : M_s \longrightarrow \mathrm{im}(\varphi_s)$. Also by exactness we have that $\ker(\varphi_{s-1}) = \mathrm{im}(\varphi_s) \simeq M_s$. Since by assumption $M_s$ is a free module, it follows that $\ker(\varphi_{s-1})$ is a free module.

For our second statement, suppose we have a free resolution of some arbitrary length, where $\ker(\varphi_s)$ is a free module for some $s$ in our resolution. Then,

$$0 \longrightarrow \ker(\varphi_{s-1}) \xrightarrow{i} M_{s-1} \xrightarrow{\varphi_{s-1}} M_{s-2} \longrightarrow \ldots \longrightarrow M_0 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

where $i$ is the inclusion mapping, defines a finite free resolution of length $s$. This proves our second assertion.

□

# 3 Hilbert's Syzygy Theorem

In this chapter we present Schreyer's theorem and use it to prove the syzygy theorem.

Before we can prove Schreyer's theorem we first need to establish some notation.

Let $\mathcal{G} = \{g_1, \ldots, g_s\}$ be a Gröbner basis for a submodule $M \subset \mathcal{R}^t$ with respect to a monomial order $>$, and let $\epsilon_1, \ldots, \epsilon_s$ denote the standard basis vectors for $\mathcal{R}^s$.

The monomial ordering on $\mathcal{R}^s$ that is denoted by $>_{\mathcal{G}}$, is defined as follows: $x^\alpha \epsilon_i >_{\mathcal{G}} x^\beta \epsilon_j$ if $\mathrm{LT}_>(x^\alpha g_i) > \mathrm{LT}_>(x^\beta g_j)$ in $\mathcal{R}^t$, or if $\mathrm{LT}_>(x^\alpha g_i) = \mathrm{LT}_>(x^\beta g_j)$ and $i < j$.

By applying Buchberger's criterion and the division algorithm we find the following expression for S-vectors of elements in $\mathcal{G}$ :

$$S(g_i, g_j) = \sum_{k=1}^{s} a_{ijk} g_k,$$

where $a_{ijk} \in \mathcal{R}$, and $\mathrm{LT}(a_{ijk}, g_k) \leq \mathrm{LT}(S(g_i, g_j))$ for all $i, j, k$. Let $m_{i,j} = \mathrm{LCM}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))$, and let $\mathbf{a}_{i,j} = \sum_{k=1}^{s} a_{ijk}\epsilon_k \in \mathcal{R}^s$.

Finally for $i, j$ such that $m_{i,j} \neq 0$, let

$$s_{i,j} = \frac{m_{i,j}}{\mathrm{LT}(g_i)}\epsilon_i - \frac{m_{i,j}}{\mathrm{LT}(g_j)}\epsilon_j - \mathbf{a}_{i,j} \in \mathcal{R}^s,$$

and $s_{i,j} = 0$ otherwise. We are now ready to state and prove Schreyer's theorem.

**Theorem 3.1** (*Schreyer's Theorem*)**.** *Let $\mathcal{G} \in \mathcal{R}^t$ be a Gröbner basis with respect to any monomial order $>$ on $\mathcal{R}^t$. Then the collection of $s_{i,j}$, as defined above, form a Gröbner basis for the syzygy module $Syz(g_1, \ldots, g_s)$ with respect to the monomial order $>_{\mathcal{G}}$ on $\mathcal{R}^s$.*

*Proof.* Note that since $s_{i,j} = -s_{j,i}$, we only have to consider $s_{i,j}$ for $i < j$, and such that $\mathrm{LT}(g_i)$ and $\mathrm{LT}(g_j)$ contain the same basis vector. We start by showing that

$$\mathrm{LT}(s_{i,j}) = \frac{m_{i,j}}{\mathrm{LT}(g_i)}\epsilon_i.$$

First note that since $i < j$, and

$$\frac{m_{i,j}}{\mathrm{LT}(g_i)}\mathrm{LT}(g_i) = \frac{m_{i,j}}{\mathrm{LT}(g_j)}\mathrm{LT}(g_j)$$

it follows that

$$\frac{m_{i,j}}{\mathrm{LT}(g_i)}\epsilon_i >_{\mathcal{G}} \frac{m_{i,j}}{\mathrm{LT}(g_j)}\epsilon_j.$$

Since the terms $a_{ijk}g_k$ in $S(g_i, g_j)$ are obtained using the division algorithm we know that

$$\mathrm{LT}(S(g_i, g_j)) \geq \mathrm{LT}(a_{ijk}g_k) \text{ for } k = 1, \ldots, s.$$

Also, note that

$$\mathrm{LT}(\frac{m_{i,j}}{\mathrm{LT}(g_i)}g_i) > \mathrm{LT}(\frac{m_{i,j}}{\mathrm{LT}(g_i)}g_i - \frac{m_{i,j}}{\mathrm{LT}(g_j)}g_j)$$

$$= \mathrm{LT}(S(g_i, g_j)) \geq \mathrm{LT}(a_{ijk}g_k), \text{ for } k = 1, \ldots, s.$$

Thus, by definition of the monomial order $>_{\mathcal{G}}$ we also have

$$\frac{m_{i,j}}{\mathrm{LT}(g_i)}\epsilon_i >_{\mathcal{G}} \mathrm{LT}(\mathbf{a}_{i,j}).$$

It follows that

$$\mathrm{LT}(s_{i,j}) = \frac{m_{i,j}}{\mathrm{LT}(g_i)}\epsilon_i.$$

Using this we will prove that the $s_{i,j}$ form a Gröbner basis for $\mathrm{Syz}(g_1, \ldots, g_s)$. Let

$$f = \sum_{i=1}^{s} f_i\epsilon_i \in \mathrm{Syz}(g_1, \ldots, g_s), \text{ and}$$

$$\mathrm{LT}_{>_{\mathcal{G}}}(f_i) = c_i h_i \epsilon_i$$

where $h_i$ is a monomial and $c_i$ a coefficient. Also, assume that $\mathrm{LT}(f) = c_v h_v \epsilon_v$ for some $v \in \{1, \ldots, s\}$. We must show that $\mathrm{LT}(f)$ is divisible by some $\mathrm{LT}(s_{i,j})$. We define the set

$$U = \{u \in \{1, \ldots, s\} | h_u \mathrm{LT}(g_u) = h_v \mathrm{LT}(g_v)\},$$

and the sum

$$F = \sum_{u \in U} c_u h_u \epsilon_u.$$

Clearly, $\mathrm{LT}(F) = \mathrm{LT}(f) = c_v h_v \epsilon_v$, and by definition of $>_{\mathcal{G}}$, because $c_v h_v$ is the leading term of $f$, we must have $u \geq v$ for all $u \in U$. Since $\sum_{i=1}^{s} c_i h_i g_i = 0$, it follows that

$$\sum_{u \in U} c_u h_u \mathrm{LT}(g_u) = 0.$$

Thus, $F \in \mathrm{Syz}(\{\mathrm{LT}(g_u) | u \in U\})$. It follows from proposition 2.13 that

$\mathrm{Syz}(\{\mathrm{LT}(g_u) | u \in U\})$ is generated by

$$\frac{m_{i,j}}{\mathrm{LT}(g_i)}\epsilon_i - \frac{m_{i,j}}{\mathrm{LT}(g_j)}\epsilon_j \text{ with } i, j \in U \text{ and } i < j.$$

In particular $F$ is some linear combination of elements of this from, thus $\mathrm{LT}(F) = \mathrm{LT}(f)$ is divisible by $\mathrm{LT}(s_{i,j}) = \frac{m_{i,j}}{\mathrm{LT}(g_i)}\epsilon_i$ for some $i < j$. From this we can conclude that the $\mathrm{LT}(s_{i,j})$ generate $\langle \mathrm{LT}(\mathrm{Syz}(g_1, \ldots, g_s)) \rangle$, and thus form a Gröbner basis for the syzygy module.

□

Schreyer's theorem gives us a way to construct a free resolution, this next lemma ensures that it is finite.

**Lemma 3.2.** *Let $\mathcal{G}$ be a Gröbner basis for a submodule $M \subset \mathcal{R}^t$ with respect to an arbitrary monomial order. Arrange the elements in $\mathcal{G}$ to form the set $G = (g_1, \ldots, g_s)$, ordered according to the following rule: if $LT(g_i)$ and $LT(g_j)$ contain the same standard basis vector $e_k$, and $i < j$, then $\frac{LM(g_i)}{e_k} >_{lex} \frac{LM(g_j)}{e_k}$. If the variables $x_1, \ldots, x_m$ do not appear in the leading terms of elements in $G$, then $x_1, \ldots, x_{m+1}$ do not appear in the leading terms of the $s_{i,j} \in Syz(g_1, \ldots, g_s)$ with respect to $>_{\mathcal{G}}$ as in in Schreyer's theorem.*

*Proof.* Start by noting that, as we saw in the proof of Schreyer's theorem,

$$\mathrm{LT}_{>_{\mathcal{G}}}(s_{i,j}) = \frac{\mathrm{LCM}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))}{\mathrm{LT}(g_i)}\epsilon_i$$

where $\epsilon_i \in \mathcal{R}^s$ is a standard basis element, $\mathrm{LT}(g_i)$ and $\mathrm{LT}(g_j)$ contain the same standard basis vector, and $i < j$. Let $g_i, g_j \in G$ such that $\mathrm{LT}(g_i)$ and $\mathrm{LT}(g_j)$ contain the same standard basis element $e_k \in \mathcal{R}^t$, and $i < j$. Then, since we ordered $G_0$ as prescribed by the lemma, we have that

$$\frac{\mathrm{LM}(g_i)}{e_k} >_{lex} \frac{\mathrm{LM}(g_j)}{e_k}$$

where $>_{lex}$ is the lexicographical order on $\mathcal{R}$ with $x_1 > \ldots > x_n$. To clarify, this implies that if $\frac{\mathrm{LM}(g_i)}{e_k} = x^\alpha$ and $\frac{\mathrm{LM}(g_j)}{e_k} = x^\beta$, then the leftmost nonzero term in $\alpha - \beta \in Z^n$ is positive. Since, by assumption $x_1 \ldots x_m$ do not appear in the leading terms of $g_i$ and $g_j$ we can write

$$\frac{\mathrm{LM}(g_i)}{e_k} = x_{m+1}^a y_i \text{ and}$$

$$\frac{\mathrm{LM}(g_j)}{e_k} = x_{m+1}^b y_j,$$

where $a \geq b$, and $y_i, y_j \in \mathcal{R}$ are monomials that do not contain the variable $x_{m+1}$. The leading term of $s_{i,j}$ becomes

$$\mathrm{LT}(s_{i,j}) = \frac{\mathrm{LCM}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))}{\mathrm{LT}(g_i)}\epsilon_i = c_{i,j}\frac{x_{m+1}^a \mathrm{LCM}(y_i, y_j)}{x_{m+1}^a y_i}\epsilon_i = c_{i,j}\frac{\mathrm{LCM}(y_i, y_j)}{y_i}\epsilon_i$$

where $0 \neq c_{i,j} \in k$. We can now conclude that, $x_1, \ldots, x_{m+1}$ are missing from the leading terms of the $s_{i,j}$. □

We are now ready to state and prove the syzygy theorem.

**Theorem 3.3** (*Hilbert's Syzygy Theorem*)**.** *Let $\mathcal{R} = k[x_1, \ldots, x_n]$. Every finitely generated $\mathcal{R}$-module $M$ has a free resolution of length $\leq n$.*

*Proof.* We start by noting that by using Buchberger's algorithm, given a set of generators for a submodule of $\mathcal{R}^s$ we can compute a Gröbner basis for the submodule. It follows that since $M$ is finitely generated that there is a presentation for $M$ given by the exact sequence

$$\mathcal{R}^{s_1} \xrightarrow{\varphi_1} \mathcal{R}^{s_0} \xrightarrow{\varphi_0} M \longrightarrow 0$$

which corresponds to a set of generators $(m_1, \ldots, m_{s_0})$ for $M$ and a Gröbner basis $\mathcal{G}_0 \subset \mathcal{R}^{s_0}$ with $s_1$ elements for $\mathrm{Syz}(m_1, \ldots, m_{s_0}) \subset \mathcal{R}^{s_0}$, with respect to any monomial order on $\mathcal{R}^{s_0}$, where

$$\mathrm{Syz}(m_1, \ldots, m_{s_0}) = \mathrm{im}(\varphi_1) = \ker(\varphi_0) \subset \mathcal{R}^{s_0}, \text{ and}$$

$$\ker(\varphi_1) = \mathrm{Syz}(\mathcal{G}_0) \subset \mathcal{R}^{s_1}.$$

Now let us order the Gröbner basis $\mathcal{G}_0$ according to the previous lemma to obtain the ordered Gröbner basis $G_0 = (g_1, \ldots, g_{s_1})$, and use Schreyer's theorem to compute a Gröbner basis $\mathcal{G}_1$ for $\mathrm{Syz}(G_0)$, with respect to the order $>_{G_0}$, which consists of elements of the form

$$s_{i,j} = \frac{\mathrm{LCM}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))}{\mathrm{LT}(g_i)}\epsilon_i - \frac{\mathrm{LCM}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))}{\mathrm{LT}(g_j)}\epsilon_j - \mathbf{a}_{i,j} \in \mathcal{R}^{s_1}$$

where $g_i$ and $g_j$ contain the same basis element and looking back at the proof, we may assume that $i < j$, and

$$\mathrm{LT}(s_{i,j}) = \frac{\mathrm{LCM}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))}{\mathrm{LT}(g_i)}\epsilon_i.$$

It follows from lemma 3.2 that in the leading terms of the $s_{i,j}$, at least the variable $x_1$ is missing. Assuming the $\mathcal{G}_1$ has $s_2$ elements, since it is a generating set for $\mathrm{Syz}(G_0)$, using proposition 2.25 we obtain a surjective homomorphism $\varphi_2 : \mathcal{R}^{s_2} \to \mathrm{Syz}(G_0)$ with $\mathrm{im}(\varphi_2) = \ker(\varphi_1) = \mathrm{Syz}(G_0) \subset \mathcal{R}^{s_1}$ and $\ker(\varphi_2) = \mathrm{Syz}(\mathcal{G}_1) \subset \mathcal{R}^{s_2}$. Now we can extend our presentation to the exact sequence

$$\mathcal{R}^{s_2} \xrightarrow{\varphi_2} \mathcal{R}^{s_1} \xrightarrow{\varphi_1} \mathcal{R}^{s_0} \xrightarrow{\varphi_0} M \longrightarrow 0.$$

Note that every time we apply this procedure the new set of generators we find is due to Schreyers theorem. Therefore since the building blocks of the leading terms of elements in this new set of generators are the generators obtained in the previous step, once we lose any number of variables in a step we can be certain they do not reappear. We can repeat this process $t-1$ times to obtain an exact sequence

$$\mathcal{R}^{s_t} \xrightarrow{\varphi_t} \mathcal{R}^{s_{t-1}} \longrightarrow \ldots \longrightarrow \mathcal{R}^{s_2} \xrightarrow{\varphi_2} \mathcal{R}^{s_1} \xrightarrow{\varphi_1} \mathcal{R}^{s_0} \xrightarrow{\varphi_0} M \longrightarrow 0.$$

Where $\mathrm{im}(\varphi_t) = \ker(\varphi_{t-1}) = \mathrm{Syz}(G_{t-2})$ and $\ker(\varphi_t) = \mathrm{Syz}(G_{t-1})$. Also, if we once more apply Schreyer's theorem and the lemma we find an ordered Gröbner basis $G_t$, for $\mathrm{Syz}(G_{t-1})$, with respect to the monomial order $>_{G_{t-1}}$, for which the leading terms of its elements miss, at least, the variables $x_1, \ldots, x_t$.

It follows that there exists an $r \leq n$ such that after repeating the procedure $r$ times at the $r$'th step we obtain a Gröbner basis for which the leading terms of its elements do not contain any of the variables $x_1, \ldots, x_n$. Thus, we can extend the presentation that we started with to an exact sequence

$$(*) \quad \mathcal{R}^{s_r} \xrightarrow{\varphi_r} \mathcal{R}^{s_{r-1}} \longrightarrow \ldots \longrightarrow \mathcal{R}^{s_2} \xrightarrow{\varphi_2} \mathcal{R}^{s_1} \xrightarrow{\varphi_1} \mathcal{R}^{s_0} \xrightarrow{\varphi_0} M \longrightarrow 0.$$

Where $\mathrm{im}(\varphi_r) = \ker(\varphi_{r-1}) = \mathrm{Syz}(G_{r-2})$, $\ker(\varphi_r) = \mathrm{Syz}(G_{r-1})$, and at the $r$'th step we get the Gröbner basis $G_r$ for $\mathrm{Syz}(G_{r-1})$ for which the leading terms of its elements do not contain any of the variables $x_1, \ldots, x_n$. Now by applying the algorithm for obtaining monic Gröbner bases to $G_r$ we have found a monic Gröbner basis $\hat{G}_r = \{\hat{g}_1, \ldots, \hat{g}_{s_r}\}$ for $\mathrm{Syz}(G_{r-1})$ with respect to the monomial order $>_{G_{r-1}}$. Note that since $\hat{G}_r$ is monic and the leading terms of its elements do not contain any variables, the leading terms are standard basis elements in $\mathcal{R}^{s_{r-1}}$. Thus, $\hat{g}_i \in \hat{G}_r$ is of the form

$$\hat{g}_i = e_i + f_i$$

where $e_i$ is the leading term for $\hat{g}_i$ and $f_i \in \mathcal{R}^{s_{r-1}}$, where none of the monomials that make up $f_i$ contain the basis element $e_i$. More so, if a basis element occurs in the leading term of some $\hat{g}_i \in \hat{G}_r$, then it is not contained in any of the monomials that make up $\hat{g}_j \in \hat{G}_r$ for all $j \neq i$. From this last fact it follows that $\hat{G}_r$ is a linearly independent set. Therefore, besides being a Gröbner basis for $\mathrm{Syz}(G_{r-1})$, since $\hat{G}_r$ is a linearly independent generating set for $\mathrm{Syz}(G_{r-1})$, it is also a basis for $\mathrm{Syz}(G_{r-1})$. Thus, $\ker(\varphi_r) = \mathrm{Syz}(G_{r-1})$ is a free module. At this point we are able to produce a free resolution of maximal length $n+1$ by applying proposition 2.31 so that we get the free resolution

$$0 \longrightarrow \ker(\varphi_r) \xrightarrow{i} \mathcal{R}^{s_r} \xrightarrow{\varphi_r} \mathcal{R}^{s_{r-1}} \longrightarrow \ldots \longrightarrow \mathcal{R}^{s_2} \xrightarrow{\varphi_2} \mathcal{R}^{s_1} \xrightarrow{\varphi_1} \mathcal{R}^{s_0} \xrightarrow{\varphi_0} M \longrightarrow 0,$$

where $i$ is the inclusion map. To get a free resolution of maximal length $n$ we proceed by showing that $\ker(\varphi_{r-1}) = \mathrm{Syz}(G_{r-2})$ is a free module.

Now consider the quotient module $\mathcal{R}^{s_r}/\langle \hat{G}_r \rangle$, we claim that this is a free module. To prove the claim, let $\hat{M} \subset \mathcal{R}^{s_r}$ be the free module generated by the set of basis elements of $\mathcal{R}^{s_r}$ that are not contained in any of the leading terms of the elements in $\hat{G}_r$, and consider the map

$$\Phi : \hat{M} \to \mathcal{R}^{s_r}/\langle \hat{G}_r \rangle$$

$$\Phi(\hat{m}) = \hat{m} + \langle \hat{G}_r \rangle.$$

With the definition of a quotient module and a module homomorphism in mind it is easily verified that the map is a homomorphism. Suppose that $\hat{m} \in \hat{M}$ as well as $\langle \hat{G}_r \rangle$. Then, since $\hat{G}_r$ is a Gröbner basis for $\langle \hat{G}_r \rangle$, it follows that there exists a $\hat{g}_i \in \hat{G}_r$ such that $\mathrm{LT}(\hat{g}_i)$ divides $\mathrm{LT}(\hat{m})$. By construction of $\hat{M}$ this can only be the case if $\hat{m} = 0$. It follows that $\Phi$ is injective. Let $[f] \in \mathcal{R}^{s_r}/\langle \hat{G}_r \rangle$ and let $r$ be the remainder of $f$ on division by $\hat{G}_r$. It follows from proposition 2.19 that $[f] = [r]$, where none of the monomials that make up $r$ can be divided by any of the $\mathrm{LM}(\hat{g}_i)$, thus $r \in \hat{M}$ and $\Phi$ is surjective. We can now conclude that $\Phi$ is an isomorphism and consequently that $\mathcal{R}^{s_r}/\langle \hat{G}_r \rangle$ is a free module.

Next, let us note that it follows from the first isomorphism theorem for modules that

$$\mathcal{R}^{s_r}/\langle \hat{G}_r \rangle = \mathcal{R}^{s_r}/\mathrm{Syz}(G_{r-1}) = \mathcal{R}^{s_r}/\ker(\varphi_r) \simeq \mathrm{im}(\varphi_r) = \mathrm{Syz}(G_{r-2}) = \ker(\varphi_{r-1}).$$

If we now return to our sequence $(*)$ and apply proposition 2.31, we obtain our desired free resolution of length $r \leq n$

$$0 \longrightarrow \ker(\varphi_{r-1}) \xrightarrow{i} \mathcal{R}^{s_{r-1}} \xrightarrow{\varphi_{r-1}} \ldots \longrightarrow \mathcal{R}^{s_2} \xrightarrow{\varphi_2} \mathcal{R}^{s_1} \xrightarrow{\varphi_1} \mathcal{R}^{s_0} \xrightarrow{\varphi_0} M \longrightarrow 0.$$

□

We will now give an example using computer algebra system Singular, and the function "sres" which computes free resolutions for quotient modules, using Schreyer's method.

**Example 3.4.** Let $I$ be the homogeneous ideal generated by $abc, ab + be, de \in \mathcal{R} = \mathbb{Z}_{907}[a, b, c, d, e]$ with the $>_{grlex}$ order. We get the free resolution

$$\mathcal{R} \xrightarrow{d_3} \mathcal{R}^3 \xrightarrow{d_2} \mathcal{R}^3 \xrightarrow{d_1} \mathcal{R} \longrightarrow \mathcal{R}/I \longrightarrow 0$$

for $\mathcal{R}/I$. The map $d_3$ sends $1 \to (c, -a - e, d)^T$,

$d_2$ sends $e_1 \to (-ab - be, de, 0)^T$, $e_2 \to (-bc, 0, d)^T$, and $e_3 \to (0, -ce, a + e)^T$, and

$$d_1 \text{ sends } e_1 \to de,\ e_2 \to ab + be \text{ and } e_3 \to bce.$$

# 4 Graded modules and Hilbert Polynomials

In this chapter we study a particular graded module, namely the homogeneous ideals $I$ in the polynomial ring $\mathcal{R} = \mathbb{C}[x_0, \ldots, x_n]$. In this chapter $\mathcal{R}$ will denote the polynomial ring $\mathbb{C}[x_0, \ldots, x_n]$. Note that $\mathcal{R}/I$ is the homogeneous coordinate ring of a closed subscheme $X \subset \mathbb{P}^n$.

This brings us to another important motivation for the study of resolutions, which is that they can be used to extract information about $X$. Examples are the dimension, the arithmetic genus, and the degree of $X$. In this chapter we will define what is meant by "graded", give three ways to construct graded free resolutions, and how to read off the discussed information. Also we will work out some examples.

**Definition 4.1.** A ring $\mathcal{S}$ is said to be **($\mathbb{Z}_{\geq 0}$-)graded** if there exists a collection of additive subgroups $\{\mathcal{S}_n\}_{n \in \mathbb{Z}_{\geq 0}}$ of $\mathcal{S}$ such that

1. $\mathcal{S} = \bigoplus_{n \in \mathbb{Z}_{\geq 0}} \mathcal{S}_n$, and
2. $\mathcal{S}_n \mathcal{S}_m \subset \mathcal{S}_{n+m}$ for all $n, m \in \mathbb{Z}_{\geq 0}$.

**Definition 4.2.** Let $\mathcal{S}$ be a graded ring and $M$ an $\mathcal{S}$-module. Then $M$ is said to be a a graded $\mathcal{S}$-module if there exists a collection of additive subgroups $\{M_n\}_{n \in \mathbb{Z}}$ of $M$ such that

1. $M = \bigoplus_{n \in \mathbb{Z}} M_n$, and
2. $\mathcal{S}_n M_m \subset M_{n+m}$ for all $n, m \in \mathbb{Z}$.

For graded rings and modules, the homogeneous elements of degree $d$ are the non zero elements respectively in $\mathcal{S}_d$ and $M_d$.

**Definition 4.3.** We say that a submodule $N$ of a graded module $\mathcal{R}$-module $M$ is a **graded submodule** if it satisfies the following equivalent conditions.

1. If $f \in N$, then every homogeneous component of $f$ is in $N$.
2. $N = \oplus_{i \in \mathbb{Z}} N_i$, where $N_i = M_i \cap N$.
3. If $\tilde{N}$ is the submodule generated by all homogeneous elements in $N$, then $N = \tilde{N}$.

**Proposition 4.4.** *If $M$ is a graded $\mathcal{R}$-module and $N \subset M$ is a graded submodule of $M$, then $M/N$ is also a graded module, with grading*

$$M/N = \oplus_{i \in \mathbb{Z}} (M/N)_i \text{ where } (M/N)_i = M_i/N_i.$$

Given a graded $\mathcal{R}$-module $M$ we can produce a new graded $\mathcal{R}$-module $M(d)$ by shifting its grading $d$ steps. That is to say we define $M(d)$ to be the to be the graded module isomorphic to $M$ with the grading $M(d)_t = M_{t+d}$. The module $M(d)$ is also said to be the d'th twist or shift of $M$.

The particular example of a graded modules that we are interested in are the homogeneous ideals $I \subset \mathcal{R}$. The ring $\mathcal{R}$ has the direct sum decomposition

$$\mathcal{R} = \bigoplus_{i \in \mathbb{Z}_{\geq 0}} \mathcal{R}_i$$

where $\mathcal{R}_i$ is the $\mathbb{C}$-vector subspace generated by homogeneous polynomials of degree $i$, with 0. The grading on the ideal can be defined by setting $I_k = I \cap \mathcal{R}_k$ for $k \geq 0$, which is the set containing all homogeneous polynomials of degree $k$ in $I$, and $I_k = 0$ for $k < 0$. Additionally, the free module $\mathcal{R}^m$ has a graded module structure given by $(\mathcal{R}^m)_k = (\mathcal{R}_k)^m$, and a submodule $M \subset \mathcal{R}^m$ also has a graded module structure, namely by setting $M_k = (\mathcal{R}_k)^m \cap M$.

**Definition 4.5.** Let $M$ and $N$ be graded $\mathcal{R}$-modules. Then a homomorphism $\varphi : M \to N$ is a **graded homomorphism of degree** $d$ if $\varphi(M_t) \subset N_{t+d}$.

We are now able to define graded free resolutions.

**Definition 4.6.** A **graded free resolution** of a graded $\mathcal{R}$-module $M$ is an exact sequence

$$\ldots \longrightarrow M_2 \xrightarrow{\varphi_2} M_1 \xrightarrow{\varphi_1} M_0 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

such that each term $M_i$ in the sequence is a twisted graded free module, i.e. of the form $\mathcal{R}(-d_1) \oplus \ldots \oplus \mathcal{R}(-d_m)$, and the maps are graded homomorphisms of degree 0.

The Hilbert function of such an ideal, and more generally a finitely generated graded module over $\mathcal{R}$ is defined as follows.

**Definition 4.7.** Let $M$ be a finitely generated graded $\mathcal{R}$-module, where $\mathcal{R}$ has the discussed grading. Then the function

$$H_M : \mathbb{Z} \to \mathbb{Z}, \text{ with } H_M(s) = dim_{\mathbb{C}} M_s$$

is the **Hilbert function of** $M$.

Let $M$ be a graded $\mathcal{R}$-module. Given a finite graded free resolution

$$(*)\ 0 \longrightarrow M_t \longrightarrow \ldots \longrightarrow M_2 \xrightarrow{\varphi_2} M_1 \xrightarrow{\varphi_1} M_0 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

where $M_i = \oplus_j \mathcal{R}(-d_{i,j})$, then using straight-forward homological algebra, the Hilbert function is given by

$$H_M(s) = dim_{\mathbb{C}} M_s = \sum_{i=0}^{t} (-1)^i \sum_j \binom{n+s-d_{i,j}}{n}.$$

**Definition 4.8.** Let $M$ be a graded $\mathcal{R}$-module with Hilbert function $H_M$. A polynomial $P_M(s) \in \mathbb{Q}[x]$ of degree $\leq n$ which is equal to the Hilbert function for sufficiently large $s$ is called the **Hilbert polynomial** for $M$.

**Proposition 4.9.** *Given a graded free resolution* $(*)$. *We have*

$$P_M(s) = H_M(s) = \sum_{i=0}^{t} (-1)^i \sum_j \frac{(s-d_{i,j}+n)(s-d_{i,j}+n-1)\dots(s-d_{i,j}+1)}{n!}.$$

*for* $s \geq \max_{i,j}\{d_{i,j} - n\}$.

This polynomial carries the information we wanted, given a Hilbert polynomial $c_m x^m + c_{m-1}x^{m-1} + \ldots + c_0$ for a coordinate ring $\mathcal{R}/I$, the dimension of the corresponding subscheme is m, the degree of the polynomial, the degree of the subscheme is the leading coefficient $c_m$, and the arithmetic genus is $(-1)^m(c_0 - 1)$.

We will proceed by giving three ways of constructing finite graded free resolutions and give examples using them.

**Definition 4.10.** Let $M$ and $M'$ be $\mathcal{R}$-modules. The **Tensor product** of $M$ and $M'$ denoted by $M \otimes_{\mathcal{R}} M'$, or $M \otimes M'$ when there is no risk of confusion, is the $\mathcal{R}$-module generated by

$$\{m \otimes m' | m \in M, m' \in M'\},$$

which for $r \in \mathcal{R}$, $m_1, m_2 \in M$ and $m_1', m_2' \in M'$ has the following relations

1. $rm_1 \otimes m_1' = m_1 \otimes rm_1'$,
2. $(m_1 + m_2) \otimes m_1' = m_1 \otimes m_1' + m_2 \otimes m_1'$ and
3. $m_1 \otimes (m_1' + m_2') = m_1 \otimes m_2' + m_1 \otimes m_2'$.

We also define **k**-fold tensor product of $M$, $M^{\otimes k}$ which for $k = 0$ is equal to $\mathcal{R}$, $k = 1$ is equal to $M$, and for $k \geq 1$

$$M^{\otimes k} = M \otimes \underset{\times k}{\ldots} \otimes M$$

The tensor power of a graded module has a grading of its own defined by

$$M^{\otimes k} = \oplus_{d\in\mathbb{Z}}(\oplus_{i_1+\ldots+i_k=d}(M_{i_1}\otimes\ldots\otimes M_{i_k})) = \oplus_{d\in\mathbb{Z}}(M^{\otimes k})_d.$$

**Definition 4.11.** Let $M$ be a $\mathcal{R}$-module. The **kth exterior power of** $M$ denoted by $\wedge^k M$ is the module

$$M^{\otimes k}/\{m_1\otimes\ldots\otimes m_k | m_1,\ldots,m_k\in M,\ m_i = m_j \text{ for some } i\neq j\}.$$

For $[m_1\otimes\ldots\otimes m_k]\in\wedge^k M$ we write $m_1\wedge\ldots\wedge m_k$.

**Remark.** Let $e_1,\ldots,e_m$ denote a basis for $\mathcal{R}^m$. Then $\wedge^k\mathcal{R}^m$ is generated by the set $G_{k,m} = \{e_{i_1,\ldots,i_k} | 1\leq i_1 < i_2 < \ldots < i_k \leq m\}$ and $\wedge^k\mathcal{R}^m \simeq \mathcal{R}^{\binom{m}{k}}$.

The exterior power of a graded module $M$ also is a graded module. The tensor power is a graded module, and $I = \{m_1\otimes\ldots\otimes m_k | m_1,\ldots,m_k\in M,\ m_i = m_j \text{ for some } i\neq j\}$ is a graded submodule of $M^{\otimes k}$. Also, recall that by proposition 4.4 the quotient of a graded module by a graded submodule is a graded module. Thus, $\wedge^k M$ is a graded $\mathcal{R}$-module with grading

$$\oplus_{d\in\mathbb{Z}}((M^{\otimes_k})_d/((M^{\otimes_k})_d\cap I)).$$

**Definition 4.12.** Let $M$ be an $\mathcal{R}$-module. We say that sequence $f_1,\ldots,f_s\in\mathcal{R}$ is a **regular sequence** on $M$ if

1. $\langle f_1,\ldots,f_s\rangle M \neq M,$ and
2. $f_i$ is a nonzerodivisor on $M/\langle f_1\ldots,f_s\rangle M$ for $i = 1,\ldots,s$.

**Definition 4.13** (Koszul Complex)**.** Let $f_1\ldots\ f_s\in\mathcal{R}$, and $e_1,\ldots,e_s$ denote a basis for $\mathcal{R}^s$. The sequence

$$K_\bullet(f_1,\ldots,f_s) := 0\longrightarrow\wedge^s\mathcal{R}^s\xrightarrow{d_s}\wedge^{s-1}\mathcal{R}^s\xrightarrow{d_{s-1}}\wedge^{s-2}\mathcal{R}^s\longrightarrow\ldots\longrightarrow\wedge^1\mathcal{R}^s\xrightarrow{d_1}\mathcal{R}$$

where

$$d_i(e_{j_1}\wedge\ldots\wedge e_{j_i}) = \sum_{k=1}^{i}(-1)^{k+1}f_{j_k}e_{j_1}\wedge\ldots\wedge\hat{e}_{j_k}\wedge\ldots\wedge e_{j_i},$$

and $\hat{e}_{j_k}$ denotes an element that is deleted, is called the **Koszul complex** on $f_1,\ldots,f_s$.

**Theorem 4.14.** *If $f_1,\ldots,f_s\in\mathcal{R}$ is a regular sequence, then $K_\bullet(f_1,\ldots,f_s)$ is a free resolution for $\mathcal{R}/\langle f_1,\ldots,f_s\rangle$*

**Definition 4.15** (Taylor Complex)**.** Let $x^{\alpha_1}, \ldots, x^{\alpha_s} \in \mathcal{R}$, $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, and $e_1, \ldots, e_s$ denote a basis for $\mathcal{R}^s$. Then the sequence

$$T_\bullet(x^{\alpha_1}, \ldots, x^{\alpha_s}) := 0 \longrightarrow \wedge^s \mathcal{R}^s \xrightarrow{\partial_s} \wedge^{s-1} \mathcal{R}^s \xrightarrow{\partial_{s-1}} \wedge^{s-2} \mathcal{R}^s \longrightarrow \ldots \longrightarrow \wedge^1 \mathcal{R}^s \xrightarrow{\partial_1} \mathcal{R}$$

where

$$\partial_i(e_{j_1} \wedge \ldots \wedge e_{j_i}) = \sum_{k=1}^{i} (-1)^{k-1} \frac{\mathrm{LCM}(x^{\alpha_{j_1}}, \ldots, x^{\alpha_{j_i}})}{\mathrm{LCM}(x^{\alpha_{j_1}} \ldots, x^{\hat{\alpha}_{j_k}}, \ldots, x^{\alpha_{j_i}})} a e_{j_1} \wedge \ldots \wedge \hat{e}_{j_k} \wedge \ldots \wedge e_{j_i},$$

and a hat denotes an element that is deleted, is called the **Taylor complex** associated with the sequence $x^{\alpha_1}, \ldots, x^{\alpha_s}$.

**Theorem 4.16.** *Let $x^{\alpha_1}, \ldots, x^{\alpha_s} \subset \mathcal{R}$, and $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$. The Taylor resolution associated with $x^{\alpha_1}, \ldots, x^{\alpha_s}$ is a free resolution for $\mathcal{R}/I$.*

**Theorem 4.17.** *Let $I \subset \mathcal{R}$ be a graded ideal and $>$ a monomial order on $\mathcal{R}$. Then $\mathcal{R}/I$ and $\mathcal{R}/LT(I)$ have the same Hilbert function.*

Note that in case of the Koszul complex as well of the Taylor complex of a graded module, if in addition to the hypotheses of theorems 4.14 and 4.16 we impose a suitable twist on each of the terms in the respective sequences, so that maps in the sequences are homomorphisms of degree 0, then both complexes define a graded free resolution.

We have now discussed two concrete methods to find a graded free resolution for $\mathcal{R}/I$ where $I$ is a homogeneous ideal. In addition we can also find a graded free resolution for $\mathcal{R}/I$ by using an almost identical construction to the one due to Schreyer that we used to prove the syzygy theorem. Next we will discuss the adjustments that we need to make for the graded version of Schreyer's method for constructing free resolutions.

Let us remark that if $I \subset \mathcal{R}$ is an homogeneous ideal, then a reduced Gröbner basis for $I$, with respect to any monomial order on $\mathcal{R}$ consists of homogeneous polynomials. Moreover for a graded submodule $M \subset \mathcal{R}^t$, a reduced Gröbner basis for $M$ with respect to any monomial order on $\mathcal{R}^t$ consists of homogeneous elements. It follows that for a syzygy module $\mathrm{Syz}(g_1, \ldots, g_s) \subset \mathcal{R}^s$ where the $g_i$ are homogeneous, and $(g_1, \ldots, g_s)$ is an ordered Gröbner basis, we can find a Gröbner basis consisting of homogeneous elements by applying Schreyer's theorem and then reducing the obtained Gröbner basis. With this in mind we make the following adjustments for the graded case:

1. At each step find a reduced Gröbner bases that consist of homogeneous elements, where the ith element has degree $d_i$.

2. Let $e_1 \ldots, e_{s_i}$ denote a basis for the ith free module in the sequence, and $g_1, \ldots, g_{s_i}$ homogeneous elements that form a Gröbner basis for $\ker(\varphi_{i-1}) = \text{Syz}(G_{i-2})$. Recall that $\varphi_i(e_i) = g_i$. We redefine $\mathcal{R}^{s_i}$ to be the twisted free module $\mathcal{R}(-d_1) \oplus \ldots \oplus \mathcal{R}(-d_{s_i})$.

We end with the following example.

**Example 4.18.**
Let $I = \langle f_1, f_2 \rangle$ be the homogeneous ideal in $\mathcal{R} = C[x, y, z, w]$, generated by the regular sequence $f_1 = x^2 - yw, f_2 = xy - zw$. This is the intersection of two quadric surfaces in $P^3$, see exercise (2.16) in chapter one of Harthshorne's book [10]. In this example we will determine the Hilbert polynomial for the coordinate ring $\mathcal{R}/I$ using three methods. First by constructing a Koszul complex. Then we find a Gröbner basis for $I$, and construct a Taylor resolution for the leading monomials of the Gröbner basis. Lastly we use computer algebra system Singular to find the graded free resolution for the leading monomials of the Gröbner basis for $I$, with Schreyer's method. It follows from theorem 4.17 that the first method and the two other methods should have the same outcome.

**(Koszul complex)**
Let $I = \langle f_1 = x^2 - yw, f_2 = xy - zw \rangle$. By definition of the Koszul complex, the sequence we obtain for $\mathcal{R}/I$ is of the form

$$0 \longrightarrow \wedge^2\mathcal{R}^2 \xrightarrow{d_2} \wedge^1\mathcal{R}^2 \xrightarrow{d_1} \mathcal{R} \xrightarrow{d_0} \mathcal{R}/I \longrightarrow 0,$$

where the $d_0$ is the homomorphism sending elements $f \in \mathcal{R}$ to $f + I \in \mathcal{R}/I$.
Let $e_1, e_2$ denote the standard basis elements for the free module $\mathcal{R}^2$. It follows that 1 defines a basis for $\mathcal{R}$, $e_1$ and $e_2$ define a basis for $\wedge^1\mathcal{R}^2$, and $e_1 \wedge e_2$ defines a basis for $\wedge^2\mathcal{R}^2$. Using these bases the maps $d_1$ and $d_2$ are defined as follows

$$d_1(e_1) = (-1)^2(f_1),\ d_1(e_2) = (-1)^2 f_2, \text{ and } d_2(e_1 \wedge e_2) = (-1)^2 f_1 e_2 + (-1)^3 f_2 e_1.$$

First we shift the domain of $d_1$ in order to make it a degree 0 map. Note that the map $d_0$ is already has degree 0. The homomorphism $d_1$, by default sends the standard basis elements of degree 0 to to an element $f_i$ of degree 2, it follows that for $d_1$ to be homogeneous we have to shift the degree of $\mathcal{R}^2$ by $-2$ so that in $\mathcal{R}(-2) \oplus \mathcal{R}(-2)$ the basis elements are homogeneous elements of degree 2. The map $d_1$ is now has degree 0. This gives us

$$(*)\ \mathcal{R}(-2) \oplus \mathcal{R}(-2) \xrightarrow{d_1} \mathcal{R} \xrightarrow{d_0} \mathcal{R}/I \longrightarrow 0.$$

Where $d_1$ has degree 0. Next we consider

$$d_2 : \wedge^2\mathcal{R}^2 \to \mathcal{R}(-2) \oplus \mathcal{R}(-2),$$

this map sends the a basis element $e_1 \wedge e_2$ of degree 0 to an element $(-1)^2 f_1 e_2 + (-1)^3 f_2 e_1$ of degree 4. We have to shift the grading by $-4$ so that we get $\wedge^2\mathcal{R}^2(-4)$ with $deg(e_i \wedge e_j) = 4$. We can now extend the sequence so that we get the graded free resolution

$$0 \longrightarrow \wedge^2\mathcal{R}^2(-4) \xrightarrow{d_2} \begin{matrix}\mathcal{R}(-2)\\ \oplus \\ \mathcal{R}(-2)\end{matrix} \xrightarrow{d_1} \mathcal{R} \xrightarrow{d_0} \mathcal{R}/I \longrightarrow 0.$$

Plugging the grades into formula from proposition 4.9 we find that the corresponding Hilbert polynomial is

$$P_{\mathcal{R}/I}(x) = 4x.$$

Thus, $X = \{P \in P(C)^3 : f_1(P) = 0, \text{ and } f_2(P) = 0\}$ has dimension 1, degree 4 and arithmetic genus 1.

**(Taylor complex)**
Equip $\mathcal{R}$ with the $>_{grevlex}$ monomial order. Using computer algebra we find the following Gröbner basis $g_1 = xy - zw,\ g_2 = x^2 - yw$ and $g_3 = y^2w - xzw$ for the ideal $\langle f_1, f_2\rangle$. It follows that $I' = \mathrm{LT}(I)$ is generated by $xy,\ x^2$ and $y^2w$. By definition of the Taylor complex we get the following sequence for $\mathcal{R}/I'$ :

$$0 \longrightarrow \wedge^3\mathcal{R}^3 \xrightarrow{\partial_3} \wedge^2\mathcal{R}^3 \xrightarrow{\partial_2} \wedge^1\mathcal{R}^3 \xrightarrow{\partial_1} \mathcal{R} \xrightarrow{\partial_0} \mathcal{R}/I' \longrightarrow 0.$$

Denote the basis elements in $\mathcal{R}^3$ by $e_1, e_2, e_3$.

$$e_1 \wedge e_2 \wedge e_3 \in \wedge^3\mathcal{R}^3 \text{ defines a basis for } \wedge^3 \mathcal{R}^3,$$

$$e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3 \in \wedge^2\mathcal{R}^3 \text{ define a basis for } \wedge^2 \mathcal{R}^3$$

$$:= \mathcal{R}^3_{e_1\wedge e_2} \oplus \mathcal{R}^2_{e_1\wedge e_3} \oplus \mathcal{R}^3_{e_2\wedge e_3},$$

$$e_1, e_2, e_3 \in \wedge^1\mathcal{R}^3 \text{ define a basis for } \wedge^1 \mathcal{R}^3.$$

The maps are

$$\partial_0(1) = 1 + I',\ \partial_1(e_1) = (-1)^0 xy,\ \partial_1(e_2) = (-1)^0 x^2 \text{ and } \partial_1(e_3) = (-1)^0 y^2 w.$$

$$\partial_2(e_1 \wedge e_2) = (-1)^0 \frac{\mathrm{LCM}(xy, x^2)}{x^2} e_2 + (-1)^1 \frac{\mathrm{LCM}(xy, x^2)}{xy} e_1 = ye_2 - xe_1,$$

$$\partial_2(e_1 \wedge e_3) = (-1)^0 \frac{\mathrm{LCM}(xy, y^2 w)}{y^2 w} e_3 + (-1)^1 \frac{\mathrm{LCM}(xy, y^2 w)}{xy} e_1 = xe_3 - ywe_1, \text{ and}$$

$$\partial_2(e_2 \wedge e_3) = (-1)^0 \frac{\mathrm{LCM}(x^2, y^2 w)}{y^2 w} e_3 + (-1)^1 \frac{\mathrm{LCM}(x^2, y^2 w)}{x^2} e_2 = x^2 e_3 - y^2 we_2.$$

$$\partial_3(e_1 \wedge e_2 \wedge e_3) = (-1)^0 \frac{\mathrm{LCM}(xy, x^2, y^2 w)}{\mathrm{LCM}(x^2, y^2 w)} e_2 \wedge e_3 +$$

$$(-1)^1 \frac{\mathrm{LCM}(xy, x^2, y^2 w)}{\mathrm{LCM}(xy, y^2 w)} e_1 \wedge e_3 + (-1)^2 \frac{\mathrm{LCM}(xy, x^2, y^2 w)}{\mathrm{LCM}(xy, x^2)} e_1 \wedge e_2$$

$$= e_2 \wedge e_3 - xe_1 \wedge e_3 + ywe_1 \wedge e_2.$$

The map $\partial_1$ sends $e_1$ to an element of order 2, $e_2$ to an element of order 2, and $e_3$ to an element of order 3. Thus we shift by, respectively $-2,\ -2$ and $-3$ so that we get

$$\mathcal{R}(-2) \oplus \mathcal{R}(-2) \oplus \mathcal{R}(-3) \xrightarrow{\partial_1} \mathcal{R} \xrightarrow{\partial_0} \mathcal{R}/I' \longrightarrow 0.$$

The map $\partial_2$ sends $e_1 \wedge e_2$ to $ye_2 - xe_1$ which is a homogeneous element of degree 3, it sends $e_1 \wedge e_3$ to $xe_3 - ywe_1$ which is of degree 4, here we have to keep in mind that $e_3$ is an element of degree 3, and it sends $e_2 \wedge e_3$ to $x^2 e_3 - y^2 we_1$ which is of degree 5. If we shift by $-3,\ -4,$ and $-5$ we get the following sequence with graded maps of degree 0 :

$$\begin{array}{ccccccccc}
\mathcal{R}^3_{e_1\wedge e_2}(-3) & & \mathcal{R}(-2) & & & & & & \\
\oplus & & \oplus & & & & & & \\
\mathcal{R}^3_{e_1\wedge e_3}(-4) & \xrightarrow{\partial_2} & \mathcal{R}(-2) & \xrightarrow{\partial_1} & \mathcal{R} & \xrightarrow{\partial_0} & \mathcal{R}/I' & \longrightarrow & 0. \\
\oplus & & \oplus & & & & & & \\
\mathcal{R}^3_{e_2\wedge e_3}(-5) & & \mathcal{R}(-3) & & & & & &
\end{array}$$

The last map $\partial_3$ sends $e_1 \wedge e_2 \wedge e_3$ to $e_2 \wedge e_3 - xe_1 \wedge e_3 + ywe_1 \wedge e_2$ which is a homogeneous element of degree 5. By shifting the domain of $\partial_3$ by $-5$ we get the following graded free resolution for $\mathcal{R}/I'$ :

$$0 \longrightarrow \wedge^3\mathcal{R}^3(-5) \xrightarrow{\partial_3} \begin{matrix}\mathcal{R}^3_{e_1\wedge e_2}(-3)\\ \oplus \\ \mathcal{R}^3_{e_1\wedge e_3}(-4)\\ \oplus \\ \mathcal{R}^3_{e_2\wedge e_3}(-5)\end{matrix} \xrightarrow{\partial_2} \begin{matrix}\mathcal{R}(-2)\\ \oplus \\ \mathcal{R}(-2)\\ \oplus \\ \mathcal{R}(-3)\end{matrix} \xrightarrow{\partial_1} \mathcal{R} \xrightarrow{\partial_0} \mathcal{R}/I' \longrightarrow 0.$$

When plugging these values into the formula for the Hilbert polynomial, we see that the Hilbert polynomials obtained by the first two methods indeed coincide.

**(Schreyer's method)**
If we use the $>_{grevlex}$ monomial order, and the function "sRes" for computing graded free resolutions with Schreyer's method, Singular returns the following graded free resolution for $\mathcal{R}/I'$ :

$$0 \longrightarrow \begin{matrix}\mathcal{R}(-3)\\ \oplus \\ \mathcal{R}(-4)\end{matrix} \xrightarrow{\varphi_2} \begin{matrix}\mathcal{R}(-2)\\ \oplus \\ \mathcal{R}(-2)\\ \oplus \\ \mathcal{R}(-3)\end{matrix} \xrightarrow{\varphi_1} \mathcal{R} \xrightarrow{\varphi_0} \mathcal{R}/I'.$$

Denote the standard basis vectors for $\mathcal{R}^2$ by $e_1$ and $e_2$, and for $\mathcal{R}^3$ by $\epsilon_1,\ \epsilon_2$ and $\epsilon_3$. The maps are

$$\varphi_2(e_1) = -x\epsilon_1 + y\epsilon_2 \text{ and } \varphi_2(e_2) = -yw\epsilon_1 + x\epsilon_3, \text{ and}$$

$$\varphi_1(\epsilon_1) = xy,\ \varphi_1(\epsilon_2) = x^2 \text{ and } \varphi_1(\epsilon_3) = y^2w.$$

Once again plugging the values into the formula for the Hilbert polynomial we see that all three methods have the same outcome.

# References


[1] David A. Cox, John Little, Donal O'Shea *Using Algebraic Geometry*, Springer-Verlag New York, 2, 2005

[2] David Eisenbud *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, 1, 1995

[3] David Eisenbud *The Geometry of Syzygies*, Springer-Verlag, 1, 2005

[4] William W.Adams, Philippe Loustaunau *An Introduction to Gröbner Bases*, American Mathematical Society, 1, 1994

[5] Gert-Martin Greuel, Gerhard Pfister *A Singular Introduction to Commutative Algebra*, Springer-Verlag, 2, 2008

[6] Irena Peeva *Graded Syzygies*, Springer-Verlag, 1, 2011

[7] Roozbeh Hazrat *Graded Rings and Graded Grothendieck Groups*, `https://arxiv.org/abs/1405.5071v4`, Consulted juni 2021

[8] Irena Swanson *Homological Algebra*, `https://www.math.purdue.edu/~iswanso/homologicalalgebra.pdf`, Consulted juni 2021

[9] Jürgen Herzog, Takayuki Hibi *Monomial Ideals*, Springer-Verlag, 1, 2011

[10] Robin Hartshorne *Algebraic Geometry*, Springer-Verlag, 1, 1977

[11] Viviana Ene, Jürgen Herzog *Gröbner Bases in Commutative Algebra*, American Mathematical Society, 1, 2011