The Abdus Salam International Centre for Theoretical Physics
Trieste, Italy

Postgraduate Diploma Dissertation

Title

Syzygies

Author

Yairon Cid Ruiz

Supervisor

Prof. Lothar Göttsche

- August, 2016 -

To mom and dad,
of course.

Algebra is the offer made by the devil to the mathematician. The devil says: "I will give you this powerful machine, it will answer any question you like. All you need to do is give me your soul: give up geometry and you will have this marvellous machine".

Michael Atiyah

Acknowledgements

I am very grateful to my supervisor *Lothar Göttsche* for his invaluable support, guidance and encouragement throughout the preparation of this project and during all this year in ICTP. Very special thanks go to *Tarig Abdelgadir* for his advices, the long and helpful conversations, and all the interesting things I was able to learn in his reading courses. I feel deep gratitude in my heart to all the professors of the Mathematics Section of ICTP for showing me a whole new world and for helping me to better appreciate the beauty of mathematics.

Finally, I thank the people responsible of my well-being. I thank my beloved *Elizabeth* and my family for their love, patience and support during this stormy year.

Contents

Introduction

The word *"syzygy"* comes to mathematics from a rather interesting route. It comes from the Greek *"syzygos"* and meaning yoked together. It was widely used in astronomy in the $18th$ century to describe three planets in a line (and thus yoked by some mysterious force). *Cayley* and *Sylvester* were the first to use it in mathematics.

The current usage inside mathematics is as follows. If M is a module and F a free module with a surjective map $\varphi : F \to M$, then the kernel $K = Ker(\varphi)$ is called the $0th$ syzygy of M. The three modules K, F and M lie in a *"line"*

$$0 \to K \to F \xrightarrow{\varphi} M \to 0,$$

and one can view this as K being yoked to M.

In general we can continue this process of finding the *"syzygies"* and construct a *"free resolution"* for a module. For example, let $R = \mathbb{K}[x, y]$ and $M = R/\mathfrak{m}$ where $\mathfrak{m} = (x, y)$. A generator for M is given by $\overline{1}$ and we find

$$0 \to \mathfrak{m} \to R \xrightarrow{\pi} M \to 0.$$

The module of syzygies is $\mathfrak{m}$, which is generated by x and y. These elements are not independent, since they satisfy the non-trivial relation $(-y)x + xy = 0$. Resolving again for $\mathfrak{m}$ we get

$$0 \to R \xrightarrow{\begin{pmatrix} -y \\ x \end{pmatrix}} R^2 \xrightarrow{\begin{pmatrix} x & y \end{pmatrix}} \mathfrak{m} \to 0.$$

Finally gluing together these two exact sequences we find a free resolution for M

$$0 \to R \xrightarrow{\begin{pmatrix} -y \\ x \end{pmatrix}} R^2 \xrightarrow{\begin{pmatrix} x & y \end{pmatrix}} R \xrightarrow{\pi} M \to 0.$$

It turns out that the finiteness of the process in the previous example is not casual and every finitely generated module M (not necessarily graded) over a polynomial ring $R = \mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is a field, has a free resolution of length at most n.

As in many places of mathematics *Hilbert* was the first person looking at this *"type"* of problems; and in his famous "Syzygy Theorem", published in 1890, he states that every finitely generated *graded module* $M = \bigoplus M_i$ over the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ has a free resolution of length at most n.

In this report we shall study several results and theorems related with syzygies, just like previous one. The outline is as follows

- In *Chapter 1*, we summarize the basic concepts and tools coming from *Commutative Algebra* and *Homological Algebra* that we will need throughout this work.
- In *Chapter 2*, we shall present three important and beautiful theorems
  - The *Hilbert's Syzygy Theorem* which could be seen as the starting point of this now rich theory.
  - The *Quillen-Suslin Theorem* that answered positively the *Serre's conjecture*: *"every finitely generated projective module over* $\mathbb{K}[x_1, \ldots, x_n]$ *is free"*.
  - The *Auslander-Buchsbaum formula* which is a surprising relation between the *depth* and the *projective dimension* of modules over a local ring.
- In *Chapter 3*, we accomplish two objectives at the same time
  - We give answer to a question posed by *David Cox* in the paper [1].
  - Along the path of answering this question, we present a short introduction to the theory in the case of *graded rings*.

One of the main goals of this report is giving a *"fair"* introduction to the *"theory of syzygies"* and make it an accessible read for any graduate student without previous knowledge on the subject (like myself).

Chapter 1

Basic concepts

In this chapter we will introduce some basic facts with the hope of making a self-contained work, but we will only prove a statement, if proving it is as easy as quoting it. The main reference for the topics related with *Commutative Algebra* will be the classic book by *Atiyah* and *MacDonald* [10] and for the use of some tools coming from *Homological Algebra* we will follow the book by *Rotman* [19].

Throughout all this exposition the word **"ring"** shall mean a **commutative ring with an identity element**, hence we will differ mainly in this aspect from the text [19], e.g. for us will not exist "left R-modules" or "right R-modules", for us only matters the term "R-modules".

1.1 Modules and Resolutions

Definition 1.1. *Let R be a ring (commutative with identity element, as always) then an R-module is an abelian group M on which R acts linearly by a mapping $R \times M \to M$ that satisfies the axioms*

$$a(x + y) = ax + ay$$
$$(a + b)x = ax + bx$$
$$(ab)x = a(bx)$$
$$1x = x$$

for all $a, b \in R$ and $x, y \in M$.

One of the most natural ways of constructing an *R-module* is taking several copies of R, more formally by defining the **free module** which is an *R-module* of the form $\bigoplus_{i\in I} M_i$, where each $M_i \cong R$. It turns out that we can always give a good description of an arbitrary module using these free modules.

Construction 1.2. *Let M be an arbitrary module and choose a set of generators $\{x_i\}_{i\in I}$ of this module, then we define the free module $F_0 = \bigoplus_{i\in I} Rx_i$; hence we can obtain an exact sequence $0 \to K_0 \to F_0 \xrightarrow{d_0} M \to 0$. We may repeat this operation for K_0 to obtain the exact sequence $0 \to K_1 \to F_1 \to K_0 \to 0$, and iterating successively we get $0 \to K_n \to F_n \to K_{n-1} \to 0$ where each F_n is a free module.*

Gluing all these short exact sequences we obtain the long exact sequence

$$\dots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0$$

which is called a ***free resolution*** *of M. The intermediate modules $K_n = Ker(d_n) = Im(d_{n+1})$ are called the* ***syzygies*** *of M.*

After this construction several questions come to our minds because certainly this construction is not unique neither the syzygies of M. To solve this problem of uniqueness we will use some techniques from *Homological Algebra*, the path that we have chosen to achieve this goal is different from the one taken in the book by *Eisenbud* [3]. We have decided to work in the general settlement of a commutative ring with a unit element without assuming extra properties, although later on we will use this marvelous text [3] for stronger results that can only be achieved making additional assumptions. The main ingredient for this generalization will be that of a **projective module**.

Definition 1.3. *A* ***projective module*** *P is a module that given any surjective R-linear map $\beta : B \to C$ and any R-linear map $\alpha : P \to C$, there exists an R-linear map $\phi : P \to B$ such that $\alpha = \beta \circ \phi$, i.e makes the following diagram*

$$\begin{tikzcd}
 & P \arrow[d, "\alpha"] \arrow[dl, dashed, "\phi"'] & \\
B \arrow[r, "\beta"'] & C \arrow[r] & 0
\end{tikzcd}$$

commute.

This type of module will give us the fundamental tool for describing modules in general.

Definition 1.4. *A **projective resolution** of a module M is an exact sequence*

$$\ldots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0$$

in which each P_n is a projective module.

The study of projective modules generalizes that of free modules because every free module is a projective module, and we will see that by doing this we have identified the key property that will abstract and simplify our work.

Theorem 1.5. *Every free module is a projective module.*

Proof. (See [19], *page 61*) ■

Then we define the term *syzygy* for any projective resolution of a module and we will see how this theory is independent of the chosen projective resolution.

Definition 1.6. *Let $\ldots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0$ be a projective resolution of M. For $n \geq 0$ we denote $K_n = Ker(d_n)$ as the nth **syzygy** of M.*

1.2 Two important types of rings

In this short section we shall introduce the basic definitions of modules over a **local ring** and over a **graded polynomial ring**. One of the biggest advantages of working over these two types of rings is the possibility of applying *Nakayama's lemma* in a pleasant way.

Definition 1.7. *A ring R with exactly one maximal ideal $\mathfrak{m}$ is called a **local ring** and will be denoted by $(R, \mathfrak{m})$ (or $(R, \mathfrak{m}, \mathbb{K})$ if we want to stress the residue field $\mathbb{K} \cong R/\mathfrak{m}$).*

Definition 1.8. *For the polynomial ring $R = \mathbb{K}[x_1, \ldots, x_n]$ we will use the standard grading with $deg(x_1^{c_1} x_2^{c_2} \ldots x_n^{c_n}) = c_1 + c_2 + \ldots + c_n$. The $\mathbb{K}$-vector space generated by the monomials of degree i is denoted by R_i. The graded polynomial ring R has a direct sum decomposition $R = \bigoplus_{i \in \mathbb{N}} R_i$ as k-vector spaces with $R_i R_j \subseteq R_{i+j}$ for all $i, j \in \mathbb{N}$.*

We say that M is a graded R-module, if it has a direct sum decomposition $M = \bigoplus_{i\in\mathbb{Z}} M_i$ as $\mathbb{K}$-vector spaces and $R_i M_j \subseteq M_{i+j}$ for all $i, j \in \mathbb{Z}$. Of particular interest for us is the free graded module $R(-p)$ defined by $R(-p)_i = R_{i-p}$, i.e., for $p \geq 0$ the module $R(-p)$ is shifted p degrees with $R(-p)_p = R_0 = \mathbb{K}$.

Lemma 1.9. *(Nakayama's lemma for local rings) Let $(R, \mathfrak{m}, \mathbb{K})$ be a local ring and M be a finitely generated R-module.*

(i) If $\mathfrak{m}M \cong M$, then $M = 0$.

(ii) If N is a submodule of M and $M = \mathfrak{m}M + N$, then $M = N$.

Proof. (i) Suppose that $\{x_1, \dots, x_r\}$ is a minimal system of generators for M. Using the hypothesis $\mathfrak{m}M \cong M$ we have $x_1 = \alpha_1 x_1 + \ldots + \alpha_r x_r$ for some $\alpha_1, \dots, \alpha_r \in \mathfrak{m}$. Since $1 - \alpha_1$ is invertible we get the contradiction $x_1 = (1 - \alpha_1)^{-1}(\alpha_2 x_2 + \ldots + \alpha_r x_r)$.

(ii) Apply (i) to the module M/N.

■

Lemma 1.10. *(Nakayama's lemma for graded rings) Let $R = \mathbb{K}[x_1, \dots, x_n]$ be a graded polynomial ring, M be a graded finitely generated R-module, and $I \subset R$ be a homogeneous proper ideal.*

(i) If $IM = M$, then $M = 0$.

(ii) If N is a submodule of M and $M = IM + N$, then $M = N$.

Proof. (i) Since M is finitely generated there exists a smallest integer $j \in \mathbb{Z}$ with $M_j \neq 0$. Because I is a proper ideal all homogeneous elements in I has positive degree and this implies the contradiction $M_j \not\subset IM$.

(ii) Apply (i) to the module M/N. ■

With the use of *Nakayama's lemma* we can define the concept of **minimal number of generators** for finitely generated modules over a local ring or over a graded polynomial ring, i.e., all minimal systems of generators have the same number of elements.

Lemma 1.11. *Let $(R, \mathfrak{m}, \mathbb{K})$ be a local ring ($R = \mathbb{K}[x_1, \dots, x_n]$ be the graded polynomial ring with $\mathfrak{m} = (x_1, \dots, x_n)$ the irrelevant ideal). Let M be a finitely generated R-module,* *then the minimal number of generators is equal to*

$$\mu(M) = dim_{\mathbb{K}}(M \otimes_R \mathbb{K}).$$

Proof. We shall prove that $\{v_1, \ldots, v_r\}$ is a minimal system of generators for M if and only if the set of residue classes $\{\overline{v_1}, \ldots, \overline{v_r}\}$ is a basis for the $\mathbb{K}$-vector space $M \otimes_R \mathbb{K}$.

If $\overline{v_1}, \ldots, \overline{v_r} \in M/\mathfrak{m}M$ are a $\mathbb{K}$-basis of $M \otimes_R \mathbb{K}$ then we have that $M = Rv_1 + \ldots + Rv_r + \mathfrak{m}M$. Then *Nakayama's lemma* ((ii) in *Lemma* 1.9 or (ii) in *Lemma* 1.10) implies that $M = Rv_1 + \ldots + Rv_r$.

If $v_1, \ldots, v_r$ is a minimal system of generators for M, then the residue classes $\overline{v_1}, \ldots, \overline{v_r} \in M/\mathfrak{m}M (\cong M \otimes_R \mathbb{K})$ clearly are a generating set for $M \otimes_R \mathbb{K}$, but we claim they also conform $\mathbb{K}$-basis. By contradiction suppose there is a linear dependence between $\overline{v_1}, \ldots, \overline{v_r}$, therefore there exists a strictly smaller subset $\{\overline{v_{i_1}}, \ldots, \overline{v_{i_s}}\} \subsetneq \{\overline{v_1}, \ldots, \overline{v_r}\}$, such that $\{\overline{v_{i_1}}, \ldots, \overline{v_{i_s}}\}$ is a $\mathbb{K}$-basis for $M \otimes_R \mathbb{K}$. By the previous implication we get the contradiction that $\{v_{i_1}, \ldots, v_{i_s}\}$ is a generating set for M.

■

Theorem 1.12. *Let $(R, \mathfrak{m}, \mathbb{K})$ be a local ring ($R = \mathbb{K}[x_1, \ldots, x_n]$ be the graded polynomial ring with $\mathfrak{m} = (x_1, \ldots, x_n)$ the irrelevant ideal). Suppose $F \xrightarrow{\psi} G \xrightarrow{\varphi} H \to 0$ is an exact sequence of R-modules, with G a free module. Then the elementary vectors of G are mapped into a minimal system of generators of H if and only if $Im(\psi) \subseteq \mathfrak{m}G$.*

Proof. From the initial exact sequence we can get the exact sequence

$$F/\mathfrak{m}F \xrightarrow{\overline{\psi}} G/\mathfrak{m}G \xrightarrow{\overline{\varphi}} H/\mathfrak{m}H \to 0.$$

The map $\overline{\varphi}$ is an isomorphism if and only if $\overline{\varphi}$ maps the elementary vectors of $G/\mathfrak{m}G$ into a basis of the $\mathbb{K}$-vector space $H/\mathfrak{m}H$ ($\cong H \otimes_R \mathbb{K}$), by *Nakayama's lemma* this happens if and only if φ maps the elementary vectors of G into a minimal system of generators of H.

The map $\overline{\varphi}$ is an isomorphism if and only if $Im(\overline{\psi}) = 0$, that is $Im(\psi) \subset \mathfrak{m}G$. ■

1.3 Homology and derived functors

Definition 1.13. *A **complex** (or **chain complex**) $\mathcal{C}$ is a sequence of modules and maps*

$$\mathcal{C}: \quad \ldots \to A_{n+1} \xrightarrow{d_{n+1}} A_n \xrightarrow{d_n} A_{n-1} \to \ldots, \quad n \in \mathbb{Z}$$

with $d_n d_{n+1} = 0$ for all $n \in \mathbb{Z}$.

The condition $d_n d_{n+1} = 0$ is equivalent to $Im(d_{n+1}) \subset Ker(d_n)$ and therefore every exact sequence could be seen as a chain complex. Here our main construction will be a functor $H_n : \mathcal{COMP} \to \mathcal{M}_R$ from the category of chain complexes [14] into the category R-modules.

Definition 1.14. *If $\mathcal{C}$ is a complex, its **nth homology module** is*

$$H_n(\mathcal{C}) = Ker(d_n)/Im(d_{n+1}).$$

Given a projective resolution of the module M we construct the **deleted complex** by suppressing M and obtaining the complex

$$\ldots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to 0$$

and by doing this we do not loose any information since $M = Coker(d_1) = P_0/Im(d_1) = P_0/Ker(d_0)$. Then we will apply certain functors to this complex and by computing the homology of the resulting complex we will obtain the derived functors Tor and Ext. That will be our two fundamental tools.

Definition 1.15. *Given a module M with its respective deleted complex $\mathcal{C} : \ldots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to 0$ coming from a projective resolution. For any module N we apply the functor $\otimes_R N$*

$$\mathcal{D} : \ldots \xrightarrow{d_{n+1} \otimes_R 1} P_n \otimes_R N \xrightarrow{d_n \otimes_R 1} \ldots \xrightarrow{d_2 \otimes_R 1} P_1 \otimes_R N \xrightarrow{d_1 \otimes_R 1} P_0 \otimes_R N \to 0$$

and we define $\mathbf{Tor_n^R(M, N) = H_n(\mathcal{D}) = Ker(d_n \otimes_R 1)/Im(d_{n+1} \otimes_R 1)}$.

Definition 1.16. *Given a module M with its respective deleted complex $\mathcal{C} : \ldots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to 0$ coming from a projective resolution. For any module N we* *apply the functor* $Hom_R(\ \ ,N)$

$$\mathcal{E}: 0 \to Hom_R(P_0,N) \xrightarrow{d_1^*} Hom_R(P_1,N) \xrightarrow{d_2^*} \dots \xrightarrow{d_n^*} Hom_R(P_n,N) \xrightarrow{d_{n+1}^*} \dots$$

and we define $\mathbf{Ext^n_R(M,N) = H_{-n}(\mathcal{E}) = Ker(d^*_{n+1})/Im(d^*_n)}$.

Now surprisingly enough we have that both functors are independent of the projective resolution chosen which is a result coming from the property of projective modules (see [19], *Theorem 6.9 (Comparison Theorem)*).

Theorem 1.17. *Let* M *and* N *be* R*-modules then*

(1) $Tor_n^R(M,N) = Tor_n^R(N,M)$.

(2) $Tor_0^R(M,N) = M \otimes_R N$.

(3) $Tor_n^R(M,N)$ *does not depend on the projective resolution chosen.*

Proof. (See [19], *Chapter 8*). ■

Theorem 1.18. *Let* M *and* N *be* R*-modules then*

(1) $Ext_R^0(M,N) = Hom_R(M,N)$.

(2) $Ext_R^n(M,N)$ *does not depend on the projective resolution chosen.*

(3) For all n *we have* $Ext_R^n(\bigoplus M_k, N) = \prod Ext_R^n(M_k,N)$.

Proof. (See [19], *Chapter 7*). ■

A fundamental result that we will use several times is the following *"long exact sequence"* argument for the functors *Tor* and *Ext*.

Theorem 1.19. *Suppose* $0 \to A \to B \to C \to 0$ *is a short exact sequence of* R*-modules. Then we have the long exact sequence*

$$\begin{array}{l} \dots \longrightarrow Tor_n^R(A,N) \longrightarrow Tor_n^R(B,N) \longrightarrow Tor_n^R(C,N) \longrightarrow \dots \\ \dots \longrightarrow Tor_1^R(A,N) \longrightarrow Tor_1^R(B,N) \longrightarrow Tor_1^R(C,N) \longrightarrow \\ \longrightarrow Tor_0^R(A,N) \longrightarrow Tor_0^R(B,N) \longrightarrow Tor_0^R(C,N) \longrightarrow 0, \end{array}$$

the long exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Ext^0_R(C,N) & \longrightarrow & Ext^0_R(B,N) & \longrightarrow & Ext^0_R(A,N) & \longrightarrow & \\ & \longrightarrow & Ext^1_R(C,N) & \longrightarrow & Ext^1_R(B,N) & \longrightarrow & Ext^1_R(A,N) & \longrightarrow & \dots \\ \dots & \longrightarrow & Ext^n_R(C,N) & \longrightarrow & Ext^n_R(B,N) & \longrightarrow & Ext^n_R(A,N) & \longrightarrow & \dots, \end{array}$$

and also the exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Ext^0_R(N,A) & \longrightarrow & Ext^0_R(N,B) & \longrightarrow & Ext^0_R(N,C) & \longrightarrow & \\ & \longrightarrow & Ext^1_R(N,A) & \longrightarrow & Ext^1_R(N,B) & \longrightarrow & Ext^1_R(N,C) & \longrightarrow & \dots \\ \dots & \longrightarrow & Ext^n_R(N,A) & \longrightarrow & Ext^n_R(N,B) & \longrightarrow & Ext^n_R(N,C) & \longrightarrow & \dots . \end{array}$$

Proof. (See [19], *Theorem 6.21*, *Theorem 6.26* and *Theorem 6.27*). ■

Using the concept of **split exact sequence** (for a good explanation on this, see [13] *page 131*) there is a complete characterization of projective modules.

Theorem 1.20. *A module M is projective if and only if every short exact sequence $0 \to A \to B \to M \to 0$ splits.*

Proof. ($\Rightarrow$) First suppose M is projective then over an exact sequence $0 \to A \to B \to M \to 0$ we can construct the following diagram

$$\begin{tikzcd} & & & M \arrow[dl, dashed, "\phi"'] \arrow[d, "id"] & \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r] & M \arrow[r] & 0, \end{tikzcd}$$

where the induced map ϕ makes the sequence split.

($\Leftarrow$) For the reverse we only need that the sequence $0 \to K_0 \xrightarrow{i} F_0 \xrightarrow{d_0} M \to 0$ splits then we get $F_0 \cong M \oplus K_0$. We know that F_0 is projective and now M can be completely identified inside F_0 by a projection and an inclusion map. Consider the diagram

$$\begin{tikzcd}
F_0 \arrow[r, shift left, "\pi_M"] \arrow[d, "\omega"'] & M \arrow[l, shift left, "i"] \arrow[dl, dashed, "\phi"'] \arrow[d, "\alpha"] & \\
B \arrow[r, "\beta"] & C \arrow[r] & 0,
\end{tikzcd}$$

then we see that M satisfy diagram of *Definition* 1.3 with $\phi = \omega \circ i$, and finally M is a projective module.

■

Corollary 1.21. *A module M is projective if and only if M is a direct summand of a free R-module. More specifically, M is projective if and only if $F_0 \cong M \oplus K_0$.*

Proof. Look at the previous proof and see that all is around the exact sequence $0 \to K_0 \xrightarrow{i} F_0 \xrightarrow{d_0} M \to 0$.

■

Example 1.22. *We have $\mathbb{Z}/15\mathbb{Z} = \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, then both $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are projective $\mathbb{Z}/15\mathbb{Z}$-modules, but neither of them are free because they have less than 15 elements.*

And we end this section with the following theorem that is a stone where much of our work rests. We have tried to give our own proof by using explicitly the syzygies of the construction 1.2, which seems reasonable given the title of this work.

Theorem 1.23. *Let M be a module if $Ext^1(M, N) = 0$ for every module N, then M is a projective module.*

Proof. We compute the $0th$ syzygy of M

$$0 \to K_0 \xrightarrow{i} F_0 \xrightarrow{d_0} M \to 0, \tag{1.1}$$

then we glue it with 1.2 to get the following commutative diagram

$$\begin{tikzcd}
\dots \arrow[r, "d_{n+1}"] & F_n \arrow[r, "d_n"] & \dots \arrow[r, "d_3"] & F_2 \arrow[r, "d_2"] & F_1 \arrow[r, "d_1"] \arrow[d, "\overline{d_1}"] & F_0 \arrow[r, "d_0"] \arrow[d, "id"] & M \arrow[r] \arrow[d, "id"] & 0 \\
& & & 0 \arrow[r] & K_0 \arrow[r, "i"] & F_0 \arrow[r, "d_0"] & M \arrow[r] & 0
\end{tikzcd}$$

where $\overline{d_1}$ is the restriction of d_1 to $Im(d_1) = K_0$ and i denotes the inclusion map.

By hypothesis we have $0 = Ext^1(M, K_0) = Ker(d_2^*)/Im(d_1^*)$, that implies $Ker(d_2^*) \cong Im(d_1^*)$. Hence we will try to relate this property on the first row of the previous commutative diagram to a property on the second row. We will obtain that 1.1 is a split exact sequence.

First lets translate the module $Ker(d_2^*)$ in terms of 1.1:

$$\begin{aligned} Ker(d_2^*) &= \{f \in \; Hom(F_1, K_0) \mid (f \circ d_2)(x) = 0 \;\; \forall x \in F_2\} \\ &= \{f \in \; Hom(F_1, K_0) \mid f\mid_{Im(d_2)} = 0\} \\ &= \{f \in \; Hom(F_1, K_0) \mid f\mid_{K_1} = 0\}, \end{aligned}$$

the quotient $K_0 = F_1/K_1$ induces an isomorphism $Ker(d_2^*) \cong Hom(K_0, K_0)$[1] given by the map

$$\Phi : Hom(K_0, K_0) \to Ker(d_2^*), \text{ where } \Phi(\varphi)(x) = \varphi([x]).$$

This map is well-defined from the *R-linearity* of $\varphi(-)$ and $[-]$, is an *R-linear* map because $\Phi(\alpha*\varphi+\beta*\psi)(x) = (\alpha*\varphi+\beta*\psi)([x]) = \alpha*\varphi([x])+\beta*\psi([x]) = \alpha*\Phi(\varphi)(x)+\beta*\Phi(\psi)(x)$. It is bijective because any $f \in Hom(F_1, K_0)$ that vanishes on K_1 is constant on every coset of F_1/K_1.

From the previous commutative diagram we take the following square

$$\begin{tikzcd} F_1 \arrow[r, "d_1"] \arrow[d, "\overline{d_1}"] & F_0 \arrow[d, "id"] \\ K_0 \arrow[r, "i"] & F_0 \end{tikzcd}$$

and applying the $Hom(\;, K_0)$ functor we get the commutative diagram

$$\begin{tikzcd} Hom(F_1, K_0) & Hom(F_0, K_0) \arrow[l, "d_1^*"'] \\ Hom(K_0, K_0) \arrow[u, "\overline{d_1}^*"] & Hom(F_0, K_0) \arrow[l, "i^*"] \arrow[u, "id"'] \end{tikzcd}.$$

[1] A good way of imagine this isomorphism is like when we compute the coordinate ring of an affine variety.

Now the isomorphism $Hom(K_0, K_0) \cong Ker(d_2^*) \cong Im(d_1^* : Hom(F_0, K_0) \to Hom(F_1, K_0))$ gives the surjection $Hom(F_0, K_0) \to Hom(K_0, K_0) \to 0$, which we identify in the previous diagram to obtain

$$\begin{tikzcd} 0 & Hom(K_0, K_0) \arrow[l] & Hom(F_0, K_0) \arrow[l] \\ & Hom(K_0, K_0) \arrow[u, "\varphi"] & Hom(F_0, K_0), \arrow[l, "i^*"'] \arrow[u, "id"'] \end{tikzcd}$$

where φ is an isomorphism, because the fact that $\overline{d_1}$ is surjective implies that $\overline{d_1}^*$ is injective. From this follows that necessarily the map $i^* : Hom(F_0, K_0) \to Hom(K_0, K_0)$ is surjective and there exists $g \in Hom(F_0, K_0)$ such that $i^*(g) = id_{K_0}$, that is $g \circ i = id_{K_0}$. Therefore we say that the exact sequence 1.1 splits and following the proof of the previous *Theorem* 1.20 we get that M is projective.

■

Remark 1.24. *For a short proof of the previous theorem, see* [19] *page 199, simply apply Theorem* 1.19 *to the short exact sequence* 1.1 *and obtain* $Hom(F_0, K_0) \xrightarrow{i^*} Hom(K_0, K_0) \to Ext^1(M, K_0) = 0$.

1.4 Regular sequences and the Koszul complex

In this section we will discuss the concept of *regular sequence* and its tight relation with the *Koszul complex*. Our exposition will be *"mixed"* between the books [9], [11] and [6]. From [9] we will use *Section 4 in Chapter 21*, from [11] the *Section 16* and from [6] the *Section 1.6*.

Definition 1.25. *Let R be a ring and M an R-module. An element $x \in R$ is regular in M if $xm \neq 0$ for any nonzero $m \in M$. A sequence of elements $x_1, \ldots, x_n$ in R is called **M-regular** (or just **M-sequence**) if the two following conditions hold*

(i) $M/(x_1, \ldots, x_n)M \neq 0$

(ii) x_1 *is regular in* M*, and for any* $i > 1$*,* x_i *is regular in* $M/(x_1, \ldots, x_{i-1})M$.

*The sequence $(x_1, \ldots, x_n)$ is called a **weak M-sequence** if only the condition (ii) is required to be satisfied.*

Theorem 1.26. *If $x_1, \ldots, x_n$ is an M-sequence then then so is $x_1^{k_1}, \ldots, x_n^{k_n}$ for any positive integers $k_1, \ldots, k_n$.*

Proof. See [11], *Theorem 16.1.* ■

We start with a small discussion on the simplest type of Koszul complex. For any $x \in R$ we can construct

$$K(x): \quad 0 \to R \xrightarrow{x} R \to 0,$$

and here we see how special are the homologies, with $H_1(K(x)) = Ann(x)$ and $H_0(K(x)) = R/xR$.

More generally, for elements $x_1, \ldots, x_n \in R$ we define the **Koszul complex** $K(\mathbf{x}) = K(x_1, \ldots, x_n)$ as follows. For $\mathbf{x} = (x_1, \ldots, x_n)$ the modules of the complex $K(\mathbf{x})$ will be

$$\begin{aligned}
K_0(\mathbf{x}) &= R; \\
K_1(\mathbf{x}) &= \text{ free module } E \text{ with basis } \{e_1, \ldots, e_n\}; \\
&\vdots \\
K_p(\mathbf{x}) &= \text{ free module } \textstyle\bigwedge^p E \text{ with basis } e_{i_1} \wedge \ldots \wedge e_{i_p}, i_1 < \ldots < i_p; \\
&\vdots \\
K_n(\mathbf{x}) &= \text{ free module } \textstyle\bigwedge^n E \text{ of rank 1 with basis } e_1 \wedge \ldots \wedge e_n.
\end{aligned}$$

The **boundary map** is defined by $d(e_i) = x_i$ and in general

$$d : K_p(\mathbf{x}) \to K_{p-1}(\mathbf{x})$$

by

$$d(e_{i_1} \wedge \ldots \wedge e_{i_p}) = \sum_{j=1}^{p} (-1)^{j+1} x_{i_j} e_{i_1} \wedge \ldots \wedge \widehat{e_{i_j}} \wedge \ldots \wedge e_{i_p}.$$

A simple verification shows that $d^2 = 0$, then using the previous modules and the boundary map, we define $K(\mathbf{x})$ as

$$K(\mathbf{x}): \quad 0 \to K_n(\mathbf{x}) \to \ldots \to K_1(\mathbf{x}) \to K_0(\mathbf{x}) \to 0.$$

In the previous definition we see that the zero homology is $H_0(K(\mathbf{x})) = R/I$, where

$I = (x_1, \ldots, x_n)$. Then we define the **augmented Koszul complex** as

$$0 \to K_n(\mathbf{x}) \to \ldots \to K_1(\mathbf{x}) \to K_0(\mathbf{x}) \to R/I \to 0.$$

The next Lemma gives the *"invariant property"* that we would like for the Koszul complex. Suppose that $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are n-tuples of elements in R. If the ideal $I' = (y_1, \ldots, y_n)$ is contained in the ideal $I = (x_1, \ldots, x_n)$, then we can make

$$y_i = \sum_{j=1}^{n} a_{ij} x_j \quad \text{with} \quad a_{ij} \in R.$$

Let $\{e_1', \ldots, e_n'\}$ be a basis for $K_1(\mathbf{y})$ then we define the R-linear map $f : K_1(\mathbf{y}) \to K_1(\mathbf{x})$ given by

$$f(e_i') = \sum_{j=1}^{n} a_{ij} e_j,$$

that we can extend for any p $(1 \leq p \leq n)$ as

$$f^{\wedge p} : K_p(\mathbf{y}) \to K_p(\mathbf{x}),$$

where $f^{\wedge p} = f \wedge \ldots \wedge f$ (p-times). In particular, we know that $f^{\wedge n}$ is just the multiplication by the determinant of the matrix $A = (a_{ij})^t$ of change of basis.

Lemma 1.27. *With notation as above, the homomorphisms $f^{\wedge p}$ define a morphism of augmented Koszul complexes*

$$\begin{tikzcd}
0 \arrow[r] & K_n(\mathbf{y}) \arrow[r] \arrow[d, "det(A)"] & \ldots \arrow[r] & K_p(\mathbf{y}) \arrow[r] \arrow[d, "f^{\wedge p}"] & \ldots \arrow[r] & K_1(\mathbf{y}) \arrow[r] \arrow[d, "f"] & R \arrow[r] \arrow[d, "id"] & R/I' \arrow[r] \arrow[d, "can"] & 0 \\
0 \arrow[r] & K_n(\mathbf{x}) \arrow[r] & \ldots \arrow[r] & K_p(\mathbf{x}) \arrow[r] & \ldots \arrow[r] & K_1(\mathbf{x}) \arrow[r] & R \arrow[r] & R/I \arrow[r] & 0
\end{tikzcd}$$

and defines an isomorphism if $det(A)$ is a unit in R.

Proof. See [9], *page 853, Lemma 4.2.* ∎

Therefore, if two n-tuples $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ generate the same ideal and the determinant of the linear transformation is a unit, then the two Koszul complexes are isomorphic. An important and special case is when $(\mathbf{y})$ is a permutation of $(\mathbf{x})$.

Given two complexes

$$K: \qquad \ldots \xrightarrow{e_{i+1}} K_i \xrightarrow{e_i} K_{i-1} \xrightarrow{e_{i-1}} \ldots \xrightarrow{e_1} K_0 \to 0$$

and

$$L: \qquad \ldots \xrightarrow{f_{i+1}} L_i \xrightarrow{f_i} L_{i-1} \xrightarrow{f_{i-1}} \ldots \xrightarrow{f_1} L_0 \to 0,$$

its **tensor product** is defined as the complex

$$K \otimes L: \qquad \ldots \xrightarrow{d_{i+1}} \bigoplus_{j+k=i} (K_j \otimes_R L_k) \xrightarrow{d_i} \bigoplus_{j+k=i-1} (K_j \otimes_R L_k) \xrightarrow{d_{k-1}} \ldots \xrightarrow{d_1} (K_0 \otimes_R L_0) \to 0,$$

with boundary map defined by

$$d_{i+j}(u \otimes_R v) = e_i(u) \otimes_R v + (-1)^i u \otimes_R f_j(v)$$

for any $u \in K_i$ and $v \in L_j$. The change of sign is necessary to make $d_{i+1}d_i = 0$.

Theorem 1.28. *For Koszul complexes there is a natural isomorphism*

$$K(x_1, \ldots, x_n) \cong K(x_1) \otimes \ldots \otimes K(x_n).$$

Proof. Follows from the definitions of tensor product of complexes and Koszul complex. ∎

Now we can extend the notion of Koszul complex for any R-module.

Definition 1.29. *Let M be an R-module, then we define the **Koszul complex of M** by*

$$K(\mathbf{x}; M) = K(x_1, \ldots, x_n; M) = K(x_1, \ldots, x_n) \otimes_R M$$

that looks like

$$K(\mathbf{x}; M): \quad 0 \to K_n(\mathbf{x}) \otimes_R M \to \ldots \to K_1(\mathbf{x}) \otimes_R M \to K_0(\mathbf{x}) \otimes_R M \to 0.$$

Generally we always have the equalities $H_0(K(\mathbf{x}; M)) \cong M/IM$ and $H_n(K(\mathbf{x}); M) \cong \{v \in M \mid x_1 v = \ldots = x_n v = 0\}$.

Given an element $x \in R$ we study what happens what when we tensor an arbitrary complex $C: \ \ldots \xrightarrow{d_{p+1}} C_p \xrightarrow{d_p} \ldots \xrightarrow{d_2} C_1 \xrightarrow{d_1} C_0 \to 0$ with the simple Koszul complex $K(x)$. We can make the exact sequence of complexes

$$0 \to C \to C \otimes K(x) \to (C \otimes K(x))/C \to 0.$$

The Koszul complex $K(x)$ is simply $0 \to R \xrightarrow{x} R \to 0$, then $(C \otimes K(x))_p = (C_p \otimes_R R) \oplus (C_{p-1} \otimes_R R) \cong C_p \oplus C_{p-1}$. Making this identification we can make explicit the previous exact sequence of complexes as

$$\begin{tikzcd}
 & {} \arrow[d] & {} \arrow[d] & {} \arrow[d] & \\
0 \arrow[r] & C_{p+1} \arrow[r, "i"] \arrow[d, "d_{p+1}"] & C_{p+1} \oplus C_p \arrow[r, "\pi_{C_p}"] \arrow[d, "e_{p+1}"] & C_p \arrow[r] \arrow[d, "d_p"] & 0 \\
0 \arrow[r] & C_p \arrow[r, "i"] \arrow[d, "d_p"] & C_p \oplus C_{p-1} \arrow[r, "\pi_{C_{p-1}}"] \arrow[d, "e_p"] & C_{p-1} \arrow[r] \arrow[d, "d_{p-1}"] & 0 \\
0 \arrow[r] & C_{p-1} \arrow[r, "i"] \arrow[d] & C_{p-1} \oplus C_{p-2} \arrow[r, "\pi_{C_{p-2}}"] \arrow[d] & C_{p-2} \arrow[r] \arrow[d] & 0 \\
 & {} & {} & {} &
\end{tikzcd}$$

where the boundary map of the complex $C \otimes K(x)$ is defined by

(i) $e_p(u) = d_p(u)$ for any $u \in C_p$;

(ii) $e_p(v) = d_{p-1}(v) + (-1)^{p-1}xv$ for any $v \in C_{p-1}$.

The corresponding homology long exact sequence is given by

$$\ldots \to H_p(C) \to H_p(C \otimes K(x)) \to H_p((C \otimes K(x))/C) \xrightarrow{\partial} H_{p-1}(C) \to \ldots,$$

by the previous discussions we have $H_p((C \otimes K(x))/C) \cong H_{p-1}(C)$ and from a simple diagram chasing we get $\partial = (-1)^{p-1}x$. Therefore we get the exact sequence

$$\ldots \to H_p(C) \to H_p(C \otimes K(x)) \to H_{p-1}(C) \xrightarrow{(-1)^{p-1}x} H_{p-1}(C) \to \ldots,$$

that can be reordered as

$$\ldots \to H_p(C) \xrightarrow{(-1)^p x} H_p(C) \to H_p(C \otimes K(x)) \to H_{p-1}(C) \to \ldots.$$

Lemma 1.30. *Let $x \in R$ and let C be a complex as above. Then x annihilates $H_p(C \otimes K(x))$ for all $p \geq 0$.*

Proof. For $p = 0$ we have $(C \otimes K(x))_0 \cong C_0$, then $e_1(u) = xu$ for any $u \in C_0$ and follows $xH_0(C \otimes K(x)) = 0$.

For $p \geq 1$, if $u+v \in C_p \oplus C_{p-1}$ is a cycle (i.e. $e_p(u+v) = 0$) with $u \in C_p$ and $v \in C_{p-1}$, then we get $(-1)^p xv = d_p(u)$ and $d_{p-1}(v) = 0$. Thus $e_{p+1}((-1)^p u) = (-1)^{2p} xu + (-1)^p d_p(u) = x(u+v)$, and we get at once $xH_p(C \otimes K(x)) = 0$. ■

We want to apply the previous considerations of the tensor product with $C = K(x_1, \ldots, x_{n-1}; M)$ and $x = x_n$. To abbreviate a little bit, we will use the notation $H_pK(\mathbf{x}; M)$ instead of $H_p(K(\mathbf{x}; M))$, and we are going to call it the **Koszul homology**.

Theorem 1.31. *Let R be a ring, M an R-module and $(x_1, \ldots, x_n)$ an arbitrary sequence then*

(i) There is an exact sequence

$$\ldots \to H_pK(x_1, \ldots, x_{n-1}; M) \xrightarrow{(-1)^p x} H_pK(x_1, \ldots, x_{n-1}; M) \to H_pK(x_1, \ldots, x_n; M) \to$$
$$\to H_{p-1}K(x_1, \ldots, x_{n-1}; M) \xrightarrow{(-1)^{p-1} x} H_{p-1}K(x_1, \ldots, x_{n-1}; M) \to H_{p-1}K(x_1, \ldots, x_n; M) \to \ldots;$$

(ii) Every element of $I = (x_1, \ldots, x_n)$ annihilates $H_pK(x_1, \ldots, x_n; M)$ for all $p \geq 0$;

(iii) If $I = R$, then $H_pK(x_1, \ldots, x_n; M) = 0$ for all $p \geq 0$.

Proof. These are consequences from *Lemma* 1.30 and *Theorem* 1.28. ■

For an R-module M and a sequence $\mathbf{x} = (x_1, \ldots, x_n)$ we can define the **augmented Koszul of M with respect to $\mathbf{x}$** as

$$0 \to K_n(\mathbf{x}; M) \to \ldots \to K_p(\mathbf{x}; M) \to \ldots \to K_1(\mathbf{x}; M) \to K_0(\mathbf{x}; M) \to M/IM \to 0,$$

and after some identifications it has the form

$$0 \to M \to \ldots \to M^{\binom{n}{p}} \to \ldots \to M^n \to M \to M/IM \to 0.$$

Theorem 1.32. *Let M be an R-module.*

(i) Let $\mathbf{x} = (x_1, \dots, x_n)$ *be a regular sequence for* M*. Then* $H_pK(\mathbf{x}; M) = 0$ *for* $p > 0$ *(of course,* $H_0K(\mathbf{x}; M) = M/IM$*), i.e., the augmented Koszul complex is exact.*

(ii) Conversely, suppose R *is a local ring (or a graded polynomial ring), and* $\mathbf{x} = (x_1, \dots, x_n)$ *inside the maximal ideal (or* $\mathbf{x} = (x_1, \dots, x_n)$ *inside the irrelevant ideal of the polynomial ring). Suppose* M *is finitely generated over* R*, and* $H_1K(\mathbf{x}; M) = 0$*. Then* $(x_1, \dots, x_n)$ *is an* M*-regular sequence.*

Proof. *(i)* We proceed making induction on n. For $n = 1$ is clear, because as previously seen $H_1K(x; M) = \{m \in M \mid xm = 0\} = 0$ when $x \in R$ is regular on M. So we assume $n > 1$. The case $p > 1$ comes directly from the piece of exact sequence $H_pK(x_1, \dots, x_{n-1}; M) \to H_pK(x_1, \dots, x_n; M) \to H_{p-1}K(x_1, \dots, x_{n-1}; M)$, which from the inductive hypothesis turns into $0 \to H_pK(x_1, \dots, x_n; M) \to 0$. For $p = 1$, we take the tail of the sequence of *Theorem* 1.31 and the isomorphism $H_0K(x_1, \dots, x_{n-1}; M) \cong M/(x_1, \dots, x_{n-1})M$ to get the exact sequence

$$H_1K(x_1, \dots, x_{n-1}; M) \to H_1K(x_1, \dots, x_n; M) \to M/(x_1, \dots, x_{n-1})M \xrightarrow{x_n} M/(x_1, \dots, x_{n-1})M.$$

The multiplication by x_n is an injective map because x_n is regular on $M/(x_1, \dots, x_{n-1})M$. From the inductive hypothesis $H_1K(x_1, \dots, x_{n-1}; M) = 0$, then joining this two facts we get $H_1K(x_1, \dots, x_n; M) = 0$.

(ii) Inductively we are going to prove that $H_1K(x_1, \dots, x_j; M) = 0$ for $j = 1, \dots, n$. Initially we have $H_1K(x_1, \dots, x_n; M) = 0$. From *Theorem* 1.31 we have the exact sequence

$$H_1K(x_1, \dots, x_{j-1}; M) \xrightarrow{-x_j} H_1K(x_1, \dots, x_{j-1}; M) \to H_1K(x_1, \dots, x_j; M),$$

so by the inductive hypothesis $H_1K(x_1, \dots, x_j; M) = 0$ and the multiplication by $-x_j$ is a surjective map. Then *Nakayama's lemma* (*Lemma* 1.9 or *Lemma* 1.10) gives that necessarily $H_1K(x_1, \dots, x_{j-1}; M) = 0$.

So $H_1K(x_1, \dots, x_j; M) = 0$ for $j = 1, \dots, n$, and from

$$0 = H_1K(x_1, \dots, x_j; M) \to M/(x_1, \dots, x_{j-1})M \xrightarrow{x_j} M/(x_1, \dots, x_{j-1})M$$

we have that the multiplication by x_j is injective, i.e., x_j is regular on $M/(x_1, \dots, x_{j-1})M$. To finalize, $M/IM \neq 0$ from *Nakayama's lemma*. ■

The previous theorem gives a complete characterization of M-regular sequences in the case of R is a local ring or a graded polynomial ring, and can be achieved with only checking the simple condition $H_1K(\mathbf{x}; M) = 0$. Also we can get important results for regular sequences by using the Koszul complex, for example from *Lemma* 1.27 we know that any permutation of a regular sequence is also regular in the case of local rings or graded polynomial rings.

An important case where we want to apply the previous theorem is when $M = R$, i.e. $\mathbf{x} = (x_1, \dots, x_n)$ is an R-regular sequence. In this case we know that the augmented Koszul complex is

$$0 \to K_n(\mathbf{x}) \to \dots \to K_1(\mathbf{x}) \to K_0(\mathbf{x}) \to R/I \to 0$$

and looks like

$$0 \to R \to \dots \to R^{\binom{n}{p}} \to \dots \to R^n \to R \to R/I \to 0.$$

Therefore we can regard the augmented Koszul complex as a free resolution of R/I, when the defining sequence of I is regular.

Definition 1.33. *Let M be an R-module and $x_1, \dots, x_n$ be elements in an ideal I. We say that $x_1, \dots, x_n$ is a* ***maximal M-sequence in I*** *if $x_1, \dots, x_n$ is M-regular and $x_1, \dots, x_n, y$ is not M-regular for any $y \in I$.*

When the ring R is a Noetherian any ideal has a maximal M-regular sequence. Surprisingly enough, the length of a maximal M-regular sequence is well-determined by means of the Koszul complex. First we have to prove that the Koszul complex is an exact functor.

Proposition 1.34. *Let R be a ring, $\mathbf{x} = (x_1, \dots, x_n)$ a sequence in R, and $0 \to L \to M \to N \to 0$ an exact sequence of R-modules. Then the induced sequence*

$$0 \to K(\mathbf{x}; L) \to K(\mathbf{x}; M) \to K(\mathbf{x}; N) \to 0$$

is an exact sequence of complexes. Therefore, one has a long exact sequence

$$\dots \to H_pK(\mathbf{x}; L) \to H_pK(\mathbf{x}; M) \to H_pK(\mathbf{x}; N) \to H_{p-1}K(\mathbf{x}; L) \to \dots$$

of homology modules.

Proof. The modules in the Koszul complex are free, hence flat R-modules. ∎

In general the Koszul complex cannot tell you if a sequence is exact or not (in the local and the graded case we saw it is true). But when the ring R is Noetherian, it can give you something even more important.

Theorem 1.35. *Let R be a Noetherian ring, $I = (y_1, \dots, y_n)$ an ideal of R, and M a finitely generated R-module such that $M \neq IM$. If we set*

$$q = \sup\{i \mid H_i K(y_1, \dots, y_n; M) \neq 0\}$$

then any maximal M-sequence in I has length $n - q$.

Proof. Let $x_1, \dots, x_m$ be a maximal M-sequence in I. We will proceed by induction on m. For $m = 0$, we have that I consists of zero divisors of M, so there exists an associated prime ideal $\mathfrak{p} \in Ass_R(M)$ such that $I \subset \mathfrak{p}$ (See *Proposition 1.2.1*, [6]). By definition of associated primes, $\mathfrak{p} = Ann_R(u)$ for some $u \in M$, hence $Iu = 0$. Therefore we get $u \in H_n K(y_1, \dots, y_n; M) = \{v \in M \mid Iv = 0\} \neq 0$ and in this case the assertion $q = n$ holds.

Now suppose $m \geq 1$, then we take $M_1 = M/x_1M$ and the exact sequence

$$0 \to M \xrightarrow{x_1} M \to M_1 \to 0.$$

Applying *Proposition* 1.34 we get the long exact sequence

$$\dots \to H_p K(\mathbf{y}; M) \xrightarrow{\overline{x_1}} H_p K(\mathbf{y}; M) \to H_p K(\mathbf{y}; M_1) \to H_{p-1} K(\mathbf{y}; M) \xrightarrow{\overline{x_1}} H_{p-1} K(\mathbf{y}; M) \to \dots,$$

using *Theorem* 1.31 *(ii)* we get the short exact sequence

$$0 \to H_p K(\mathbf{y}; M) \to H_p K(\mathbf{y}; M_1) \to H_{p-1} K(\mathbf{y}; M) \to 0$$

for every p. Thus $H_{q+1} K(\mathbf{y}; M_1) \neq 0$ and $H_p K(\mathbf{y}; M_1) = 0$ for $p > q + 1$. But $x_2, \dots, x_m$ is a maximal M_1-sequence in I and by the inductive hypothesis $m - 1 = n - (q + 1)$. Therefore $m = n - q$. ∎

This previous theorem has the interesting interpretation, that regular sequences have always length smaller or equal than the number of elements in any generating set of an ideal and that all maximal regular sequences have the same length.

There is a dual version of the Koszul complex from which we can obtain all the same results. In fact, in the book of Eisenbud [3] is taken this approach to the *Koszul cohomology.*

Definition 1.36. *For a sequence* $\mathbf{x} = (x_1, \dots, x_n) \subset R$ *and an* R*-module* M*, the* ***dual Koszul complex*** *is defined by* $Hom_R(K(\mathbf{x}), M)$

$$Hom_R(K(\mathbf{x}), M): \quad 0 \to Hom_R(K_0(\mathbf{x}), M) \xrightarrow{d_1^*} \dots \xrightarrow{d_n^*} Hom_R(K_n(\mathbf{x}), M) \to 0.$$

The ***Koszul cohomology*** *is given by* $H^p(Hom_R(K(\mathbf{x}), M))$ *and we are going to denote it by* $H^pK(\mathbf{x}; M)$*.*

It turns out that the Koszul complex is self-dual. With the isomorphism $Hom_R(K(\mathbf{x}), M) \cong K(\mathbf{x})^* \otimes_R M$, we can reduce the problem to prove that $K(\mathbf{x})$ and $K(\mathbf{x})^*$ are isomorphic. For the dual Koszul complex the basis of each module $K_p(\mathbf{x})^*$ is given by

$$(e_{i_1} \wedge \dots \wedge e_{i_p})^*, \qquad i_1 < \dots < i_p,$$

where $(e_{i_1} \wedge \dots \wedge e_{i_p})^*$ is the function that takes 1 on $e_{i_1} \wedge \dots \wedge e_{i_p}$ and 0 on all the other basis elements.

There is a natural isomorphism $\omega_n : K_n(\mathbf{x}) \to R$ that takes $e_1 \wedge \dots \wedge e_n$ into 1. We can define $\omega_p : K_p(\mathbf{x}) \to K_{n-p}(\mathbf{x})^*$ by setting

$$(\omega_p(u))(v) = \omega_n(u \wedge v) \qquad \text{for } u \in K_p(\mathbf{x}), v \in K_{n-p}(\mathbf{x}).$$

We can consider the following commutative diagram, that in fact induces an isomorphism between the complexes $K(\mathbf{x})$ and $K(\mathbf{x})^*$ (See [6], *pages 47 and 48*).

$$\begin{array}{cccccccccccc}
K(\mathbf{x}): & 0 & \longrightarrow & K_n(\mathbf{x}) & \xrightarrow{d_n} \dots \xrightarrow{d_{p+1}} & K_p(\mathbf{x}) & \xrightarrow{d_p} \dots \xrightarrow{d_1} & K_0(\mathbf{x}) & \longrightarrow & 0 \\
& & & \downarrow{\scriptstyle \omega_n} & & \downarrow{\scriptstyle \omega_p} & & \downarrow{\scriptstyle \omega_0} & & \\
K(\mathbf{x})^*: & 0 & \longrightarrow & K_0(\mathbf{x})^* & \xrightarrow{d_1^*} \dots \xrightarrow{d_{n-p}^*} & K_{n-p}^* & \xrightarrow{d_{n-p+1}^*} \dots \xrightarrow{d_n^*} & K_n(\mathbf{x})^* & \longrightarrow & 0
\end{array}$$

Theorem 1.37. *Let* $\mathbf{x} = (x_1, \dots, x_n)$ *be a sequence in* R*. Then*

(i) The complexes $K(\mathbf{x})$ *and* $K(\mathbf{x})^*$ *are isomorphic (the previous diagram is an isomorphism between them; we say that* $K(\mathbf{x})$ *is self-dual).*

(ii) More generally, for every R*-module* M *the complexes* $K(\mathbf{x}; M) = K(\mathbf{x}) \otimes_R M$ *and*

$Hom_R(K(\mathbf{x}), M)$ are isomorphic.

(iii) $H_pK(\mathbf{x}; M) \cong H^{n-p}K(\mathbf{x}; M)$ *for* $p = 0, \ldots, n$.

Proof. See *Proposition 1.6.10*, [6]. ■

1.5 Dimension and depth

One very basic notion in mathematics is that of dimension and we shall deal with the concept in this section. Here we will call the classic Krull dimension, define the projective dimension and give a meaning to the length of *"maximal regular sequences"*.

Let R be a ring. The supremum of the lengths r, taken over all strictly decreasing chains $p_0 \supsetneq p_1 \supsetneq \ldots \supsetneq p_r$ of prime ideals of R, is called the **Krull dimension**, or simply the **dimension** of R, and denoted by

$$dim\ R.$$

The **codimension** of a prime ideal $\mathfrak{p}$ is defined as $codim\ \mathfrak{p} = dim\ R_{\mathfrak{p}}$ and the **dimension** as $dim\ \mathfrak{p} = dim\ R/\mathfrak{p}$. For an arbitrary ideal I we define the codimension as

$$codim\ I = \inf\{dim\ R_{\mathfrak{p}} \mid \mathfrak{p} \in V(I)\}.$$

If M is an R-module then the dimension is given by

$$dim\ M = dim(R/Ann(M)).$$

If M is finitely generated then $dim\ M$ is the combinatorial dimension of the closed subspace $Supp(M) = V(Ann(M))$ of $Spec(R)$, i.e., the length of the longest chain of closed irreducible subsets in $Supp(M)$.

Now comes the numerical invariant with biggest importance for us.

Definition 1.38. *Let M be an R-module then we define $pd_R(M)$ as the* ***projective dimension****, where $pd_R(M) = n$ if n is the smallest natural number such that there is a projective resolution*

$$0 \to P_n \xrightarrow{d_n} \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0.$$

If no such resolution exists then we define $pd_R(M) = \infty$*.*

Example 1.39. $pd_R(M) = 0$ *if and only if* M *is projective.*

Example 1.40. $pd_R(R[x_1, x_2, \ldots, x_n]) = 0$*, because is free with basis* $\{x_1, x_2, \ldots, x_n\}$*.*

Example 1.41. *Let* V *be a module over the field* $\mathbb{K}$ *(vector space) then* $pd_{\mathbb{K}}(V) = 0$*, since we can always find a basis.*

Here we get an important characterization of the projective dimension of a module using the functor *Ext*.

Proposition 1.42. *Let* $\{K_n\}$ *be the syzygies of* M *coming from a projective resolution of* M*, then* $Ext^{n+1}(M, N) \cong Ext^1(K_{n-1}, N)$ *for every module* N *and every* $n \geq 1$*.*

Proof. Suppose that $\ldots \to P_n \xrightarrow{d_n} \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0$ is the projective resolution that defines the syzygies $\{K_n\}$. Then using $K_{n-1} = Ker(d_{n-1}) = Im(d_n)$ we get the following projective resolution of K_{n-1}

$$\ldots \xrightarrow{d_{n+3}} P_{n+2} \xrightarrow{d_{n+2}} P_{n+1} \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} K_{n-1} \to 0.$$

Then we delete K_{n-1} and apply the functor $Hom(\ ,N)$ to obtain

$$0 \to Hom(P_n, N) \xrightarrow{d^*_{n+1}} Hom(P_{n+1}, N) \xrightarrow{d^*_{n+2}} Hom(P_{n+2}, N) \xrightarrow{d^*_{n+3}} \ldots$$

and from this follows $Ext^1(K_{n-1}, N) = Ker(d^*_{n+2})/Im(d^*_{n+1}) = Ext^{n+1}(M, N)$.

■

Theorem 1.43. *The following three conditions are equivalent for a module* M

(1) $pd(M) \leq n$*;*

(2) $Ext^k(M, N) = 0$ *for all modules* N *and all* $k \geq n + 1$*;*

(3) $Ext^{n+1}(M, N) = 0$ *for all modules* N*.*

Proof. (1) ⇒ (2) If $pd(M) \leq n$ then there is a projective resolution where $P_k = 0$ for all $k \geq n + 1$. Therefore $Hom(P_k, N) = 0$ for any module N and also

$$Ext^k(M, N) = \frac{Ker(d^*_{k+1} : Hom(P_k, N) \to Hom(P_{k+1}, N))}{Im(d^*_k : Hom(P_{k-1}, N) \to Hom(P_k, N))} = 0.$$

(2) $\Rightarrow$ (3) It is clear.

(3) $\Rightarrow$ (1) We proceed with the construction 1.2 of finding a free resolution (which is also projective) until we obtain an exact sequence

$$0 \to K_{n-1} \to F_{n-1} \xrightarrow{d_{n-1}} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0$$

where K_{n-1} is the $(n-1)th$ syzygy. If we obtain before a zero syzygy then the result follows trivially. Otherwise, by hypothesis and *Proposition* 1.42 we have $Ext^1(K_{n-1}, N) = Ext^{n+1}(M, N) = 0$ for all N. Then *Theorem* 1.23 implies that K_{n-1} is projective and $pd(M) \leq n$.

■

Corollary 1.44. *Let M be an R-module with $pd(M) \leq n$, then for any projective resolution of M the corresponding syzygies K_j $(j \geq n-1)$ are projective modules.*

Proof. For $j \geq n-1$ and any module N we have $Ext^1(K_j, N) = Ext^{j+2}(M, N) = 0$ by *Proposition* 1.42 and the previous *Theorem* 1.43. Thus K_j is projective from *Theorem* 1.23.

■

Corollary 1.45. *Suppose M is a module with $pd(M) = n < \infty$ then the sequence*

$$0 \to K_{n-1} \to F_{n-1} \xrightarrow{d_{n-1}} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0$$

from the step n of 1.2 is a projective resolution of M.

This previous corollary says that any module M with $n = pd_R(M) < \infty$ has a projective resolution of length n that is "almost free" and that our initial and rather naive construction 1.2 will always give a projective resolution exactly at the step $n = pd(M)$, i.e., a projective resolution of minimal length. Later we will see that for a finitely generated module over $\mathbb{K}[x_1, \dots, x_n]$ we can get a free resolution of length $n = pd(M)$. For a very nice treatment on *Free Resolutions* one can see [15] in *Chapter 6*.

Corollary 1.46. $pd(M) = inf\{k \in \mathbb{N} \mid Ext^{k+1}(M, N) = 0$ *for all modules* $N\}$.

Corollary 1.47. *Given a family of modules $\{A_i : i \in I\}$, then*

$$pd(\bigoplus_{i \in I} A_i) = \sup\{pd(A_i) : i \in I\}.$$

Proof. Using the previous characterization of projective dimension and *Theorem* 1.18 *(3)*, the result follows. ∎

Example 1.48. *Let* $R = \mathbb{K}[x]/(x^2)$ *and* M *the* R*-module defined by* $M = (x)$*, then* $pd_R(M) = \infty$.[2]

Proof. First let's compute who are F_0 and K_0, since M is generated by one element we get $F_0 = R$, then $K_0 = Ker(R \xrightarrow{x} M) = (x) = M$. Inductively for any n we get the exact sequence $0 \to K_n \to R \xrightarrow{x} K_{n-1}(= M) \to 0$, then all syzygies are equal to $Ker(R \xrightarrow{x} M) = M$.

For any $y \in R \setminus M$ we have $xy \notin R \setminus M$, then the exact sequence $0 \to K_0 \xrightarrow{i} R \xrightarrow{x} M \to 0$ does not split because $i(K_0) = K_0(= M)$ cannot be a direct summand of R. From *Theorem* 1.20 we get M is not projective. Therefore all syzygies are not projective and by *Corollary* 1.45 we get $pd_R(M) = \infty$. ∎

After defining the projective dimension of any R*-module* then we can define the **global dimension** of the ring R.

Definition 1.49. *The global dimension of a ring* R *is defined as*

$$gDim(R) = \sup\{pd_R(M) \mid M \in \mathcal{M}_R\},$$

where $\mathcal{M}_R$ *is the category of* R*-modules.*

Example 1.50. $gDim(\mathbb{K}) = 0$ *because we always have* $pd_{\mathbb{K}}(V) = 0$.

Example 1.51. $gDim(\mathbb{K}[x]/(x^2)) = \infty$ *because as previously stated* $pd_{\mathbb{K}[x]/(x^2)}((x)) = \infty$.

From *Theorem* 1.35 in the previous section, we saw that for a Noetherian ring R and a finite R-module M in the case $IM \neq M$ we can define the numeric invariant of *"length of maximal sequences"*.

Definition 1.52. *Let* R *be a Noetherian ring,* M *a finite* R*-module, and* I *an ideal such that* $IM \neq M$*. The common length of all the maximal* M*-sequences in* I *is called the* ***depth of I on M****, denoted by* $\mathbf{depth(I, M)}$*. When* $M = R$ *is simply called the* ***depth of I*** *and denoted by* $\mathbf{depth(I)}$*. If* $IM = M$ *we adopt the convention* $depth(I, M) = \infty$*.*

[2] Taken from [15], *Exercise 11, page 258.*

We now want to give a characterization of *depth* in terms of the *Ext* functor.

Proposition 1.53. *Let R be a ring, and M, N R-modules. Set $I = Ann(N)$.*

(i) If I contains an M-regular element, then $Hom_R(N, M) = 0$.

(ii) Conversely, if R is Noetherian, and M, N are finite and $Hom_R(N, M) = 0$, implies that I contains an M-regular element.

Proof. See *Proposition 1.2.3*, [6].

■

Proposition 1.54. *Let R be a ring, M, N be R-modules, and $\mathbf{x} = (x_1, \dots, x_n)$ a weak M-sequence in $Ann(N)$. Then*

$$Hom_R(N, M/\mathbf{x}M) \cong Ext_R^n(N, M).$$

Proof. We proceed by induction on n, for $n = 0$ we have trivially $Hom_R(N, M) \cong Ext_R^0(N, M)$. Let $n \geq 1$, and set $\mathbf{x}' = (x_1, \dots, x_{n-1})$. By the induction hypothesis we have $Ext_R^{n-1}(N, M) \cong Hom_R(N, M/\mathbf{x}'M)$. Since x_n is $(M/\mathbf{x}'M)$-regular, then $Ext_R^{n-1}(N, M) = 0$ by the previous *Proposition* 1.53.

The exact sequence

$$0 \to M \xrightarrow{x_1} M \to M/x_1M \to 0$$

yields the exact sequence

$$0 \to Ext_R^{n-1}(N, M/x_1M) \to Ext_R^n(N, M) \xrightarrow{\overline{x_1}} Ext_R^n(N, M).$$

But the multiplication by x_1 annihilates N, therefore we have the isomorphism $Ext_R^n(N, M) \cong Ext_R^{n-1}(N, M/x_1M)$. Again, the inductive hypothesis and the fact that $(x_2, \dots, x_n)$ is regular in M/x_1M, gives the expected result $Ext_R^n(N, M) \cong Hom_R(N, M/\mathbf{x}M)$.

■

Theorem 1.55. ***(Rees).*** *Let R be a Noetherian ring, M a finite R-module, and I an ideal such that $IM \neq M$. Then all maximal M-sequences in I have the same length n given by*

$$depth(I, M) = \min\{i \mid Ext_R^i(R/I, M) \neq 0\}.$$

Proof. Suppose $\mathbf{x} = (x_1, \dots, x_n)$ is a maximal M-sequence in I. From *Proposition* 1.54 we know that $Ext_R^{i-1}(R/I, M) \cong Hom_R(R/I, M/(x_1, \dots, x_{i-1})M)$ for $i = 1, \dots, n$, and by *Proposition* 1.53

$$Ext_R^{i-1}(R/I, M) \cong Hom_R(R/I, M/(x_1, \dots, x_{i-1})M) = 0.$$

Since $IM \neq M$ and $\mathbf{x}$ is maximal in I we have that I consists of zero-divisors of $M/\mathbf{x}M$, then I is contained in some associated prime $\mathfrak{p} = Ann(m)$ for some $m \in M/\mathbf{x}M$ (See *Proposition 1.2.1* [6]). The assignment $1 \mapsto m$ induces a monomorphism $\phi' : R/\mathfrak{p} \to M/\mathbf{x}M$, and thus a non-zero homomorphism $\phi : R/I \to M/\mathbf{x}M$. Therefore we have

$$Ext_R^n(R/I) \cong Hom_R(R/I, M/\mathbf{x}M) \neq 0.$$

■

A very special case is when $(R, \mathfrak{m}, \mathbb{K})$ is a Noetherian local ring, and M finite R-module. We call the depth of M as

$$depth(M) = \min\{i \mid Ext_R^i(\mathbb{K}, M) \neq 0\},$$

where $\mathbb{K} = R/\mathfrak{m}$ is the residue field.

At this point we should stress that the condition $IM \neq M$ is not superfluous and the concept of depth is not well defined when $IM = M$.

Example 1.56. *Let $\mathbb{K}$ be a field and $R = \mathbb{K}[[x]][y]$. Then we have that $\{x, y\}$ and $\{xy-1\}$ are both maximal R-sequences.*[3]

Proof. Since $R/(x, y) \cong \mathbb{K}$, adding any other $q \in R \setminus (x, y)$ will make $(x, y, q) = R$, thus (x, y) is a maximal R-sequence.

Taking the quotient $\mathbb{K}[[x]][y]/(xy-1)$ (the *"Rabinowski's trick"*), is like adjoining the inverse of x, i.e., $\mathbb{K}[[x]][y]/(xy-1) \cong \mathbb{K}[[x]][x^{-1}]$. In general we know that $\sum_{k=0}^{\infty} a_k x^k \in \mathbb{K}[[x]]$ is invertible if and only if $a_0 \neq 0$. Now let $0 \neq \sum_{k=n}^{\infty} a_k x^k \in \mathbb{K}[[x]][x^{-1}]$, where $n \in \mathbb{Z}$ is the smallest integer with $a_n \neq 0$, then $\sum_{k=n}^{\infty} a_k x^k = (x^n)(\sum_{k=n}^{\infty} a_k x^{k-n})$ is clearly invertible. Therefore $\mathbb{K}[[x]][y]/(xy-1)$ is a field and as before $\{xy-1\}$ is a maximal R-sequence. ■

In the following proposition we collect some important results. (From now on, $V(I)$ denotes the set of prime ideals containing I.)

[3] *Exercise 1.2.20*, [6].

Proposition 1.57. *Let R be a Noetherian ring, I, J ideals of R, and M a finite R-module. Then*

(i) $depth(I, M) = inf\{depth(M_{\mathfrak{p}}) \mid \mathfrak{p} \in V(I)\}$;

(ii) $depth(I, M) = depth(rad(I), M)$;

(iii) $depth(I \cap J, M) = min(depth(I, M), depth(J, M))$;

(iv) if $\mathbf{x} = (x_1, \ldots, x_n)$ *is an M-sequence in I, then* $depth(I/(\mathbf{x}), M/\mathbf{x}M) = depth(I, M/\mathbf{x}M) = depth(I, M) - n$;

(v) if N is a finite R-module with $Supp(N) = V(I)$, *then* $depth(I, M) = inf\{i \mid Ext^i_R(N, M) \neq 0\}$.

Proof. See *Proposition 1.2.10*, [6]. ■

In the case of Noetherian local rings there is an important relation between the depth and the dimension.

Proposition 1.58. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and $M \neq 0$ a finite R-module. Then $depth(M) \leq dim(M)$.*

Proof. See *Proposition 1.2.12*, [6]. Also one could see *Theorem 6.5*, [11]. ■

This local property leads to the following very desirable inequality.

Proposition 1.59. *Let R be a Noetherian ring and $I \supset R$ an ideal. Then $depth(I) \leq codim(I)$.*

Proof. We have $depth(I) = inf\{depth(R_{\mathfrak{p}}) \mid \mathfrak{p} \in V(I)\}$ and $codim(I) = inf\{dim(R_{\mathfrak{p}}) \mid \mathfrak{p} \in V(I)\}$, then the previous *Proposition* 1.58 implies the inequality. ■

Finally, as one could expect there is a relation between the characterization of *depth* by means of the *Koszul complex* and by means of the *Ext* functor.

Theorem 1.60. *Let R be a ring, $\mathbf{x} = (x_1, \ldots, x_n)$ a sequence in R, and M a finitely generated R-module. If $I = (\mathbf{x})$ contains a weak M-sequence $\mathbf{y} = (y_1, \ldots, y_m)$, then*

$H_{n+1-i}K(\mathbf{x}, M) = 0$ *for* $i = 1, \ldots, m$ *and*

$$H_{n-m}K(\mathbf{x}, M) \cong Hom_R(R/I, M/\mathbf{y}M) \cong Ext_R^m(R/I, M).$$

Proof. See *Theorem 1.6.16*, [6]. ■

Chapter 2

Some fundamental theorems on syzygies

In this chapter as the title says we will state and prove some interesting results in the theory of syzygies. To begin with, we will choose the *Hilbert's syzygy theorem* that was the starting point of this theory in his famous paper on *Invariant Theory* [7]. Secondly we shall prove a beautiful result conjectured by *Serre*: *"every finitely generated projective module over* $\mathbb{K}[x_1, \ldots, x_n]$ *is free"*. Lastly we shall deal with the theory of our syzygies in the case of a local ring.

2.1 Towards Hilbert's syzygy theorem and more

Lemma 2.1. *If* $0 \to A \to B \to C \to 0$ *is exact then*

$$pd(C) \leq 1 + max(pd(A), pd(B)).$$

Proof. If $max(pd(A), pd(B))$ is infinite we don't have anything to prove, therefore we assume it is finite. Let $n = max(pd(A), pd(B))$ then applying *Theorem* 1.19 for any module N we get the following piece of exact sequence

$$\ldots \to Ext^{n+1}(A, N) \to Ext^{n+2}(C, N) \to Ext^{n+2}(B, N) \to \ldots$$

Thus *Theorem* 1.43 and $pd(A), pd(B) \leq n$ implies

$$\ldots \to 0 \to Ext^{n+2}(C, N) \to 0 \to \ldots$$

that is $Ext^{n+2}(C, N) = 0$. Finally by *Theorem* 1.43 we get $pd(C) \leq 1 + n$. ■

If M is an R-module then we denote

$$M[x] = M \otimes_R R[x] \tag{2.1}$$

as the R-module generated by the elements $m \otimes_R x^k$, where $k \in \mathbb{N}$ and $m \in M$, that is

$$M[x] = \bigoplus_{k=0}^{\infty} M \otimes_R x^k$$

which may be regarded as an $R[x]$-module taking into account the grading of the x^k's. Also we have that if P is R-projective then $P \otimes_R R[x]$ is $R[x]$-projective, suppose we have the following diagram as in *Definition* 1.3, where B and C are $R[x]$-modules

$$\begin{tikzcd}
 & P \otimes_R R[x] \arrow[dl, dashed, "\phi"'] \arrow[d, "\alpha"] & \\
B \arrow[r, "\beta"'] & C \arrow[r] & 0.
\end{tikzcd}$$

Given the graded structure of $P \otimes_R R[x]$, it is enough to induce a function ϕ that accomplish $\alpha(P \otimes_R x^k) = (\beta \circ \phi)(P \otimes_R x^k)$ as an R-linear map and then we extend it to all of $P \otimes_R R[x]$ with the grading of the x^k's. The isomorphism $P \otimes_R x^k \cong P$, the projectivity of P and looking at B and C as R-modules induces a map $\phi : P \otimes_R R[x] \to B$, where each restriction $\phi\mid_{P \otimes_R x^k}$ is an R-*linear* map that makes commute the previous diagram.

Lemma 2.2. *For every R-module M we have*

$$pd_{R[x]}(M[x]) \leq pd_R(M).$$

Proof. Suppose $pd_R(M) = n$ then there is an R-projective resolution

$$0 \to P_n \xrightarrow{d_n} \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0.$$

The ring of polynomials $R[x]$ is a flat R-module (it is even free), then we can tensor

$\otimes_R R[x]$ and obtain the exact sequence

$$0 \to P_n \otimes_R R[x] \xrightarrow{d_n \otimes_R 1} \ldots \xrightarrow{d_2 \otimes_R 1} P_1 \otimes_R R[x] \xrightarrow{d_1 \otimes_R 1} P_0 \otimes_R R[x] \xrightarrow{d_0 \otimes_R 1} M[x] \to 0.$$

Where each $P_k \otimes_R R[x]$ is an $R[x]$-projective module, then we get $pd_{R[x]}(M[x]) \leq n$. ■

If M is an $R[x]$-module certainly we can see it as an R-module and we can also make the construction $M[x] = M \otimes_R R[x]$ that is an $R[x]$-module, where technically the action of x is given by $x(m \otimes_R x^k) = m \otimes_R x^{k+1}$. Although xm is perfectly well defined, the operation $x(m \otimes_R x^k) = xm \otimes_R x^k$ is not correct for our construction 2.1.

Lemma 2.3. *If M is an $R[x]$-module then there is an $R[x]$-exact sequence*

$$0 \to M[x] \xrightarrow{\alpha} M[x] \xrightarrow{\beta} M \to 0.$$

Proof. We define the map β by $\beta(m \otimes_R x^k) = x^k m$ (M is already an $R[x]$-module) and the map α by $\alpha(m \otimes_R x^k) = m \otimes_R x^{k+1} - xm \otimes_R x^k$, for any $k \geq 0$ and any $m \in M$. It is clear that β is surjective, for example restricting it we get $\beta(M \otimes_R 1) = M$.

If $w = \sum_{k=0}^n m_k \otimes_R x^k \in M[x]$ and $\alpha(w) = \sum_{k=0}^n m_k \otimes_R x^{k+1} - \sum_{k=0}^n xm_k \otimes_R x^k = -xm_0 \otimes_R 1 + \sum_{k=1}^n (m_{k-1} - xm_k) \otimes_R x^k + m_n \otimes_R x^{n+1} = 0$ then

$$m_0 - xm_1 = m_1 - xm_2 = \ldots = m_{n-1} - xm_n = m_n = 0,$$

so $m_0 = m_1 = \ldots = m_n = 0$ and α is injective.

By the given definitions we have trivially $\beta \circ \alpha = 0$ then $Im(\alpha) \subset Ker(\beta)$. But let $w = \sum_{k=0}^n m_k \otimes_R x^k \in Ker(\beta)$, hence $\beta(w) = 0$ and $\sum_{k=0}^n x^k m_k = 0$, which gives $m_0 = -\sum_{k=1}^n x^k m_k$. The following elements

$$\begin{aligned} u_{n-1} &= m_n \\ u_{n-2} &= m_{n-1} + xm_n \\ u_{n-3} &= m_{n-2} + xm_{n-1} + x^2 m_n \\ &\vdots \\ u_0 &= m_1 + xm_2 + \ldots + x^{n-1} m_n \end{aligned}$$

have the property that

$$\alpha(\sum_{k=0}^{n-1} u_k \otimes_R x^k) = -xu_0 \otimes_R 1 + \sum_{k=1}^{n-1}(u_{k-1} - xu_k) \otimes_R x^k + u_{n-1} \otimes_R x^n$$
$$= \sum_{k=0}^{n} m_k \otimes_R x^k.$$

Therefore actually we have $Im(\alpha) = Ker(\beta)$. ■

At this point we are finally ready to state and prove the main result of this section which relates the projective dimension over $R[x]$ and over R.

Theorem 2.4. *Let M be an $R[x]$-module then*

$$pd_{R[x]}(M) \leq 1 + pd_R(M).$$

Proof. We take the previous $R[x]$-exact sequence

$$0 \to M[x] \xrightarrow{\alpha} M[x] \xrightarrow{\beta} M \to 0,$$

with *Lemma* 2.1 we find the inequality $pd_{R[x]}(M) \leq 1 + pd_{R[x]}(M[x])$ and *Lemma* 2.2 gives $pd_{R[x]}(M[x]) \leq pd_R(M)$, which combined prove our assertion. ■

Corollary 2.5. *Let M be an $R[x_1, x_2, \dots, x_n]$-module then $pd_{R[x_1,x_2,\dots,x_n]}(M) \leq n + pd_R(M)$.*

Proof. Make induction by successively taking $R[x_1, \dots, x_{k-1}, x_k] = R[x_1, \dots, x_{k-1}][x_k]$. ■

Corollary 2.6. *Let $\mathbb{K}$ be a field and M be a $\mathbb{K}[x_1, x_2, \dots, x_n]$-module then $pd_{\mathbb{K}[x_1,x_2,\dots,x_n]}(M) \leq n$.*

Corollary 2.7. *Let R be a ring then $gDim(R[x_1, x_2, \dots, x_n]) \leq n + gDim(R)$.*

Remark 2.8. *We have achieved our goal of exposing a version of Hilbert's syzygy theorem in the most general settlement inside Commutative Algebra, i.e for commutative ring R; for a different approach see [3] in Chapter 19 and [5] in Chapter 3. Now unfortunately we will have to put additional properties to our ring R in order to get more interesting results. In the future we will stress which type of ring we are working and if it is not mentioned by* *default will be a general commutative ring.*

Proposition 2.9. *Let R be a Noetherian ring and M a finitely generated R-module with $pd_R(M) = n < \infty$, then it has a projective resolution of length n which is composed of finitely generated modules.*

Proof. Again our prays will be answered by the construction 1.2. Take a projective resolution like in Corollary 1.45

$$0 \to K_{n-1} \to F_{n-1} \xrightarrow{d_{n-1}} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0.$$

Since M is finitely generated then can we can take the free module F_0 also as a finitely generated module. The module F_0 is Noetherian because R is Noetherian and F_0 is finitely generated (see [3] *Proposition 1.4*), therefore we have that $K_0 = Ker(d_0) \subset F_0$ is finitely generated because is a submodule of a Noetherian module.

Following this procedure we get from the exact sequence $0 \to K_1 \to F_1 \to K_0 \to 0$ that F_1 and K_1 are finitely generated, inductively from $0 \to K_j \to F_j \to K_{j-1} \to 0$ we get that all the free modules F_j and all the syzygies K_j are finitely generated. In particular, our previous projective resolution is composed of finitely generated modules.

■

Corollary 2.10. *Over a Noetherian ring R every finitely generated module M has a free resolution composed of finitely generated free modules.*

Proof. We can continue infinitely the process in the previous Proposition 2.9 to obtain

$$\dots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} F_{n-1} \xrightarrow{d_{n-1}} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0,$$

where each F_j is finitely generated and free.

■

Corollary 2.11. ***(Hilbert's syzygy theorem)*** *Let $\mathbb{K}$ be a field and M be a finitely generated $\mathbb{K}[x_1, x_2, \dots, x_n]$-module then M has a free resolution (consists of finitely generated modules) of length at most n.*

Proof. From *Corollary* 2.6 we have $pd(M) \leq n$. The ring $\mathbb{K}[x_1, x_2, \dots, x_n]$ is Noetherian because of Hilbert Basis theorem (see [3] *Theorem 1.2*), then the previous *Proposition* 2.9 implies M has a projective resolution of length at most n that is composed of finitely generated modules. Finally by the *Quillen-Suslin Theorem* 2.31 the modules in the projective resolution are actually free. ■

We finish this section by remarking that in *Corollary* 2.7 we have actually an equality

$$gDim(R[x_1, x_2, \ldots, x_n]) = n + gDim(R),$$

but proving it lies outside the interests of this work. The way of proving it is by making a **change of rings** (see [19] page 245). Here we have tried to give an example to illustrate this construction, where is present the equality $pd_{R[x]}(R) = 1 + pd_R(R)$.

Example 2.12. *Let R be a ring and $R[x]$ its polynomial ring, then $pd_{R[x]}(R) = 1$.*

Proof. Certainly we have to elaborate more the enunciate: how can we see R as an $R[x]$-module? Using the projection map $\pi : R[x] \to R[x]/xR[x] \cong R$, we define for $p \in R[x]$ and $r \in R$ the scalar product $p * r = \pi(p)r$, i.e., if $p(x) = a_n x^n + \ldots + a_0$ then $p * r = a_0 r$ (for a better explanation on this type of construction, see [10] *page 30*). Then we can get a projective resolution of R as an $R[x]$-module by

$$0 \to R[x] \xrightarrow{x} R[x] \xrightarrow{\pi} R \to 0$$

where the first map is multiplication by x, hence we get $pd_{R[x]}(R) \leq 1$. But $xR[x]$ cannot be a direct summand of $R[x]$ and then the previous exact sequence does not split. Finally, by *Theorem* 1.20 we get R is not a projective $R[x]$-module and $pd_{R[x]}(R) = 1$. ■

2.2 On Serre's conjecture

It the famous article *"Faisceaux algébriques cohérents"* (FAC, 1955), Serre wrote: *"On ignore s'il existe des A-modules projectifs de type fini qui ne soient pas libres"* ($A = \mathbb{K}[x_1, \ldots, x_n]$, $\mathbb{K}$ a field); shortly thereafter, the freeness of finitely generated projective modules over $\mathbb{K}[x_1, \ldots, x_n]$ became known to the mathematical world as **"Serre's Conjecture"**. After twenty years, in 1976 *Daniel Quillen* and *Andrei Suslin* independently proved that finitely generated projective modules over $\mathbb{K}[x_1, \ldots, x_n]$ are, indeed, free.[1]

[1] Quoted from [8], where there is a complete development both historical and mathematical of the Serre's Conjecture.

During this section we will prove this strong assertion, that in part gave the *Fields Medal* to *Quillen* in 1978. In [8] there are several proofs, but we have chosen to follow one that is very close to our work. Using our developed machinery to deal with *syzygies* we will prove the *Serre's theorem: every finitely generated projective module over* $\mathbb{K}[x_1, \ldots, x_n]$ *is stably free*. Finally we will follow the *"Suslin's elementary proof"* to show that *every stably free module over* $\mathbb{K}[x_1, \ldots, x_n]$ *is free.*

2.2.1 A theorem of Serre

From now on, we will use the term f.g. every time we want to say *finitely generated*. We will follow the proof from [19] (pages $251 - 256$) and we will fill some details that are left to the reader.

Definition 2.13. *A module M is* ***stably free*** *if $F \cong M \oplus G$ where F and G are both f.g. free modules.*

Definition 2.14. *A module M has a* ***finite free resolution*** *of length n if there is an exact sequence*

$$0 \to F_n \to \ldots \to F_0 \to M \to 0$$

in which each F_i is f.g. free.

The following lemma relates the previous two definitions.

Lemma 2.15. *A projective module P has a finite free resolution if and only if is stably free.*[2]

Proof. ($\Leftarrow$) If P is stably free then $F = P \oplus G$ with F and G f.g. free. Therefore $0 \to G \to F \to P \to 0$ is a finite free resolution of P.

($\Rightarrow$) We proceed with induction on n, if $n = 0$ then P is stably free (actually free). Otherwise, if $n \geq 1$ then

$$0 \to F_n \to \ldots \to F_0 \to P \to 0$$

is a finite free resolution of P. From *Corollary* 1.21 we have $F_0 \cong K_0 \oplus P$ and K_0 is also

[2] *Exercise 9.15* from [19].

a projective module, then we have the following finite free resolution

$$0 \to F_n \to \ldots \to F_1 \to K_0 \to 0.$$

By the inductive hypothesis K_0 is stably free and there exists f.g. free modules F and G with $F = G \oplus K_0$. Therefore we have $G \oplus F_0 \cong G \oplus K_0 \oplus P \cong F \oplus P$ and P is stably free. ∎

Lemma 2.16. *Given two exact sequences, where the P's and Q's are projective,*

$$0 \to A \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \xrightarrow{d_{n-1}} \ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0, \tag{2.2}$$
$$0 \to B \xrightarrow{e_{n+1}} Q_n \xrightarrow{e_n} Q_{n-1} \xrightarrow{e_{n-1}} \ldots \xrightarrow{e_2} Q_1 \xrightarrow{e_1} Q_0 \xrightarrow{e_0} M \to 0, \tag{2.3}$$

then $A \oplus Q_n \oplus P_{n-1} \oplus \ldots \cong B \oplus P_n \oplus Q_{n-1} \oplus \ldots$.[3]

Proof. For the exact sequences 2.2 and 2.3 we denote their syzygies as $K_j = Ker(d_j)$ and $L_j = Ker(e_j)$. For their corresponding 0th syzygies we have K_0 and L_0

$$0 \to K_0 \to P_0 \xrightarrow{d_0} M \to 0$$
$$0 \to L_0 \to Q_0 \xrightarrow{e_0} M \to 0.$$

Using that P_0 and Q_0 are projective modules, by *Schanuel's Lemma* (*Theorem 3.62*, [19]) we get the isomorphism $K_0 \oplus Q_0 \cong L_0 \oplus P_0$.

With 2.2 and 2.3 we can also obtain

$$0 \to A \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \xrightarrow{d_{n-1}} \ldots \xrightarrow{d_2} P_1 \xrightarrow{\overline{d_1}} K_0 \to 0,$$
$$0 \to B \xrightarrow{e_{n+1}} Q_n \xrightarrow{e_n} Q_{n-1} \xrightarrow{e_{n-1}} \ldots \xrightarrow{e_2} Q_1 \xrightarrow{\overline{e_1}} L_0 \to 0,$$

where $\overline{d_1}$ and $\overline{e_1}$ are the restrictions of d_1 and e_1 to their images. Then we can construct the new exact sequences

$$0 \to A \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} \ldots \xrightarrow{d_3} P_2 \xrightarrow{i_1 \circ d_2} P_1 \oplus Q_0 \xrightarrow{\overline{d_1} \oplus id_{Q_0}} K_0 \oplus Q_0 \to 0 \tag{2.4}$$
$$0 \to B \xrightarrow{e_{n+1}} Q_n \xrightarrow{e_n} \ldots \xrightarrow{e_3} Q_2 \xrightarrow{j_1 \circ e_2} Q_1 \oplus P_0 \xrightarrow{\overline{e_1} \oplus id_{P_0}} L_0 \oplus P_0 \to 0 \tag{2.5}$$

where $i_1(x) = (x, 0)\ \forall x \in P_1$, $j_1(y) = (y, 0)\ \forall y \in Q_1$ and id_{P_0}, id_{Q_0} are identity maps. From $Ker(\overline{d_1} \oplus id_{Q_0}) \cong Ker(d_1) = K_1$, $Ker(\overline{e_1} \oplus id_{P_0}) \cong Ker(e_1) = L_1$, $Ker(i_1 \circ d_2) =$

[3] *Exercise 3.37* from [19].

$Ker(d_2) = K_2$ and $Ker(j_1 \circ e_2) = Ker(e_2) = L_2$, we get that up to isomorphisms the new sequences have the same syzygies as the original ones.

Using the obtained isomorphism $K_0 \oplus Q_0 \cong L_0 \oplus P_0$ and the fact that $P_1 \oplus Q_0$ and $Q_1 \oplus P_0$ are projective modules, we can apply the previous process to 2.4 and 2.5, reducing again the sequences and getting the isomorphism $K_1 \oplus Q_1 \oplus P_0 \cong L_1 \oplus P_1 \oplus Q_0$.

Iterating with this process we get

$$0 \to A \to (P_n \oplus Q_{n-1} \oplus \dots) \to (K_{n-1} \oplus Q_{n-1} \oplus \dots) \to 0$$
$$0 \to B \to (Q_n \oplus P_{n-1} \oplus \dots) \to (L_{n-1} \oplus P_{n-1} \oplus \dots) \to 0$$

where $(K_{n-1} \oplus Q_{n-1} \oplus \dots) \cong (L_{n-1} \oplus P_{n-1} \oplus \dots)$, and $(P_n \oplus Q_{n-1} \oplus \dots)$ and $(Q_n \oplus P_{n-1} \oplus \dots)$ are projective modules. Finally, again by *Schanuel's lemma*

$$A \oplus Q_n \oplus P_{n-1} \oplus \dots \cong B \oplus P_n \oplus Q_{n-1} \oplus \dots .$$

■

Lemma 2.17. *Let R be a Noetherian ring and M an R-module with a finite free resolution of length $\leq n$. Then every free resolution(not necessarily finite) of M composed of f.g. modules, has a stably free and f.g n-th syzygy.*[4]

Proof. Let $0 \to F_n \xrightarrow{d_n} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0$ be the given finite free resolution of M with length n (if it had length smaller than n we fill it with some $F_j = 0$). All syzygies are f.g. because over a Noetherian ring submodules of f.g. modules are f.g. (just like in *Proposition* 2.9).

Let $\dots \xrightarrow{e_{n+1}} G_n \xrightarrow{e_n} G_{n-1} \xrightarrow{e_{n-1}} \dots \xrightarrow{e_2} G_1 \xrightarrow{e_1} G_0 \xrightarrow{e_0} M \to 0$ be a free resolution of M with all G_j f.g. free. Then we want to prove that $Q_n = Ker(e_n) = Im(e_{n+1})$ is stably free and f.g., the finiteness of Q_n follows in the same way by the previous Noetherian argument.

We make the following two exact sequences

$$0 \to 0 \to F_n \xrightarrow{d_n} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0$$
$$0 \to Q_n \xrightarrow{i} G_n \xrightarrow{e_n} \dots \xrightarrow{e_2} G_1 \xrightarrow{e_1} G_0 \xrightarrow{e_0} M \to 0,$$

then with the *Lemma* 2.16 we get $Q_n \oplus F_n \oplus G_{n-1} \oplus \dots \cong G_n \oplus F_{n-1} \oplus \dots$. Therefore Q_n is stably free because all F_i, G_i are f.g. free. ■

[4] *Exercise 9.16* from [19].

Lemma 2.18. *If M has a projective resolution*

$$0 \to P_n \xrightarrow{d_n} \ldots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0.$$

where each P_i is stably free, then M has a finite free resolution.

Proof. We proceed making induction on n. If $n = 0$ then $P_0 \cong M$ and *Lemma* 2.15 gives the finite free resolution of M. If $n \geq 1$, then we take the f.g. free module F that makes $P_0 \oplus F$ f.g. free, and we construct the following exact sequence

$$0 \to P_n \xrightarrow{d_n} \ldots \xrightarrow{d_3} P_2 \xrightarrow{i_1 \circ d_2} P_1 \oplus F \xrightarrow{d_1 \oplus id_F} P_0 \oplus F \xrightarrow{d_0 \circ \pi_{P_0}} M \to 0,$$

where i_1 is an inclusion map (as before), id_F the identity map and π_{M_0} a projection map. With the 0-th syzygy $K_0 = Ker(d_0)$ we can get

$$0 \to P_n \xrightarrow{d_n} \ldots \xrightarrow{d_3} P_2 \xrightarrow{i_1 \circ d_2} P_1 \oplus F \xrightarrow{d_1 \oplus id_F} K_0 \oplus F \to 0$$
$$0 \to K_0 \oplus F \to P_0 \oplus F \xrightarrow{d_0 \circ \pi_{P_0}} M \to 0.$$

Then $K_0 \oplus F$ has a projective resolution of length $n-1$ with each member stably free, hence by the inductive hypothesis there exists a finite free resolution $0 \to E_m \to \ldots \to E_0 \to K_0 \oplus F \to 0$ and gluing it with the second equation we get the finite free resolution

$$0 \to E_m \to \ldots \to E_0 \to P_0 \oplus F \to M \to 0$$

for the module M.

∎

Theorem 2.19. *Let R be a Noetherian ring and $0 \to L \to M \to N \to 0$ an exact sequence of R-modules. If two of the modules have a finite free resolution, then so does the third.*

Proof. The two modules that have finite free resolution are f.g.; if L and M, then N is f.g. because the second map is surjective; if L and N, then $M \cong L + N$ is f.g.; if M and N, then L is f.g. because is a submodule of M and the Noetherian hypothesis. Therefore we assume that the free modules are f.g.

Using *Corollary* 2.10 we obtain the free resolutions $\ldots \to F_1 \to F_0 \to L \to 0$ and $\ldots \to H_1 \to H_0 \to H \to 0$ composed of f.g. modules. Then the *Horseshoe Lemma* (*Lemma 6.20*, [19]) induces a projective resolution for M that makes commute the diagram below, where each row and each column is exact. Each row $0 \to F_n \to G_n \to H_n \to 0$

splits because each H_n is free, then $G_n \cong F_n \oplus H_n$ and the induced projective resolution for M is actually a free resolution composed of f.g. modules. Also, let I_n, J_n and K_n be the syzygies of the respective rows of L, M and N, then there are short exact sequences $0 \to I_n \to J_n \to K_n \to 0$.

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d, dashed] & \vdots \arrow[d] & \\
0 \arrow[r] & F_1 \arrow[r, dashed] \arrow[d] & G_1 \arrow[r, dashed] \arrow[d, dashed] & H_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & F_0 \arrow[r, dashed] \arrow[d] & G_0 \arrow[r, dashed] \arrow[d, dashed] & H_0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, dashed] & N \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Assuming two of $\{L, M, N\}$ have a finite free resolution, then by *Lemma* 2.17 two of $\{I_m, J_m, K_m\}$ are stably free, where m is the maximal length between the two given finite free resolutions. If one of these is K_m then the sequence $0 \to I_m \to J_m \to K_m \to 0$ splits ($J_m \cong I_m \oplus K_m$) and the third one is necessarily stably free, thus we get the resolutions composed of stably free modules: $0 \to I_m \to F_m \to \ldots \to F_0 \to L \to 0$, $0 \to J_m \to G_m \to \ldots \to G_0 \to M \to 0$ and $0 \to K_m \to H_m \to \ldots \to H_0 \to N \to 0$.

The remaining case is when I_m and J_m are stably free, then by a simple diagram chasing

$$0 \to I_m \to J_m \to H_m \to \ldots \to H_0 \to N \to 0$$

is a projective resolution of N composed of stably free modules.

Therefore in every cases by *Lemma* 2.18 the three modules L, M and N have finite free resolution. ∎

Let M be an R-module then its annihilator is the ideal $Ann(M) = \{r \in R \mid rM = 0\}$, and for an element $x \in M$ its annihilator is the ideal $Ann(x) = \{r \in R \mid rx = 0\}$. Sometimes we will write $Ann_R(M)$ when we want to stress the ring over which we are taking the annihilator.

Lemma 2.20. *Let R be a Noetherian ring and $M \neq 0$ an R-module. Then $\sum(M) = \{Ann(x) \mid x \in M, x \neq 0\}$ has a maximal ideal in $\sum(M)$ that is prime.*

Proof. The collection of ideals $\sum(M)$ is not empty since $M \neq 0$, then $\sum(M)$ has a maximal element $I = Ann(x)$ for some $x \in M \setminus \{0\}$, because R is Noetherian (see *Chapter 6*, [10]). Suppose by contradiction $a \notin I$, $b \notin I$ and $ab \in I$; then $I + (a) \supsetneq I$, $bx \neq 0$ and $abx = 0$. Combining this we get $Ann(bx) \supset I + (a) \supsetneq I$, that contradicts the maximality of I in $\sum(M)$.

∎

Proposition 2.21. *Let R be an Noetherian ring and $M \neq 0$ be a f.g. R-module. Then there is a chain*

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_n = M$$

where $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ where each $\mathfrak{p}_i$ is a prime ideal, and for each we have $\mathfrak{p}_i \supset Ann(M)$.

Proof. By *Lemma* 2.20, let $\mathfrak{p}_1 = Ann(x_1)$ be the prime ideal that is maximal in $\sum(M)$, we define $M_1 = (x_1)$ and with the surjective homomorphism $R \xrightarrow{x_1} M_1$ we get $M_1 \cong R/\mathfrak{p}_1$. In the same way choose $\mathfrak{p}_2 = Ann(x_2 + M_1)$ as the maximal element in $\sum(M/M_1)$, define $M_2 = (x_1, x_2)$ and with the surjective homomorphism $R \xrightarrow{x_2+M_1} M_2/M_1$ follows the isomorphism $M_2/M_1 \cong R/\mathfrak{p}_2$.

Inductively, if $M_k = (x_1, \ldots, x_k) \neq M$ then $M/M_k \neq 0$, thus we can choose $\mathfrak{p}_{k+1} = Ann(x_{k+1} + M_k)$ maximal in $\sum(M/M_k)$ and $M_{k+1}/M_k \cong R/\mathfrak{p}_{k+1}$. But the module M is Noetherian because is f.g. over R and such infinite ascending chain cannot exists (see *Chapter 6*, [10]). Therefore $M_n = M$ for some n. For stated inclusion $\mathfrak{p}_k \supset Ann(M)$, since $x_k + M_{k-1} \in M/M_{k-1}$ we always have $\mathfrak{p}_k = Ann(x_k + M_{k-1}) \supset Ann(M/M_{k-1}) \supset Ann(M)$.

∎

Theorem 2.22. *Let R be a Noetherian ring and assume every f.g. R-module has a finite free resolution, then every f.g. $R[x]$-module has a finite free resolution.*

Proof. By contradiction suppose there is a f.g. $R[x]$-module that has no finite free resolution. Then the family of ideals of R

$$\sum = \{Ann_R(M) \mid M \text{ is a f.g. } R[x]\text{-module and has no finite free resolution}\}$$

is not empty, and using R is Noetherian we choose an $R[x]$-module M^* with $I = Ann_R(M^*)$ is maximal in the previous family (here were are stressing $Ann_R(M)$ because M is an $R[x]$-module, although we could have used also $Ann_{R[x]}(M) \cap R (= Ann_R(M))$).

From *Proposition* 2.21 we can get

$$
\begin{aligned}
0 \to M_0(=0) \to M_1 \to R[x]/\mathfrak{p}_1 \to 0 \\
0 \to M_1 \to M_2 \to R[x]/\mathfrak{p}_2 \to 0 \\
\vdots \\
0 \to M_{n-1} \to M_n(=M^*) \to R[x]/\mathfrak{p}_n \to 0.
\end{aligned}
$$

Thus if we show that each $R[x]/\mathfrak{p}_j$ has a finite free resolution, applying *Theorem* 2.19 iteratively we get that M^* has a finite free resolution, which is the contradiction we are looking for.

From *Proposition* 2.21 we have $Ann_{R[x]}(R[x]/\mathfrak{p}_k) \supset \mathfrak{p}_k \supset Ann_{R[x]}(M)$ and intersecting with R we get $Ann_R(R[x]/\mathfrak{p}_k) \supset \mathfrak{p}_k \cap R \supset I$. If $\mathfrak{p}_k \cap R \supsetneq I$ then by the maximality of I we get that $R[x]/\mathfrak{p}_k$ has a finite free resolution.

Therefore we only have to deal with the case $\mathfrak{p}_k \cap R = I$, and I will be a prime ideal in R because by *Proposition* 2.21 the ideal $\mathfrak{p}_k$ is prime in $R[x]$. Also in this case $R_0 \cong R/I$ is an integral domain. Here using $R[x]I \subset \mathfrak{p}_k$ we get the isomorphism

$$
R_0[x]/\mathfrak{q}_k \cong \frac{R[x]/(R[x]I)}{\mathfrak{p}_k/(R[x]I)} \cong R[x]/\mathfrak{p}_k \tag{2.6}
$$

where $R_0[x] = R[x]/(R[x]I)$ and $\mathfrak{q}_k = \mathfrak{p}_k/(R[x]I)$. We may see $R_0[x]$ and $\mathfrak{q}_k$ as $R_0[x]$-modules and as $R[x]$-modules.

Suppose $g_1, \ldots, g_m$ are the generators of $\mathfrak{q}_k$ and choose f of minimal degree in $\mathfrak{q}_k$. We take K_0 the field of fractions of R_0. By an application of the division algorithm in $K_0[x]$ and the minimality of degree of f, we have $g_i = p_i f$ for $p_i \in K_0[x]$. Clearing denominators, for each g_i we get some $a_i \in R_0$ with $a_i g_i \in (f)$. With the product $a = \prod a_i$ we have $a\mathfrak{q}_k \subset (f)$, then $Ann_{R_0}(\mathfrak{q}_k/(f)) \neq 0$ since it contains the element a.

We have $Ann_{R_0}(\mathfrak{q}_k/(f)) = J/I$ for some ideal J in R, then $Ann_{R_0}(\mathfrak{q}_k/(f)) \neq 0$ implies $J \supsetneq I$. But then we have $J(\mathfrak{q}_k/(f)) = 0$ when we look it as an $R[x]$-module via the map $R[x] \to R[x]/(R[x]I)$. Thus by the maximality of I we get that $\mathfrak{q}_k/(f)$ has a finite free resolution as an $R[x]$-module.

By the hypothesis of the theorem we have that I has a finite free resolution

$$
0 \to F_r \to \ldots \to F_1 \to F_0 \to I \to 0,
$$

computing tensor product with the flat R-module $R[x]$ we get

$$0 \to F_r \otimes_R R[x] \to \ldots \to F_1 \otimes_R R[x] \to F_0 \to I \otimes_R R[x] \to 0$$

then $R[x]I \cong I \otimes_R R[x]$ has a finite free resolution.

With the exact sequence

$$0 \to R[x]I \to R[x] \to R_0[x] \to 0$$

and *Theorem* 2.19, $R_0[x]$ has finite free resolution as $R[x]$-module.

In the exact sequence

$$0 \to (f) \to \mathfrak{q}_k \to \mathfrak{q}_k/(f) \to 0$$

we have that $(f) \cong R_0[x]$ because $R_0[x]$ is an integral domain. Therefore applying *Theorem* 2.19 we finally get that $\mathfrak{q}_k$ and $R_0[x]/\mathfrak{q}_k \cong R[x]/\mathfrak{p}_k$ have finite free resolution as $R[x]$-modules.

■

Theorem 2.23. ***(Serre)*** *If $\mathbb{K}$ is a field, then every f.g. projective $\mathbb{K}[x_1, \ldots, x_n]$-module is stably free.*

Proof. The proof follows by induction on n. If $n = 1$ then $\mathbb{K}[x]$ is a principal ideal domain and clearly every f.g. module (ideal) has a finite free resolution (are actually free). If $n > 1$ then by the induction hypothesis every f.g. module over $\mathbb{K}[x_1, \ldots, x_{n-1}]$ has a finite free resolution. From Hilbert Basis Theorem $\mathbb{K}[x_1, \ldots, x_{n-1}]$ is a Noetherian ring, then by *Theorem* 2.22 we get that every f.g. module over $\mathbb{K}[x_1, \ldots, x_{n-1}, x_n] = \mathbb{K}[x_1, \ldots, x_{n-1}][x_n]$ has a finite free resolution.

In particular, any f.g. projective module over $\mathbb{K}[x_1, \ldots, x_n]$ has a finite free resolution, therefore by *Lemma* 2.15 is a stably free module. ■

2.2.2 The Calculus of Unimodular Rows

In this subsection we shall prove that any stably free module over $R = \mathbb{K}[x_1, \ldots, x_n]$ is a free module. Our exposition will be based on *Chapter 3, Section 2* from [8] and *Chapter 21, Section 3* from [9]. We shall show a simplification made by *Vaserstein* to the proof of *Suslin.*

The ideas introduced by *Suslin* are very important because they established the **calculus of unimodular rows** as a new theme for research in commutative ring theory, and made the *Serre's conjecture* accessible to any graduate student.

Definition 2.24. *Let R be a ring and $(f_1, \ldots, f_r) \in R^{1\times r}$ be a row of elements. We say that $(f_1, \ldots, f_r)$ is a* ***unimodular row*** *if $f_1R + \ldots + f_rR = R$.*

For preference of notation we shall work using columns and throughout this subsection f will always denote the column vector $f = (f_1, \ldots, f_r)^t \in R^{r\times 1}$. We say that f has the **unimodular extension property** if there exists a matrix $GL_r(R)$ with f as the first column.

Theorem 2.25. ***(Horrocks)*** *Let $(R, \mathfrak{m})$ be a local ring and let $R[x]$ be the polynomial ring in one variable over R. Let f be a unimodular vector in $R[x]^r$ such that some component has leading coefficient 1. Then f has the unimodular extension property in $R[x]$.*

Proof. If $r = 1$ the statement is trivial and if $r = 2$ we can always construct such matrix because $1 \in (f_1, f_2)$. Thus we assume that $r \geq 3$ and we will proceed by induction on the smallest degree d of a component of f with leading coefficient 1. We will make several row operations that will take f into the elementary vector $e_1 = (1, 0, \ldots, 0)^t$, since this is equivalent to the existence of elementary matrices $E_1, \ldots, E_m$ with $E_m \ldots E_1 f = e_1$, we will get that f is the first column of the matrix $E_1^{-1} \ldots E_m^{-1} \in GL_r(R[x])$. Also these elementary transformations does not change the unimodularity of a vector.

We assume that f_1 has leading coefficient 1 and degree d. By the possibility of applying the Euclidean division algorithm when a polynomial has leading coefficient 1, we may assume that $deg(f_i) < d$ for all $2 \leq i \leq r$. Since f is unimodular, there exist polynomials g_i with $\sum_{i=1}^{r} f_i g_i = 1$ and from this we may conclude that not all coefficients of $f_2, \ldots, f_r$ belongs to the maximal ideal $\mathfrak{m}$. By contradiction we suppose that all coefficients of $f_2, \ldots, f_r$ belong to $\mathfrak{m}$, then for the polynomial $f_1 g_1$ we have $(f_1 g_1)_0 \in 1 - \mathfrak{m}$ and $(f_1 g_1)_j \in \mathfrak{m}$ for $j \geq 1$. We have that $f_1 = x^d + a_{d-1}x^{d-1} + \ldots + a_0$ and $g_1 = c_m x^m + c_{m-1}x^{m-1} + \ldots + c_0$, the coefficient $(f_1 g_1)_{m+d} = c_m$ implies that $c_m \in \mathfrak{m}$, and following inductively with the coefficients $(f_1 g_1)_k = c_{k-d} + a_{d-1}c_{k-d+1} + \ldots \in \mathfrak{m}$ until $k = d$ we get that all $c_i \in \mathfrak{m}$. So we get $a_0 c_0 \in 1 - \mathfrak{m}$ and $a_0 c_0 \in \mathfrak{m}$, that implies the contradiction $1 \in \mathfrak{m}$.

Therefore we assume that some coefficient of f_2 does not lie in $\mathfrak{m}$ and so is a unit since R

is local. We write

$$\begin{aligned} f_1(x) &= x^d + a_{d-1}x^{d-1} + \ldots + a_0 \quad && \text{with } a_i \in R, \\ f_2(x) &= \qquad\qquad b_s x^s + \ldots + b_0 \quad && \text{with } b_i \in R, s \leq d-1, \end{aligned}$$

so that some b_i is a unit. Let I be the ideal generated by all the leading coefficients of polynomials $h_1 f_1 + h_2 f_2$ of degree $\leq d-1$. Then I contains all the coefficients b_i. This can be proved by induction, we have trivially that $b_s \in I$, with the linear combination $p_{s-1}(x) = x^{d-s} f_2(x) - b_s f_1(x) = (b_{s-1} + b_s a_{d-1})x^{d-1} + \ldots$ follows $b_{s-1} \in I$, with $p_{s-2}(x) = x p_{s-1}(x) - (b_{s-1} + b_s a_{d-1}) f_1(x)$ we get $b_{s-2} \in I$, and proceeding in this way we can obtain that $b_i \in I$ for $0 \leq i \leq s$.

Therefore $I = R$, and there exists a polynomial $h_1 f_1 + h_2 f_2$ of degree $\leq d-1$ and leading coefficient 1. By row operations, we may now get a polynomial of degree $\leq d-1$ and leading coefficient 1 as some component in the i-th position for $i \neq 1, 2$. Finally, by induction, we may assume that $d = 0$ in which case the theorem is trivial and this concludes the proof. ■

Over a ring R, for two column vectors f and g we write $f \sim_{GL_r(R)} g$ (or just $f \sim g$) if there exists $M \in GL_r(R)$ such that

$$f = Mg,$$

and we say that f is **equivalent to** g **over** R. The previous theorem implies that over a local ring $(R, \mathfrak{m})$, a unimodular vector $f \in R[x]^r$ with one component having leading coefficient 1 is $R[x]$-equivalent to the elementary vector $e_1 = (1, 0, \ldots, 0)^t$.

Corollary 2.26. *Let $(R, \mathfrak{m})$ be a local ring. Let f be a unimodular vector in $R[x]^r$ with some component having leading coefficient* 1. *Then $f(x) \sim f(0)$ over $R[x]$.*

Proof. We have that necessarily $f(0) \in R^r$ has some component not inside $\mathfrak{m}$ and so a unit. Therefore, $f(x) \sim e_1 \sim f(0)$ over $R[x]$.

■

Lemma 2.27. *Let R be an integral domain, and let S be a multiplicative subset in R. Let x, y be independent variables. If $f(x) \sim f(0)$ over $R_S[x]$, then there exists $c \in S$ such that $f(x + cy) \sim f(x)$ over $R[x, y]$.*

Proof. Let $M \in GL_r(R_S[x])$ be such that $f(x) = M(x) f(0)$. Then $M(x)^{-1} f(x) = f(0)$ is constant, and thus invariant under the substitution $x \mapsto x + y$. We define

$$G(x, y) = M(x)M(x + y)^{-1} \in R_S[x, y].$$

Then $G(x, y)f(x + y) = M(x)M(x + y)^{-1}f(x + y) = M(x)f(0) = f(x)$. By definition we have $G(x, 0) = M(x)M(x)^{-1} = I$, then we can make

$$G(x, y) = I + yH(x, y),$$

with $H(x, y) \in R_S[x, y]$. We can clear denominators by choosing some $c \in S$ such that $cH \in R[x, y]$, then $G(x, cy)$ has coefficients in R. Since $det(M(x))$ is a constant in R_S then $det(M(x + cy))$ is equal to this same constant, and $det(G(x, cy)) = det(M(x))det(M(x + cy))^{-1} = 1$. Therefore $G(x, cy) \in GL_r(R[x, y])$ and $G(x, cy)f(x + cy) = f(x)$.

■

Theorem 2.28. *Let R be an entire ring, and let f be a unimodular row in $R[x]^r$, such that one component has leading coefficient 1. Then $f(x) \sim f(0)$ over $R[x]$.*

Proof. Let J denote the set of elements $c \in R$ such that $f(x + cy) \sim f(x)$ over $R[x, y]$. If $c_1, c_2 \in J$ and $a \in R$, then $f(x + cay) \sim f(x)$ over $R[x, ay]$ (so also over $R[x, y]$) and $f(x + (c_1 + c_2)y) \sim f(x + c_1y) \sim f(x)$ over $R[x, y]$. Therefore J is an ideal.

Let $\mathfrak{p}$ be an arbitrary prime ideal in R. By *Corollary* 2.26 we have that $f(x) \sim f(0)$ over $R_{\mathfrak{p}}[x]$, and by *Lemma* 2.27 there exists some $c \in R \setminus \mathfrak{p}$ such that $f(x + cy) \sim f(x)$ over $R[x, y]$. Hence J is not contained in any maximal ideal, and we get that $J = (1)$. Therefore there exists an invertible matrix $M(x, y)$ over $R[x, y]$ such that

$$f(x + y) = M(x, y)f(x).$$

Since $det(M(x, y))$ is a unit in R then it does not depend on x neither y, and the substitution $x = 0$ maintains the matrix invertible. So we get

$$f(y) = M(0, y)f(0),$$

and we rename y by x. ■

In one of the steps for proving *Noether Normalization Theorem* we normally show that for any polynomial $p(x_1, \dots, x_n) \in \mathbb{K}[x_1, \dots, x_n]$ with the change of variables

$$y_n = x_n, \qquad y_i = x_i - x_i^{r_i}, \tag{2.7}$$

for some suitable r_i's, we can get a new polynomial $q(y_1, \dots, y_n) \in \mathbb{K}[y_1, \dots, y_n]$ such that $p(x_1, \dots, x_n) = q(y_1, \dots, y_n)$ and the leading coefficient with respect to y_n belongs to the field $\mathbb{K}$.

Theorem 2.29. *Let $\mathbb{K}$ be a field and let f be a unimodular vector in $\mathbb{K}[x_1, \dots, x_n]^r$. Then f has the unimodular extension property.*

Proof. We proceed by induction on n. In the case $n = 1$ we have that $\mathbb{K}[x]$ is an Euclidean domain, so iteratively for $f = (f_1, \dots, f_r)$ we can take the polynomial with smallest degree into the first position and apply the division algorithm to the other positions, and repeating this process we can transform f into e_1 since $gcd(f_1, \dots, f_r) = 1$.

Therefore we assume that $n \geq 2$. Now we see f as a polynomial vector in $\mathbb{K}[x_1, \dots, x_{n-1}][x_n]$ and making a substitution like in 2.7 we can get a polynomial vector $g(y_1, \dots, y_n)$ such that

$$f(x_1, \dots, x_n) = g(y_1, \dots, y_n)$$

and has one component with leading coefficient 1 (actually a unit, but that's the same to our purposes).

From *Theorem* 2.28 there exist an invertible matrix $N(y_1, \dots, y_n) \in \mathbb{K}[y_1, \dots, y_n]$ such that

$$g(y_1, \dots, y_n) = N(y_1, \dots, y_n) g(y_1, \dots, y_{n-1}, 0)$$

and $g(y_1, \dots, y_{n-1}, 0)$ is unimodular. Therefore from the inductive hypothesis we have that

$$g(y_1, \dots, y_n) = M(y_1, \dots, y_n) e_1$$

with M invertible, and a substitution back to the variables x_i's gives the result

$$f(x_1, \dots, x_n) = M(x_1 - x_1^{r_1}, \dots, x_{n-1} - x_{n-1}^{r_{n-1}}, x_n) e_1.$$

■

Theorem 2.30. *Let M be a stably free module over $R = \mathbb{K}[x_1, \dots, x_n]$, then M is free.*

Proof. By definition we have $M \oplus R^s = R^r$ for some $r, s \in \mathbb{N}$. Since $(M \oplus R^{s-1}) \oplus R = R^r$, we can proceed by induction and only analyze the case $s = 1$.

Therefore we assume $M \oplus R = R^r$ and we shall prove that M is free. Let

$$\pi : R^r \to R$$

be the projection map induced from the direct sum $M \oplus R = R^r$. We choose u_1 as the generator of R inside $M \oplus R = R^r$ with $\pi(u_1) = 1$, then we have that $u_1 = (a_{11}, a_{21}, \dots, a_{n1})^t$ is unimodular.

From *Theorem* 2.29 we find an invertible matrix $F \in R^{r\times r}$ with u_1 as first column. Let

$$u_j = Fe_j \quad \text{for} \quad j = 1\dots, n,$$

where e_j is the j-th unit column vector. Since F induces an automorphism over R^r, we have that $\{u_1, u_2, \dots, u_r\}$ is a basis for R^r.

For $i \geq 2$ we define

$$w_i = u_i - \pi(u_i)u_1,$$

then $\{u_1, w_2, \dots, w_r\}$ is also a basis for R^r and $w_i \in M$ because $\pi(w_i) = 0$. Therefore we get that $\{w_2, \dots, w_r\}$ is a basis for the now free R-module M. ■

We finally end this section with the promised theorem

Theorem 2.31. ***(Quillen-Suslin)*** *Every f.g. projective module over $\mathbb{K}[x_1, \dots, x_n]$ is free.*

Proof. By *Theorem* 2.23 f.g. projective $\mathbb{K}[x_1, \dots, x_n]$-module is stably free. Then from *Theorem* 2.30 every stably free $\mathbb{K}[x_1, \dots, x_n]$-module is free. ■

2.3 The Auslander-Buchsbaum formula

This section discusses some interesting results for Noetherian local rings and throughout this section R will always denote $(R, \mathfrak{m}, \mathbb{K})$, i.e., a local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{K}$.

In the case of local rings (and graded, as we will see later) we can take advantage of a very special type of resolutions: *"minimal free resolutions"*. As the name suggests, now in the *Construction* 1.2 rather than taking an arbitrary set of generators, we instead take in every step a minimal set of generators. Making this process we obtain a *"minimal free resolution"*

$$F: \quad \dots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0.$$

From *Theorem* 1.12 we know that taking a minimal system of generators is equivalent to the condition $Im(d_i) \subset \mathfrak{m}F_{i-1}$ for $i \geq 1$. Therefore we can make the following definition

Definition 2.32. *Let* $(R, \mathfrak{m}, \mathbb{K})$ *be a local ring and* M *be an* R*-module. A free resolution*

$$F: \quad \dots \xrightarrow{d_{n+1}} F_n \xrightarrow{d_n} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0$$

is said to be ***minimal*** *if* $Im(d_i) \subset \mathfrak{m}F_{i-1}$ *for* $i \geq 1$.

Theorem 2.33. *Let* $(R, \mathfrak{m}, \mathbb{K})$ *be a local ring and* M *be a finitely generated nonzero* R*-module, then* $pd_R(M)$ *is the length of every minimal free resolution of* M*. Furthermore,* $pd_R(M)$ *is the biggest integer* i *for which* $Tor_i^R(\mathbb{K}, M) = Tor_i^R(M, \mathbb{K}) \neq 0$.

Proof. Since Tor is independent of the chosen projective resolution we have that

$$Tor_{j+1}^R(M, \mathbb{K}) = 0 \text{ for } j \geq pd_R(M). \tag{2.8}$$

Now suppose that

$$F: \quad 0 \to F_n \xrightarrow{d_n} \dots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0$$

is a projective resolution of length n. If i is the biggest integer for which $Tor_i^R(M, \mathbb{K}) \neq 0$, then from 2.8 we have $n \geq pd_R(M) \geq i$. But if F is a minimal free resolution then the differentials in the complex $F \otimes_R \mathbb{K}$ are 0,

$$F \otimes_R \mathbb{K}: \quad 0 \to F_n \xrightarrow{0} \dots \xrightarrow{0} F_1 \xrightarrow{0} F_0.$$

Thus $Tor_i^R(M, \mathbb{K}) = F_i \otimes_R \mathbb{K} \neq 0$ if and only if $F_i \neq 0$, which gives $i = n$. Therefore we have that $pd_R(M)$ is equal to the length of any minimal free resolution, which is also equal to the biggest integer i such that $Tor_i^R(M, \mathbb{K}) \neq 0$. ■

With this previous theorem we get a type of *"Quillen-Suslin Theorem"* 2.31 in the case of local rings.

Corollary 2.34. *Let $(R, \mathfrak{m}, \mathbb{K})$ be a local ring and M be a finitely generated projective module, then M is free.*

Proof. We have $pd_R(M) = 0$, then with the previous theorem we have a minimal free resolution of the form $0 \to F \to M \to 0$. ■

The following theorem, *"the Auslander-Buchsbaum formula"* is very important from a theoretical point of view and an effective instrument for the computation of the depth of a module.

Theorem 2.35. ***(Auslander-Buchsbaum)*** *Let $(R, \mathfrak{m}, \mathbb{K})$ be a Noetherian local ring, and $M \neq 0$ a finite R-module. If $pd_R(M)$ is finite, then*

$$pd_R(M) + depth(\mathfrak{m}, M) = depth(\mathfrak{m}, R),$$

or just

$$pd_R(M) + depth(M) = depth(R).$$

Proof. We proceed by induction on the projective dimension of M. If $pd_R(M) = 0$ then M is free and the result $depth(M) = depth(R)$ follows because M is just several copies of R.

If $pd_R(M) > 0$, the we make the first step of taking a minimal free resolution

$$F: \quad 0 \to N \xrightarrow{\varphi} F \to M \to 0,$$

i.e., $Im(\varphi) \subset \mathfrak{m}F$. By *Theorem* 2.33 we have $pd_R(N) = pd_R(M) - 1$, so we may apply the theorem inductively to N. Writing $d = depth(N)$, we must show $depth(M) = d - 1$ in order to maintain the equality.

We shall explode the characterization of depth by the Koszul complex (*Theorem* 1.35). Let $\mathbf{x} = (x_1, \ldots, x_n)$ be a set of generators of the maximal ideal $\mathfrak{m}$. We apply the *Proposition* 1.34 to obtain the long exact sequence

$$\ldots \to H_i K(\mathbf{x}, N) \to H_i K(\mathbf{x}, F) \to H_i K(\mathbf{x}, M) \to H_{i-1} K(\mathbf{x}, N) \to \ldots .$$

Since $pd_R(F) = 0$ by the inductive hypothesis we have that $depth(F) = depth(R) \geq d$. From *Theorem* 1.35 follows that $H_j K(\mathbf{x}, N) = 0$ and $H_j K(\mathbf{x}, F) = 0$ for $j > n - d$. Thus for any $j > n-d+1$ we have the exact sequence

$$0\ (= H_jK(\mathbf{x}, F)) \to H_jK(\mathbf{x}, M) \to 0\ (= H_{j-1}(\mathbf{x}, N)),$$

and $H_jK(\mathbf{x}, M) = 0$.

To prove that $depth(M) = d-1$, again by *Theorem* 1.35, it suffices to show that

$$H_{n-d+1}K(\mathbf{x}, M) \neq 0.$$

Since $depth(N) = d$ we know that $H_{n-d}K(\mathbf{x}, N) \neq 0$, and from the exact sequence

$$H_{n-d+1}K(\mathbf{x}, M) \to H_{n-d}K(\mathbf{x}, N) \xrightarrow{\Phi} H_{n-d}K(\mathbf{x}, F)$$

will be more that enough to prove that the induced map Φ from φ, is the zero map.

If $pd_R(N) > 0$, by the induction hypothesis we have $d < depth(R)$, so that in fact $H_{n-d}K(\mathbf{x}, F) = 0$. Otherwise $pd_R(N) = 0$, so that N is free, and we have

$$H_{n-d}K(\mathbf{x}, N) = N \otimes H_{n-d}K(\mathbf{x}),$$
$$H_{n-d}K(\mathbf{x}, F) = F \otimes H_{n-d}K(\mathbf{x}).$$

In this case the induced map Φ can be identified as $\varphi \otimes id$. We know that $Im(\varphi) \subset \mathfrak{m}F$ and from *Theorem* 1.31 *(ii)* we have that $\mathfrak{m}$ annihilates $H_{n-d}K(\mathbf{x})$, thus the tensor product $\varphi \otimes id$ is the zero map. ■

Chapter 3

Applying syzygies

In the article [1] is proved that any *rational surface* has a *μ-basis.* That strong result obtained by *Falai Chen*, *David Cox*, and *Yang Liu*, geometrically means that any *rational surface* is the intersection of *three moving planes without extraneous factors.* There, is stated: *"This is an unexpected result, for after ten years of exploration, researchers in the geometric modelling community generally believed that this was not true".*

In [1] there are left several questions of interest for further research and better understanding. During this chapter we shall address the question:

- **What can be said about the degrees of the polynomials in a minimal μ-basis?**

We will try to make a more or less detailed exposition of the bound we found for the degree of the polynomials in a minimal μ-basis for any rational surface. This chapter could be seen as our small result in this rich theory of syzygies and also it will serve the purpose of giving small introduction to the study of the graded polynomial ring $R = \mathbb{K}[x_1, \dots, x_n]$.

3.1 The μ-basis of a rational surface

In this section we will discuss the existence of a *μ-basis* for any *rational surface*, because it turns out that a principal ingredient is dealing with our syzygies!. We give a different proof for the result about syzygies stated there, which we also generalize.

Our goal here is to roughly give the principal definitions to prove the *Theorem 3.1* in [1] and use our different approach with syzygies.

Definition 3.1. *A rational surface in homogeneous form is defined by*

$$P(s,t) = (a(s,t), b(s,t), c(s,t), d(s,t)) \tag{3.1}$$

where $a, b, c, d \in \mathbb{R}[s,t]$ are bi-degree (m,n) polynomials and $gcd(a,b,c,d) = 1$. Where the rational surface is properly parametrized, i.e., the map

$$(s,t) = \left(\frac{a(s,t)}{d(s,t)}, \frac{b(s,t)}{d(s,t)}, \frac{c(s,t)}{d(s,t)} \right)$$

is birational.

Definition 3.2. *A moving plane is a quadruple $(A(s,t), B(s,t), C(s,t), D(s,t)) \in \mathbb{R}[s,t]^4$ such that*

$$A(s,t)\frac{a(s,t)}{d(s,t)} + B(s,t)\frac{b(s,t)}{d(s,t)} + C(s,t)\frac{c(s,t)}{d(s,t)} + D(s,t) = 0 \tag{3.2}$$

for all $s, t \in \mathbb{R}$.

From the previous definition we see that a *moving plane* is a collection of planes parametrized by polynomials, that for each $s, t \in \mathbb{R}$ the point $\left(\frac{a(s,t)}{d(s,t)}, \frac{b(s,t)}{d(s,t)}, \frac{c(s,t)}{d(s,t)}\right)$ of the rational surface is contained in the corresponding plane to (s,t).

We denote the collection of moving planes of the rational surface $P(s,t)$ as $L_{s,t} \subset \mathbb{R}[s,t]^4$. The equation 3.2 is equivalent to

$$A(s,t)a(s,t) + B(s,t)b(s,t) + C(s,t)c(s,t) + D(s,t)d(s,t) = 0$$

for all $s, t \in \mathbb{R}$. Thus the polynomial above is the zero polynomial and the collection $L_{s,t}$ is equal to the *0-th syzygy* K_0 of the $\mathbb{R}[s,t]$-module(ideal) generated by the polynomials $\{a(s,t), b(s,t), c(s,t), d(s,t)\}$, that is $I = (a,b,c,d) \subset \mathbb{R}[s,t]$. Thus we have the following exact sequence

$$0 \to K_0 (= L_{s,t}) \to \mathbb{R}[s,t]^4 \xrightarrow{[a,b,c,d]} I \to 0. \tag{3.3}$$

In [1] is used the notation $Syz(a,b,c,d)$ to denote the *0-th syzygy* K_0, which seems appropriate now to use because we want to stress that the previous exact sequence depends on the generators $\{a,b,c,d\}$, and is not a general construction like 1.2 where we pointed out that was not important the generators chosen.

Definition 3.3. *Let* $\mathbf{p} = (p_1, p_2, p_3, p_4), \mathbf{q} = (q_1, q_2, q_3, q_4), \mathbf{r} = (r_1, r_2, r_3, r_4) \in L_{s,t}(=$

$K_0 = Syz(a,b,c,d))$ *be three moving planes such that*

$$[\mathbf{p},\mathbf{q},\mathbf{r}] = \alpha P(s,t) \tag{3.4}$$

for some constant $\alpha \in \mathbb{R}$. *Then* $\mathbf{p},\mathbf{q},\mathbf{r}$ *are said to be a* $\mu -$ **basis** *of the rational surface 3.1. Where* $[\mathbf{p},\mathbf{q},\mathbf{r}]$ *is defined as the outer product*

$$[\mathbf{p},\mathbf{q},\mathbf{r}] = \left(\begin{vmatrix} p_2 & p_3 & p_4 \\ q_2 & q_3 & q_4 \\ r_2 & r_3 & r_4 \end{vmatrix}, - \begin{vmatrix} p_1 & p_3 & p_4 \\ q_1 & q_3 & q_4 \\ r_1 & r_3 & r_4 \end{vmatrix}, \begin{vmatrix} p_1 & p_2 & p_4 \\ q_1 & q_2 & q_4 \\ r_1 & r_2 & r_4 \end{vmatrix}, - \begin{vmatrix} p_1 & p_1 & p_3 \\ q_1 & q_2 & q_3 \\ r_1 & r_2 & r_3 \end{vmatrix} \right).$$

The previous condition means that the rational surface $P(s,t)$ can be represented as the intersection of three moving planes $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$ without extraneous factors.

Now we state the following result about syzygies (*Proposition 2.1* in [1]).

Proposition 3.4. *Let* $a,b,c,d \in R[s,t]$ *be four relatively prime polynomials. Then the syzygy module* $Syz(a,b,c,d)$ *is a free module of rank* 3.

Proof. The proof of being free will be given in the next section and the proof of having rank 3 can be found in [1]. ∎

In the following theorem is proved the existence of a μ-basis for any rational surface and we will see that the previous result on syzygies is the fundamental base that reduces all to linear algebra.

Theorem 3.5. *For any rational surface defined as in 3.1, there always exist three moving planes* $\mathbf{p},\mathbf{q},\mathbf{r}$ *such that 3.4 holds.*[1]

Proof. Using that a,b,c,d are coprime then by *Proposition* 3.4 the $R[s,t]$-module $Syz(a,b,c,d)$ is a free module of rank 3, and we choose a basis $\{\mathbf{p},\mathbf{q},\mathbf{r}\}$. Then we shall prove there is a linear dependence between $[\mathbf{p},\mathbf{q},\mathbf{r}]$ and $P(s,t)$ (as elements in a module), i.e., there exist polynomials $f,g \in \mathbb{R}[s,t]$ such that $f[\mathbf{p},\mathbf{q},\mathbf{r}] = gP(s,t)$, and we also may assume that

[1]See [1] for a different argument in proving the linear dependence between $[\mathbf{p},\mathbf{q},\mathbf{r}]$ and $P(s,t)$.

$gcd(f,g)=1$. For that we write the matrix

$$\begin{pmatrix} [\mathbf{p},\mathbf{q},\mathbf{r}] \\ P(s,t) \end{pmatrix} = \left(\underset{a}{\begin{vmatrix} p_2 & p_3 & p_4 \\ q_2 & q_3 & q_4 \\ r_2 & r_3 & r_4 \end{vmatrix}} \quad - \underset{b}{\begin{vmatrix} p_1 & p_3 & p_4 \\ q_1 & q_3 & q_4 \\ r_1 & r_3 & r_4 \end{vmatrix}} \quad \underset{c}{\begin{vmatrix} p_1 & p_2 & p_4 \\ q_1 & q_2 & q_4 \\ r_1 & r_2 & r_4 \end{vmatrix}} \quad - \underset{d}{\begin{vmatrix} p_1 & p_1 & p_3 \\ q_1 & q_2 & q_3 \\ r_1 & r_2 & r_3 \end{vmatrix}} \right),$$

and if we prove that every 2×2-minor vanishes then we get the expected result. For example if we take the first minor we get

$$b\begin{vmatrix} p_2 & p_3 & p_4 \\ q_2 & q_3 & q_4 \\ r_2 & r_3 & r_4 \end{vmatrix} + a\begin{vmatrix} p_1 & p_3 & p_4 \\ q_1 & q_3 & q_4 \\ r_1 & r_3 & r_4 \end{vmatrix} = \begin{vmatrix} b & -a & 0 & 0 \\ p_1 & p_2 & p_3 & p_4 \\ q_1 & q_2 & q_3 & q_4 \\ r_1 & r_3 & r_3 & r_4 \end{vmatrix} = 0.$$

The last equality follows from the fact $(b,-a,0,0)\in Syz(a,b,c,d)$ and $\mathbf{p},\mathbf{q},\mathbf{r}$ form a basis for $Syz(a,b,c,d)$. In the same way we can compute that all minors vanish.

Since $gcd(f,g)=1$ and $gcd(a,b,c,d)=1$, we may assume $f=1$. Using that $(-b,a,0,0)$, $(-c,0,a,0)$ and $(-d,0,0,a)$ belongs to $Syz(a,b,c,d)$, there exist polynomials $h_{i,j}\in\mathbb{R}[s,t]$ such that

$$\begin{aligned}
(-b,a,0,0) &= h_{11}\mathbf{p}+h_{12}\mathbf{q}+h_{13}\mathbf{r},\\
(-c,0,a,0) &= h_{21}\mathbf{p}+h_{22}\mathbf{q}+h_{23}\mathbf{r},\\
(-d,0,0,a) &= h_{31}\mathbf{p}+h_{32}\mathbf{q}+h_{33}\mathbf{r}.
\end{aligned}$$

Forming the outer product of the above three vector polynomials, one has

$$a^2P(s,t)=det(h_{ij})[\mathbf{p},\mathbf{q},\mathbf{r}]=det(h_{ij})gP(s,t).$$

Thus we have $g|a^2$, and similarly we can get $g|b^2$, $g|c^2$ and $g|d^2$. Hence $g|gcd(a,b,c,d)=1$, g is a constant and we get the equality

$$[\mathbf{p},\mathbf{q},\mathbf{r}]=\alpha P(s,t)$$

for some $\alpha\in\mathbb{R}$. ■

The term *"without extraneous factors"* means that we can achieve the $[\mathbf{p},\mathbf{q},\mathbf{r}]=\alpha P(s,t)$ with $\alpha\in\mathbb{R}$, because we can always get some vectors $\mathbf{p},\mathbf{q},\mathbf{r}$ that achieve the equality *"with extraneous factors"*, that is $[\mathbf{p}, \mathbf{q}, \mathbf{r}] = gP(s,t)$ for some $g \in \mathbb{R}[s,t]$. For instance, if $P = (a,b,c,d)$, then we make

$$\mathbf{p} = (-d, 0, 0, a)$$
$$\mathbf{q} = (0, -d, 0, b)$$
$$\mathbf{r} = (0, 0, -d, c)$$

and follows $[\mathbf{p}, \mathbf{q}, \mathbf{r}] = (ad^2, bd^2, cd^2, d^3) = d^2(a,b,c,d) = d^2P(s,t)$.

Surprisingly enough, there is a $1-1$ relationship between a **μ-basis** and a basis for the syzygy module $Syz(a,b,c,d)$ given in the following form:

- (*Corollary 3.1*, [1]) $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$ form an μ-basis if and only if $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$ are a basis of $Syz(a,b,c,d)$.

Definition 3.6. *$\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$ are said to form a **minimal μ-basis** of the rational surface 3.1 if*

(i) among all the triples $\mathbf{p_1}$, $\mathbf{q_1}$ and $\mathbf{r_1}$ satisfying 3.4, $deg_t(\mathbf{p}) + deg_t(\mathbf{q}) + deg_t(\mathbf{r})$ is the smallest, and

(ii) among all triples $\mathbf{p_1}$, $\mathbf{q_1}$ and $\mathbf{r_1}$ satisfying 3.4 and item (i), $deg_s(\mathbf{p})+deg_s(\mathbf{q})+deg_s(\mathbf{r})$ is the smallest.

Here, $deg_t(\mathbf{p}) = max_{1\leq i\leq 4}(deg_t(p_i))$ when $\mathbf{p} = (p_1, p_2, p_3, p_4)$, and $deg_t(\mathbf{q})$, $deg_t(\mathbf{r})$, $deg_s(\mathbf{p})$, $deg_s(\mathbf{q})$, $deg_s(\mathbf{r})$ are defined similarly.

Our approach to answer the question

- **What can be said about the degrees of the polynomials in a minimal μ-basis?,**

will be to prove the existence of a basis for the syzygy module $Syz(a,b,c,d)$, where the polynomials in this basis are bounded in terms of the maximal degree $max(deg(a), deg(b), deg(c), deg(d))$ (deg denotes the maximal total degree in the variables s and t).

3.2 The freeness of the syzygies

Proving the freeness of $Syz(a, b, c, d)$ is an important step in [1] to show the existence of a μ-basis. In this section we give a different proof for that statement, which we also generalize because we will need the case of three variables after homogenizing the ideal $I = (a, b, c, d)$.

Statement in the Appendix of [1]: Let $\mathbb{K}$ be a field and $R = \mathbb{K}[s, t]$. For any $f_1, \ldots, f_k \in R$, the syzygy module $Syz(f_1, \ldots, f_k) = \{(h_1, \ldots, h_k) \in R^k \mid h_1 f_1 + \ldots + h_k f_k \equiv 0\}$ is a free module.

We claim that for any $n \geq 2$ and any ideal in $\mathbb{K}[x_1, \ldots, x_n]$ the (n-2)-th syzygy K_{n-2} is free (for us the first syzygy is the 0-th syzygy, although there are other sources that start counting in 1). For $n = 1$ is not needed because any nonzero ideal in $k[x]$ is principal, therefore is isomorphic to $k[x]$ and clearly free. For $n = 2$ is just the previous statement, because by Hilbert Basis Theorem any ideal is finitely generated, so for any ideal $I = (f_1, \ldots, f_k)$ we have that $K_0 = Syz(f_1, \ldots, f_k)$ is free. For $n = 3$ we have that K_1 is free, i.e., the syzygy of $Syz(f_1, \ldots, f_k)$ is free.

We shall see that the proof will be rather short by quoting from previous sections. In some sense the next theorem is like the Hilbert's Syzygy Theorem in a sharped way for modules inside the polynomial ring, i.e., ideals.

Proposition 3.7. *Let $\mathbb{K}$ be a field and I an ideal in $R = \mathbb{K}[x_1, \ldots, x_n]$ then we have $pd_R(I) \leq n - 1$.*

Proof. Take the exact sequence

$$0 \to I \to R \to R/I \to 0.$$

Using *Theorem* 1.19 for any R-module N we get the exact sequence

$$\ldots \to Ext^n_R(R, N) \to Ext^n_R(I, N) \to Ext^{n+1}_R(R/I, N) \to \ldots .$$

By *Corollary* 2.6 we know that $pd_R(R/I) \leq n$, then applying *Theorem* 1.43 we get $Ext^{n+1}_R(R/I, N) = 0$. We always have $Ext^n_R(R, N) = 0$ (for $n \geq 1$), thus we transform the previous exact sequence into

$$\ldots \to 0 \to Ext^n_R(I, N) \to 0 \to \ldots,$$

so $Ext^n_R(I, N) = 0$. Finally, again by *Theorem* 1.43 we get $pd_R(I) \le n-1$. ■

Now we are ready to prove our promised generalization of *Proposition* 3.4 in the following theorem.

Theorem 3.8. *Let $\mathbb{K}$ be a field and I be an ideal in $R = \mathbb{K}[x_1, \ldots, x_n]$, with $n \ge 2$. Then for any projective resolution of I composed of f.g. modules, the corresponding (n-2)th syzygy K_{n-2} is free.*

Proof. Let $\ldots \xrightarrow{d_n} P_{n-1} \xrightarrow{d_{n-1}} P_{n-2} \xrightarrow{d_{n-2}} P_{n-3} \xrightarrow{d_{n-3}} \ldots \xrightarrow{d_1} P_0 \xrightarrow{d_0} I \to 0$ be a projective resolution of I where each P_i is a f.g. projective module. From *Quillen-Suslin Theorem* 2.31 we know that in this case the modules P_i are actually free.

With the obtained bound $pd_R(I) \le n-1$ and *Corollary* 1.44, we get that the (n-2)-th syzygy $K_{n-2} = Ker(d_{n-2})$ is a projective module. Using P_{n-2} is f.g. and R Noetherian we get that P_{n-2} is a Noetherian module, then $K_{n-2} \subset P_{n-2}$ is a f.g. module. Finally, by the *Quillen-Suslin Theorem* 2.31 the (n-2)-th syzygy K_{n-2} is a free $\mathbb{K}[x_1, \ldots, x_n]$-module. ■

Remark 3.9. *In the previous proof we only need that P_{n-2} is f.g. to get that K_{n-2} is free. Here we see that for the special case $n = 2$ we can take a projective resolution for $I = (f_1, \ldots, f_k)$ as*

$$\ldots \to \mathbb{R}[s,t]^k \xrightarrow{[f_1,\ldots,f_k]} I \to 0,$$

then $K_0 = Syz(f_1, \ldots, f_k)$ is a free $\mathbb{R}[s,t]$-module.

Therefore, we get the exact sequence

$$0 \to K_0 = Syz(f_1, \ldots, f_k) \xrightarrow{i} \mathbb{R}[s,t]^k \xrightarrow{[f_1,\ldots,f_k]} I \to 0$$

with $Syz(f_1, \ldots, f_k)$ as a free module.

Remark 3.10. *We have given a specific reference for the Hilbert Syzygy Theorem as Corollary 2.6, because the standard proof using the Koszul complex only works in the graded case. For instance, in the excellent book [3] by Eisenbud the proof of Hilbert Syzygy Theorem for the non graded case says:*

- *(Corollary 19.8 in [3]) "Every finitely generated module over $\mathbb{K}[x_1, \ldots, x_n]$ has a **finite free resolution**".*

Actually if we go through the proof of this Corollary, we see that can only be concluded the existence of a resolution of length $\leq n+1$*, and this result is obtained after a process of "homogenizing" the initial module.*

Using a computer algebra system like *Macaulay2* ([2], [4]) we can check the veracity of all kinds of results we expect to be true or that we think we have proven. To test our previous result, we programmed the following simple code to see if we could find an ideal with projective dimension equal to *numVar*, i.e., *numVar* is n in the polynomial ring $\mathbb{K}[x_0, \ldots, x_{n-1}]$.

```
numVar = 3
R = QQ[vars (0..(numVar-1))]

constructRandomIdeal = (numGen, maxDeg) -> (
    I := {};
    for i from 1 to numGen do (
      polynom := random(maxDeg,R);
      I = append(I, polynom);
    );
    ideal I
  )

checkIneq = (numIter, numGen, maxDeg) -> (
    J := 0;
    for i from 1 to numIter do (
      I := constructRandomIdeal(numGen, maxDeg);
      n := pdim module I;
      if n == numVar then (
        J = I;
        break;
      );
    );
    J
  )
```

The implemented function **checkIneq** tries to find an ideal with projective dimension equal to **numVar** and generated by **numGen** polynomials of degree at most **maxDeg**; and the function tries to do this process **numIter** times. We have run the previous function *checkIneq* with several configurations and never has been able to find an ideal $I \in \mathbb{K}[x_0, \ldots, x_{n-1}]$ with $pd(I) = n$. Therefore computations made in *Macaulay2* agree with our given proof.

We could play a little more with *Macaulay2* and using its functionalities we can implement a very short algorithm to compute the projective dimension of a module. From *Corollary* 1.45 we know that the "obvious" method of computing one kernel (syzygy) after another will always give the projective dimension of a module. The following simple algorithm does this iterative process and with it computes the projective dimension of a module.

```
reduceM = M -> trim minimalPresentation image gens gb M

PDIM = M -> (
     K := reduceM image presentation reduceM M;
     n := 0;
     while K != 0 do (
          K = reduceM image presentation K;
          n = n + 1;
     );
     n
  )
```

This algorithm successively evaluates the function *presentation* that returns a map ϕ with $Coker(\phi) = M$, then the *image* of ϕ will successively return the *syzygies*. In the function *reduceM* we tried to use several functionalities of *Macaulay2* to reduce modules and check when we get the first *syzygy* that vanishes.

3.3 The outline of our proof

In this section we describe how we are going to prove the existence of a basis with a certain bound in terms of the maximal degree in the polynomials a, b, c and d. For notational purposes from now on, we assume that $a_1, a_2, a_3, a_4 \in \mathbb{R}[s,t]$ are the polynomials defining the rational surface 3.1 and that $d = max_{1 \leq i \leq 4}(deg(a_i))$. Therefore we will try to solve the following problem for the rest of this document.

- Given an ideal $I \subset \mathbb{R}[s,t]$ defined by $I = (a_1, a_2, a_3, a_4)$, with $d = max_{1 \leq i \leq 4}(deg(a_i))$, and $gcd(a_1, a_2, a_3, a_4) = 1$. Then find a basis of $Syz(a_1, a_2, a_3, a_4)$ with polynomials bounded in degree by certain formula in terms of d.

For us is not clear at all how to define a bound in the "degree of the polynomials" if we are working with modules over the polynomial ring $\mathbb{R}[s,t]$. Instead we will try to reduce the problem to a graded case where we can exploit the structure of the grading.

Given the ideal $I = (a_1, a_2, a_3, a_4) \subset \mathbb{R}[s,t]$, then we define the homogeneous ideal $\hat{I} = (b_1, b_2, b_3, b_4)$ with

$$b_i = u^d a_i(\frac{s}{u}, \frac{t}{u}) \in \mathbb{R}[s,t,u]. \tag{3.5}$$

For the ideal $\hat{I} \subset \mathbb{R}[s,t,u]$ we can find a graded free resolution that starts as

$$\ldots \to \mathbb{R}[s,t,u]^4 \xrightarrow{[b_1,b_2,b_3,b_4]} \hat{I} \to 0,$$

we can continue this process of finding a graded free resolution until the step

$$0 \to K_1 \to F_1 \to \mathbb{R}[s,t,u]^4 \xrightarrow{[b_1,b_2,b_3,b_4]} \hat{I} \to 0,$$

and from *Theorem* 3.8 we know that the first syzygy K_1 is a free $\mathbb{R}[s,t,u]$-module. Therefore we can assure that the ideal $\hat{I}$ has a graded free resolution of the form

$$0 \to \mathbb{R}[s,t,u]^b \to \mathbb{R}[s,t,u]^a \to \mathbb{R}[s,t,u]^4 \xrightarrow{[b_1,b_2,b_3,b_4]} \hat{I} \to 0. \tag{3.6}$$

Intuitively we could expect that if we make the substitution $u = 1$ in the previous resolution we find a free resolution (perhaps no longer graded) of the ideal $I = (a_1, a_2, a_3, a_4)$. This hunch turns out to be true and the way of state it rigorously is to say that tensoring with $\otimes_{\mathbb{R}[s,t,u]}\mathbb{R}[s,t,u]/(u-1)$ is an exact functor, for a proof of this fact one can see *Corollary 19.8* in [3] or *Proposition 1.1.5* in [6].

Finding a resolution like in 3.6 with certain "regularity" or bound for the degree of the polynomials involved in the differential maps of 3.6 will give us a resolution of I in the form

$$0 \to \mathbb{R}[s,t]^b \to \mathbb{R}[s,t]^a \to \mathbb{R}[s,t]^4 \xrightarrow{[a_1,a_2,a_3,a_4]} I \to 0,$$

with the same "regularity" or bound.

From now on we shall use the notations $S = \mathbb{R}[s,t,u]$ and $R = \mathbb{R}[s,t] \cong S/(u-1)$. There are two possible cases of 3.6 that we have to analyze:

(I) If $pd_S(\hat{I}) = 1$ then the resolution 3.6 is of the form

$$0 \to S^a \xrightarrow{d_1} S^4 \xrightarrow{[b_1,b_2,b_3,b_4]} \hat{I} \to 0,$$

and by tensoring with $\otimes_S R$ we obtain the free resolution

$$0 \to R^a \xrightarrow{d_1 \otimes_S R} R^4 \xrightarrow{[a_1,a_2,a_3,a_4]} I \to 0,$$

where we can conclude that $a = 3$ because as previously stated $Syz(a_1, a_2, a_3, a_4)$ has rank 3. So we know that $d_1 \otimes_S R \in R^{4\times 3}$ is a 4×3 matrix with entries in R and the columns of $d_1 \otimes_S R$ conform a basis of $Syz(a_1, a_2, a_3, a_4)$ as a submodule of R^4. If we find a bound for the polynomials in the entries of the matrix $d_1 \in S^{4\times 3}$, then we will get automatically a bound for the degree of the polynomials in a basis of $Syz(a_1, a_2, a_3, a_4)$ and our proof will be completed for this case.

(II) If $pd_S(\hat{I}) = 2$ then the resolution 3.6 is of the form

$$0 \to S^b \xrightarrow{d_2} S^a \xrightarrow{d_1} S^4 \xrightarrow{[b_1,b_2,b_3,b_4]} \hat{I} \to 0,$$

again by tensoring with $\otimes_S R$ we can obtain the exact sequence

$$0 \to R^b \xrightarrow{d_2 \otimes_S R} R^a \xrightarrow{d_1 \otimes_S R} Syz(a_1, a_2, a_3, a_4) \to 0.$$

We know that $Syz(a_1, a_2, a_3, a_4)$ is a free module of rank 3, thus the previous exact sequence splits and we can conclude $a = b + 3$. Unfortunately we will have to work a lot more to give a bound in this case and we will dedicate a complete section for this case.

We can easily compute various examples for the two previous cases.

Example 3.11. *Let $I = (s^2, t^2, s^2 - t^2, s^2 + t^2)$, then $pd_S(\hat{I}) = 1$ and we can find the following resolution*

$$0 \to S^3 \xrightarrow{\begin{pmatrix} -1 & 0 & -t^2 \\ 1 & -2 & s^2 \\ 1 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix}} S^4 \xrightarrow{\begin{pmatrix} s^2 & t^2 & s^2 - t^2 & s^2 + t^2 \end{pmatrix}} \hat{I} \to 0.$$

Example 3.12. *Let $I = (s^2, t^2, s^2 - 1, s^2 + 1)$, then $pd_S(\hat{I}) = 2$ and we can find the following resolution*

$$0 \to S \xrightarrow{\begin{pmatrix} 0 \\ s^2 \\ -u^2 \\ -t^2 \end{pmatrix}} S^4 \xrightarrow{\begin{pmatrix} -2 & -t^2 & -t^2 & u^2 - s^2 \\ 0 & u^2 & s^2 & 0 \\ 1 & t^2 & 0 & s^2 \\ 1 & 0 & 0 & 0 \end{pmatrix}} S^4 \xrightarrow{\begin{pmatrix} s^2 & t^2 & s^2 - u^2 & s^2 + u^2 \end{pmatrix}} \hat{I} \to 0.$$

3.4 Bounds for the regularity and the Betti numbers

This section will be devoted to find a bound for the regularity and the Betti numbers of $\hat{I}$. We will try to be more specific and rigorous than in the previous section and our main reference will be the chapter *"Graded Free Resolutions"* of [17]. For convenience we will make an exposition for $S = \mathbb{R}[s,t,u]$, although all the definitions given here work for the general case $S = \mathbb{K}[x_1, \ldots, x_n]$.

Definition 3.13. *The* ***Hilbert function*** *of a graded S-module M is denoted by $H_M : \mathbb{Z} \to \mathbb{N}$ and defined by $H_M(i) = dim_{\mathbb{R}}(M_i)$.*

Definition 3.14. *A graded free resolution of a finitely generated S-module M is an exact sequence of graded free S-modules*

$$\ldots \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} \ldots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0,$$

where each map has degree 0, i.e., $d_i((F_i)_k) \subseteq (F_{i-1})_k$.

By choosing homogeneous generators iteratively we can construct a graded free resolution for any graded finitely generated S-module.

Construction 3.15. *Given a graded finitely generated S-module M we will construct a graded free resolution of M.*

Step -1: Set $K_{-1} = M$. Choose homogeneous generators $m_1, \ldots, m_r$ of K_{-1}. Let $a_1, \ldots, a_r$ be their degrees, respectively. Set $F_0 = S(-a_1) \oplus \ldots \oplus S(-a_r)$. For $1 \leq j \leq r$ we denote by f_j the 1-generator of $S(-a_j)$. Thus, $deg(f_j) = a_j$. We define

$$\begin{aligned} d_0 : F_0 &\to K_{-1} \\ f_j &\mapsto m_j \text{ for } 1 \leq j \leq r, \end{aligned}$$

and this is a homomorphism of degree 0.

Assume by induction, that F_i and d_i are defined.

Step $i+1$: Set $K_i = Ker(d_i)$ (from Proposition 2.9 in [17], we know that $Ker(d_i)$ is a graded module). Choose homogeneous generators $l_1, \ldots, l_s$ of K_i. Let $c_1, \ldots, c_s$ be their *degrees, respectively. Set* $F_{i+1} = S(-c_1) \oplus \ldots \oplus S(-c_s)$*. For* $1 \le j \le s$ *we denote by* g_j *the* 1*-generator of* $S(-c_j)$*. Thus,* $deg(g_j) = c_j$*. We define*

$$\begin{aligned} d_{i+1} : F_{i+1} &\to K_i \subset F_i \\ g_j &\mapsto l_j \text{ for } 1 \le j \le s, \end{aligned}$$

and this is a surjective homomorphism of degree 0.

The constructed complex is exact and is just like in 1.2 but only taking some extra care for the homogeneous elements.

Example 3.16. *Let* $R = \mathbb{K}[x, y]$ *and* $J = (x^3, xy, y^5)$*, then for the module* R/J *we have the following graded free resolution*

$$0 \to R(-4) \oplus R(-6) \xrightarrow{\begin{pmatrix} y & 0 \\ -x^2 & -y^4 \\ 0 & x \end{pmatrix}} R(-3) \oplus R(-2) \oplus R(-5) \xrightarrow{\begin{pmatrix} x^3 & xy & y^5 \end{pmatrix}} R \to R/J \to 0.$$

As a consequence of the *Nakayama's lemma* (*Lemma* 1.10 for the graded case) we can define the concept of **minimal system of homogeneous generators** for any finitely generated graded S-module (*Lemma* 1.11). Using this fact we can give a **"minimal resolution"** for any module M by choosing a minimal system of generators in each step of the previous construction. Luckily, from *Theorem* 1.12 we can come up with an equivalent condition which is more easy definition to handle.

Definition 3.17. *A graded free resolution of a graded finitely generated module* S*-module is said to be* ***minimal*** *if*

$$d_{i+1}(F_{i+1}) \subseteq (s, t, u)F_i \quad \text{for all } i \ge 0.$$

This means, that no invertible elements (non-zero constants) appear in the differential matrices.

The resolution given in *Example* 3.16 is minimal, but the ones given in *Example* 3.11 and *Example* 3.12 are not minimal. Unfortunately we are interested in resolutions that are not always minimal, because we want extract information about the syzygy module $Syz(b_1, b_2, b_3, b_4)$ and in several cases $\{b_1, b_2, b_3, b_4\}$ is not a minimal system of homogeneous generators for $\hat{I}$. Therefore, this section is “aside” of our original problem and is dedicated to find some numerical invariants of $\hat{I}$ for later use.

Theorem 3.18. *(i) A graded free resolution is minimal if and only if at each step we choose a minimal system of homogeneous generators.*

(ii) A minimal free resolution is unique up to isomorphisms.

Proof. See *Theorem* 1.12 and *Theorem 7.5*, [17]. ∎

Using this convenient uniqueness we can define the Betti numbers for a graded finitely generated S-module M. For the rest of this section F_i will denote the modules in a minimal free resolution of M.

Definition 3.19. *The i'th* ***Betti number*** *of M over S is defined by*

$$\beta_i(M) = dim_{\mathbb{R}}(F_i).$$

Theorem 3.20.

$$\beta_i(M) = dim_{\mathbb{R}}(Tor_i^S(M, \mathbb{R})).$$

Proof. If we tensor the minimal free resolution F of M with $\otimes_S \mathbb{R}$ we can obtain the complex

$$F \otimes_S \mathbb{R} : \qquad \ldots \xrightarrow{0} \mathbb{R}^{\beta_i(M)} \xrightarrow{0} \ldots \xrightarrow{0} \mathbb{R}^{\beta_1(M)} \xrightarrow{0} \mathbb{R}^{\beta_0(M)}.$$

Thus we have

$$Tor_i^S(M, \mathbb{R}) \cong H_i(F \otimes_S \mathbb{R}) = \mathbb{R}^{\beta_i(M)}.$$

∎

Definition 3.21. *We define the* ***graded Betti numbers*** *of M by*

$$\beta_{i,p}(M) = \text{ number of summands in } F_i \text{ of the form } \mathbb{R}(-p).$$

In the same way we can compute the graded Betti numbers by means of the Tor functor.

Theorem 3.22.

$$\beta_{i,p}(M) = dim_{\mathbb{R}}(Tor_i^S(M, \mathbb{R})_p).$$

Just as in the case for local rings, for graded polynomial rings the projective dimension is determined by the length of a minimal free resolution.

Theorem 3.23. *Let M be an S-module, then the projective dimension of M is equal to*

$$pd_S(M) = \max\{i \mid \beta_i \neq 0\}.$$

Proof. Almost verbatim to *Theorem* 2.33, with $\mathfrak{m} = (s, t, u)$ the irrelevant ideal. ■

As an appreciation of how important is the graded structure in a polynomial ring, here we can give an almost trivial proof for the *Quillen-Suslin Theorem* 2.31 when the polynomial ring is graded.

Corollary 3.24. *Let M be a graded finitely generated projective S-module, then M is free.*

Proof. See *Corollary* 2.34. ■

We would like to know how the graded Betti numbers behave and thus we study the concept of regularity.

Definition 3.25. *The* ***Castelnuovo-Mumford regularity*** *(or simply* ***regularity****) of a graded finitely generated S-module M is*

$$reg(M) = \max\{j \mid \beta_{i,i+j}(M) \neq 0 \text{ for some } i\}.$$

Computing the depth of the ideal $\hat{I}$ will proof that the condition $gcd(a_1, a_2, a_3, a_4) = 1$ is an essential assumption to obtain good bounds for the regularity and the Betti numbers.

Proposition 3.26. *$depth(\hat{I}) \geq 2$.*

Proof. *Step 1:* From the hypothesis $gcd(a_1, a_2, a_3, a_4) = 1$ we can conclude that $gcd(b_1, b_2, b_3, b_4) = 1$. By contradiction suppose that $g \in \mathbb{R}[s, t, u]$ is a non-constant polynomial with $g \mid b_i$, then we may assume that g is a polynomial that depends only on the variable u because $g(s, t, 1)$ is a common divisor for the polynomials a_i. From the construction 3.5 we know that one of the polynomials b_i has a term that is free of u, without loss of generality we assume that $b_1(s, t, u) = \lambda s^\alpha t^{d-\alpha} + up(s, t, u)$ with $p \in \mathbb{R}[s, t, u]$. Then for some $h \in \mathbb{R}[s, t, u]$ we have $b_1(s, t, u) = g(u)h(s, t, u)$ and thus h has a term of the form

$\beta s^{\alpha}t^{d-\alpha}$ that multiplied with the highest power of u in g gives a term of degree bigger than d which cannot be reduced, and this contradicts the fact that b_1 is homogeneous of degree d.

Step 2: There exists two elements p and q in $\hat{I} = (b_1, b_2, b_3, b_4)$, that are relatively prime, i.e., $gcd(p, q) = 1$. Disappointingly, we were able to prove this statement only by making a more complicated reformulation.

- Let $f_1, \dots, f_n \in \mathbb{R}[x_1, \dots, x_m]$ be relatively prime polynomials ($gcd(f_1, \dots, f_n) = 1$), then there exists an infinite sequence of polynomials $\{h_i\}_{i=1}^{\infty} \subset (f_1, \dots, f_n)$, with $gcd(h_i, h_j) = 1$ for $i \neq j$.

For $n = 1$ we assume that the only polynomial in this case is equal to 1, so the ideal is whole polynomial ring and we can find such infinite sequence. In the case $n > 1$, we compute $g = gcd(f_1, \dots, f_{n-1})$ and the new polynomials $f_1^{'} = f_1/g, \dots, f_{n-1}^{'} = f_{n-1}/g$. Then using $gcd(f_1^{'}, \dots, f_{n-1}^{'}) = 1$ and the inductive hypothesis we can obtain an infinite sequence $\{h_i^{'}\}_{i=1}^{\infty} \subset (f_1^{'}, \dots, f_{n-1}^{'})$ with $gcd(h_i^{'}, h_j^{'}) = 1$ for $i \neq j$.

For each $h_i^{'}$ we have that $gcd(f_n, f_n + gh_i^{'}) = gcd(f_n, f_n + gh_i^{'} - f_n) = gcd(f_n, gh_i^{'})$. From $gcd(f_1, \dots, f_n) = 1$ we conclude that $gcd(f_n, g) = 1$ and for some $j \in \mathbb{N}$ we should have $gcd(f_n, gh_j^{'}) = 1$, because all the $h_i^{'}$'s have different prime factors but f_n can have only a finite amount of prime factors.

Now we use another induction argument where the inductive step is similar to the previous paragraph. Suppose we have computed a sequence of polynomials $h_1, \dots, h_k$ and a polynomial g_k, with the properties $gcd(h_i, h_j) = 1$ for $1 \leq i < j \leq k$ and $gcd(h_i, g_k) = 1$ for $1 \leq i \leq k$. Again, for each $h_i{'}$ we have

$$gcd(h_1 \dots h_k, h_1 \dots h_k + g_k h_i^{'}) = gcd(h_1 \dots h_k, g_k h_i^{'}) = gcd(h_1 \dots h_k + g_k h_i^{'}, g_k h_i^{'}), \quad (3.7)$$

and should exist some $j \in \mathbb{N}$ with $gcd(h_1 h_2 \dots h_k, g_k h_j^{'}) = 1$. Thus we define the next elements in the inductive step as

$$h_{k+1} = h_1 h_2 \dots h_k + g_k h_j^{'} \quad \text{and} \quad g_{k+1} = g_k h_j^{'}.$$

From the equality 3.7 we have that $gcd(h_1 h_2 \dots h_k, h_{k+1}) = gcd(h_1 h_2 \dots h_k, g_{k+1}) = gcd(h_{k+1}, g_{k+1}) = 1$, which implies $gcd(h_i, h_j) = 1$ for $1 \leq i < j \leq k+1$ and $gcd(h_i, g_{k+1}) = 1$ for $1 \leq i \leq k+1$. Starting with $h_1 = f_n,\ g_1 = g$ and following this iteratively process we can construct the required sequence $\{h_i\}_{i=1}^{\infty} \subset (f_1, \dots, f_n)$ with $gcd(h_i, h_j) = 1$ for $i \neq j$.

Step 3: We choose the two relatively prime elements p and q from the previous step. Then p is regular on $\mathbb{R}[s,t,u]$, and q is regular on $\mathbb{R}[s,t,u]/p$ because $gcd(p,q)=1$. Therefore $\{p,q\}$ is a regular sequence and $depth(\hat{I}) \geq 2$. ∎

In [20] is proven that for a general homogeneous ideal $J \subset \mathbb{K}[x_1,\ldots,x_n]$ (in any characteristic) generated by homogeneous elements with degree $\leq d$, the regularity of J is bounded by

$$reg(J) \leq (2d)^{2^{n-2}}. \tag{3.8}$$

Using similar ideas, in [16] is proven a bound for the regularity of a quotient ring, with

$$reg(\mathbb{K}[x_1,\ldots,x_n]/J) \leq n(d-1)$$

if $dim(\mathbb{K}[x_1,\ldots,x_n]/J) \leq 1$.

Theorem 3.27. *The regularity of* $\hat{I} = (b_1,b_2,b_3,b_4)$ *is bounded by* $reg(\hat{I}) \leq 3d-2$.

Proof. If we prove $dim(S/\hat{I}) \leq 1$, then we could cite *Theorem 19.4* from [16] and obtain the linear bound for the regularity $reg(\hat{I}) = reg(S/\hat{I}) + 1 \leq 3d-2$, that in some sense is the best result we could expect.

From the previous *Proposition* 3.26 we obtain a lower bound for the codimension (or height) of $\hat{I}$ by means of $codim(\hat{I}) \geq depth(\hat{I}) \geq 2$ (see *Proposition* 1.59).

Finally, we have the general inequality

$$codim(\hat{I}) + dim(S/\hat{I}) \leq dim(S) = 3,$$

that implies our desired inequality $dim(S/\hat{I}) \leq 1$.

∎

Remark 3.28. *From the fact that all the elements in the differential matrices are homogeneous of degree at least one, we can conclude that* $\beta_{i,p}(\hat{I}) = 0$ *for* $p < i+d$ *(see Proposition 12.3,* [17]*).*

With the computation of the regularity will be enough for our problem in the case $pd_S(\hat{I}) = 1$. Therefore for the rest of this section we will assume that $pd_S(\hat{I}) = 2$ and we shall try to find a bound for the Betti number $\beta_2 = dim_{\mathbb{R}}(Tor_2^S(\hat{I},\mathbb{R}))$ in this case.

Our main tool for this computation will be the Koszul complex. We know that $\mathfrak{m} = \{s,t,u\}$ is a regular sequence in $S = \mathbb{R}[s,t,u]$, then the Koszul complex $\mathbf{K}(\mathfrak{m})$ has zero homology

$H_iK(\mathfrak{m}) = 0$ for $i \geq 1$ (see *Theorem* 1.32). So we can regard the Koszul complex as a graded free resolution of $\mathbb{R} = S/(s,t,u)$, that is

$$\mathbf{K}(\mathfrak{m}): \quad 0 \to \bigwedge^3 S(-3)^3 \xrightarrow{d_3} \bigwedge^2 S(-2)^3 \xrightarrow{d_2} \bigwedge^1 S(-1)^3 \xrightarrow{d_1} \bigwedge^0 S^3 \to \mathbb{R} \to 0.$$

We tensor it with $\hat{I}$ and obtain the Koszul complex $\mathbf{K}(\mathfrak{m};\hat{I})$

$$0 \to \hat{I}\otimes_S \bigwedge^3 S(-3)^3 \xrightarrow{id\otimes_S d_3} \hat{I}\otimes_S \bigwedge^2 S(-2)^3 \xrightarrow{id\otimes_S d_2} \hat{I}\otimes_S \bigwedge^1 S(-1)^3 \xrightarrow{id\otimes_S d_1} \hat{I}\otimes_S \bigwedge^0 S^3 \to 0,$$

then we find the following relationship between the *Tor* functor and the *Koszul homology*

$$H_iK(\mathfrak{m};\hat{I}) \cong Tor_i^S(\mathbb{R},\hat{I}) \cong Tor_i^S(\hat{I},\mathbb{R}).$$

At this moment we have an explicit formula for computing the Betti number

$$\beta_2 = dim_{\mathbb{R}}(H_2K(\mathfrak{m};\hat{I})),$$

and yet we don't know how to compute a bound for the $\mathbb{R}$-dimension of the S-module $H_2K(\mathfrak{m};\hat{I})$. Instead we are going to use the fact that each map $id \otimes_S d_i$ has degree 0, and so we can form the complex

$$\begin{aligned} 0 \to \hat{I}_{p-3} \otimes_S \bigwedge^3 S^3 \xrightarrow{(id\otimes_S d_3)_{p-3}} \hat{I}_{p-2}\otimes_S \bigwedge^2 S^3 \xrightarrow{(id\otimes_S d_2)_{p-2}} \\ \hat{I}_{p-1} \otimes_S \bigwedge^1 S^3 \xrightarrow{(id\otimes_S d_1)_{p-1}} \hat{I}_p \otimes_S \bigwedge^0 S^3 \to 0, \end{aligned}$$

for each graded component $\hat{I}_p$ of $\hat{I}$. In this settlement we obtain huge advantages because each $\hat{I}_p$ is an $\mathbb{R}$-vector space and so the previous complex is conformed of $\mathbb{R}$-vector spaces.

For the moment we assume that we know the Hilbert function of the ideal $\hat{I}$ and our bound will be related with it. We make this "fair" assumption because for completely general ideals we cannot give an interesting result and later we will try to give some bounds for the Hilbert function of $\hat{I}$.

Proposition 3.29. $\beta_{2,p} \leq H_{\hat{I}}(p) - H_{\hat{I}}(p-1).$

Proof. We consider the complex

$$0 \to \hat{I}_{p-1} \otimes_S \bigwedge^3 S^3 \xrightarrow{(id \otimes_S d_3)_{p-1}} \hat{I}_p \otimes_S \bigwedge^2 S^3 \xrightarrow{(id \otimes_S d_2)_p}$$
$$\hat{I}_{p+1} \otimes_S \bigwedge^1 S^3 \xrightarrow{(id \otimes_S d_1)_{p+1}} \hat{I}_{p+2} \otimes_S \bigwedge^0 S^3 \to 0,$$

and by definition we have the formula

$$H_2 K(\mathfrak{m}; \hat{I})_p = \frac{Ker(id \otimes_S d_2)_p}{Im(id \otimes_S d_3)_p} = \frac{Ker((id \otimes_S d_2)_p)}{Im((id \otimes_S d_3)_{p-1})}.$$

Then using the fact that $Ker((id \otimes_S d_2)_p)$ and $Im((id \otimes_S d_3)_{p-1})$ are $\mathbb{R}$-vector spaces, we can compute the graded Betti number $\beta_{2,p}$ with

$$\beta_{2,p} = dim_{\mathbb{R}}(Ker((id \otimes_S d_2)_p)) - dim_{\mathbb{R}}(Im((id \otimes_S d_3)_{p-1})).$$

Since $pd_S(\hat{I}) = 2$ we have $H_3 K(\mathfrak{m}; \hat{I}) \cong Tor_3^S(\hat{I}, \mathbb{R}) = 0$ and so $Ker(id \otimes_S d_3) = 0$. From this we conclude that $(id \otimes_S d_3)_{p-1}$ is an injective map and $dim_{\mathbb{R}}(Im((id \otimes_S d_3)_{p-1})) = dim_{\mathbb{R}}(\hat{I}_{p-1} \otimes_S \bigwedge^3 S^3) = H_{\hat{I}}(p-1)$.

Let $h_{12} \otimes_S e_1 \wedge e_2 + h_{13} \otimes_S e_1 \wedge e_3 + h_{23} \otimes_S e_2 \wedge e_3 \in Ker((id \otimes_S d_2)_p)$, then by applying the differential map of the Koszul complex we have

$$sh_{12} \otimes_S e_2 - th_{12} \otimes_S e_1 + sh_{13} \otimes_S e_3 - uh_{13} \otimes_S e_1 + th_{23} \otimes_S e_3 - uh_{23} \otimes_S e_2 = 0,$$

and from this follows the equations

$$\begin{aligned} th_{12} &= -uh_{13}, \\ sh_{12} &= uh_{23}, \\ sh_{13} &= -th_{23}. \end{aligned}$$

Therefore one of the terms can completely define the other two, e.g., by knowing h_{12} we can determine h_{13} and h_{23}. This simple fact implies the inequality

$$dim_{\mathbb{R}}(Ker((id \otimes_S d_2)_p)) \leq H_{\hat{I}}(p).$$

■

Theorem 3.30. $\beta_2 \leq H_{\hat{I}}(3d)$.

Proof. Since $reg(\hat{I}) \leq 3d-2$, we have that $\beta_{2,p} = 0$ for $p > 3d-2+2 = 3d$. Then we compute

$$\beta_2 = \sum_{p \leq 3d} \beta_{2,p} \leq \sum_{p \leq 3d} (H_{\hat{I}}(p) - H_{\hat{I}}(p-1)) = H_{\hat{I}}(3d).$$

∎

Here we give a simple combinatorial bound for the Hilbert function of the ideal $\hat{I} = (b_1, b_2, b_3, b_4) \subseteq \mathbb{R}[s,t,u]$ generated by four elements. For any $p \geq d$ we have that the vector space $\hat{I}_p$ is generated by elements of the form mb_i $(1 \leq i \leq 4)$ where m is a monomial of degree $p-d$. We know that the number of monomials of degree $p-d$ in $\mathbb{R}[s,t,u]$ is $\binom{p-d+2}{2}$. Therefore we have have that the Hilbert function of $\hat{I}$ is bounded by

$$H_{\hat{I}}(p) \leq 4\binom{p-d+2}{2},$$

and the Betti number β_2 has the bound

$$\beta_2 \leq 4\binom{2d+2}{2}.$$

3.5 The case with projective dimension one

We remember that for this case the resolution of $\hat{I}$ is of the form

$$0 \to S(-\alpha_1) \oplus S(-\alpha_2) \oplus S(-\alpha_3) \xrightarrow{d_1 = \begin{pmatrix} \hat{p}_1 & \hat{q}_1 & \hat{r}_1 \\ \hat{p}_2 & \hat{q}_2 & \hat{r}_2 \\ \hat{p}_3 & \hat{q}_3 & \hat{r}_3 \\ \hat{p}_4 & \hat{q}_4 & \hat{r}_4 \end{pmatrix}} S(-d)^4 \xrightarrow{\begin{pmatrix} b_1 & b_2 & b_3 & b_4 \end{pmatrix}} \hat{I} \to 0. \tag{3.9}$$

In some cases we have that this resolution is not minimal and thus we cannot proceed with the same proof as in *Theorems* 3.20 and 3.22. But we can manage to give a bound for $\alpha = max(\alpha_1, \alpha_2, \alpha_3)$. The key issue is that for a free module $F = \bigoplus_{q \in J} S(-q)$ (J is an index set) we have $(F \otimes_S \mathbb{R})_p = 0$ if and only if $p \notin J$.

Lemma 3.31. *The grading of the previous resolution 3.9 can be bounded just as if it were a minimal resolution, i.e,* $\alpha = max(\alpha_1, \alpha_2, \alpha_3) \leq 3d-1$.

Proof. Let $p > 3d - 2 + 1 = 3d - 1$ then from $reg(\hat{I}) \leq 3d - 2$ we have that $\beta_{1,p} = 0$, and in this case implies that

$$Ker((d_1 \otimes_S \mathbb{R})_p) = Tor_1^S(\hat{I}, \mathbb{R})_p = 0,$$

hence we may conclude that the map $(d_1 \otimes_S \mathbb{R})_p$ is an injective map, and $(S(-\alpha_1) \oplus S(-\alpha_2) \oplus S(-\alpha_3))_p = 0$ because $(S(-d)^4)_q = 0$ for $q > d$. Therefore we have the inequality $\alpha \leq 3d - 1$, which is the same result we can obtain for the minimal free resolution (i.e. $(3d - 2) + 1$). ■

From the inequalities $\alpha_1, \alpha_2, \alpha_3 \leq 3d - 1$ and the fact that in the previous resolution the graded free module $S(-d)^4$ has all its grading exactly in d, we have that the degree of the polynomials $\hat{p}_i, \hat{q}_i, \hat{r}_i$ is bounded by $2d - 1 = 3d - 1 - d$. Therefore we have obtained the following result.

Partial Result: *Given an ideal $I \subset \mathbb{R}[s,t]$ defined by $I = (a_1, a_2, a_3, a_4)$, with $d = max_{1 \leq i \leq 4}(deg(a_i))$, and $gcd(a_1, a_2, a_3, a_4) = 1$. If $pd_S(\hat{I}) = 1$ ($\hat{I}$ is the ideal obtained in 3.5), then there exists a basis for $Syz(a_1, a_2, a_3, a_4)$ (a μ-basis for the rational surface defined by $P(s,t) = (a_1, a_2, a_3, a_4)$) with polynomials bounded in degree by $2d - 1$.*

Remark 3.32. *Here we have found a family of surfaces for which a minimal μ-basis has an optimal bound for the degree of its polynomials, i.e., linear with bound $\leq 2d - 1$. One could say that we already had this type of bound for the case in which a_1, a_2, a_3, a_3 were homogeneous polynomials since the beginning, because we could quote the bound $(2d)^{2^{n-2}}$ equal to $2d$ for $n = 2$. But the family of surfaces with $pd_S(\hat{I}) = 1$ is much broader than the one defined by homogeneous polynomials. For instance the surface*

$$P(s,t) = (st, st + t, t + 1, 2t - 1)$$

is not defined by homogeneous polynomials, but the homogeneous ideal $\hat{I} = (st, st + tu, tu + u^2, 2tu - u^2)$ has $pd_S(\hat{I}) = 1$ and we can find the following minimal free resolution

$$0 \to S(-3)^2 \xrightarrow{\begin{pmatrix} t & 0 \\ -u & s \\ 0 & -u \end{pmatrix}} S(-2)^3 \xrightarrow{\begin{pmatrix} u^2 & tu & st \end{pmatrix}} \hat{I} \to 0.$$

3.6 The case with projective dimension two

As we have already computed, we remember that the case with $pd_S(\hat{I}) = 2$ is of the form

$$0 \to S^a \xrightarrow{\hat{d_2}} S^{a+3} \xrightarrow{\hat{d_1}} S^4 \xrightarrow{[b_1,b_2,b_3,b_4]} \hat{I} \to 0, \tag{3.10}$$

and now we want to compute who is this number a.

In the previous resolution 3.10 we cannot assure that b_1, b_2, b_3, b_4 is a minimal system of generators. But we can assure that in the next step we find a minimal system of generators for $Syz(b_1, b_2, b_3, b_4)$, then using the exact sequence

$$0 \to S^a \xrightarrow{\hat{d_2}} S^{a+3} \xrightarrow{\hat{d_1}} Syz(b_1, b_2, b_3, b_4) \to 0$$

and the *Theorem* 1.12 we have $Im(\hat{d_2}) \subseteq \mathfrak{m}S^{a+3}$.

Making a proof with the same spirit as in *Theorem* 3.20, we have that

$$a = dim_{\mathbb{R}}(Tor_2^S(\hat{I}, \mathbb{R})) = \beta_2.$$

Therefore in this case the resolution of $\hat{I}$ is of the form

$$0 \to S^{\beta_2} \xrightarrow{\hat{d_2}} S^{\beta_2+3} \xrightarrow{\hat{d_1}} S^4 \xrightarrow{[b_1,b_2,b_3,b_4]} \hat{I} \to 0.$$

Using a similar argument as in *Lemma* 3.31 we have that the grading in the free module S^{β_2+3} is bounded by $3d-1$, and using the fact that $Im(\hat{d_2}) \subseteq \mathfrak{m}S^{a+3}$ then the grading in the free module S^{β_2} is the same as the one for the minimal free resolution. Therefore, the polynomials in the entries of the matrix d_1 have degree bounded by $3d-1-d = 2d-1$, and the polynomials in the entries of the matrix d_2 are bounded by $(3d-2)+2-d = 2d$.

Now finally, we can return to our original problem in $R = \mathbb{R}[s,t]$. We apply the tensor product with $\otimes_S S/(u-1)$ to obtain the exact sequence

$$0 \to R^{\beta_2} \xrightarrow{d_2} R^{\beta_2+3} \xrightarrow{d_1} R^4 \xrightarrow{[a_1,a_2,a_3,a_4]} I \to 0,$$

where $d_1 = \hat{d_1} \otimes_S S/(u-1)$ and $d_2 = \hat{d_2} \otimes_S S/(u-1)$ are matrices with entries in R bounded in degrees by $2d-1$ and $2d$, respectively.

For the rest of this document we shall work with the exact sequence

$$0 \to R^{\beta_2} \xrightarrow{d_2} R^{\beta_2+3} \xrightarrow{d_1} Syz(a_1, a_2, a_3, a_4)\ (\subset R^4) \to 0, \tag{3.11}$$

which is a **split** exact sequence because we know that $Syz(a_1, a_2, a_3, a_4)$ is a free module of rank 3.

Here we are in a position where the only thing that we "know" is the split exact sequence 3.11 (for the only thing we have bounds is for the matrices d_1 and d_2) and we want to find a bound for a basis of $Syz(a_1, a_2, a_3, a_4)$. For this task we will follow the paper [21], where there is an algorithmic proof based on the original Suslin's proof for the Serre's conjecture.

An $r \times s$ $(r > s)$ polynomial matrix $A \in R^{r\times s}$ is said to be **unimodular** if it satisfies one the following equivalent conditions (see [8])

(i) A can be completed into a invertible $r \times r$ square matrix.

(ii) there exists an $s \times r$ polynomial matrix $B \in R^{s\times r}$ such that $AB = I_r$.

(iii) there exists an $s \times r$ polynomial matrix $B \in R^{s\times r}$ such that $BA = I_s$.

(iv) the $s \times s$ minors of A have no common zeros.

The *"calculus of unimodular rows"* presented in the previous chapter is an elegant theory that deals with the problem

- Given a unimodular row $f \in R^{1\times r}$, then find a unimodular matrix $A \in R^{r\times r}$ $(det(A) \in \mathbb{R})$ such that f is the first row of A.

This simpler problem of completing a unimodular row is equivalent to the problem of completing a unimodular $r \times s$ matrix $(r > s)$ into a unimodular $r \times r$ matrix (for an elementary proof of this fact see *Lemma 1* from [18]).

We define the degree of a matrix $M = (a_{ij}) \in R^{r\times s}$ as the maximum degree of the polynomial entries of M, i.e., $deg(M) = max(deg(a_{ij}))$. For an *"effective"* solution of completing an unimodular matrix we are going to use the following result from [21].

Theorem 3.33. *Let $R = \mathbb{R}[s,t]$ and assume that $F \in R^{r\times s}$ $(r < s)$ is unimodular. Then there exists a square matrix $M \in R^{s\times s}$ such that*

(i) M is unimodular,

(ii) $FM = [I_r, 0] \in R^{r\times s}$,

(iii) $deg(M) \leq 2D(1+2D)(1+D^4)(1+D)^4$, *where* $D = r(1+deg(F))$.

Proof. See the Appendix section for a discussion. ■

This previous result is given for completing rows (i.e., $r < s$), but we want to complete columns (i.e., $r > s$). By simply taking the transpose of (ii) in the previous theorem we get the following corollary.

Corollary 3.34. *Let* $R = \mathbb{R}[s,t]$ *and assume that* $F \in R^{r\times s}$ $(r > s)$ *is unimodular. Then there exists a square matrix* $M \in R^{r\times r}$ *such that*

(i) M *is unimodular,*

(ii) $MF = \begin{bmatrix} I_s \\ 0 \end{bmatrix} \in R^{r\times s}$,

(iii) $deg(M) \leq 2D(1+2D)(1+D^4)(1+D)^4$, *where* $D = s(1+deg(F))$.

For notational purposes we make the following conventions

- $r = \beta_2 + 3$ and $s = \beta_2$,
- d_2 denotes the $r \times s$ matrix $F \in R^{r\times s}$ with $deg(F) \leq 2d$,
- d_1 denotes the $4 \times r$ matrix $G \in R^{4\times r}$ with $deg(G) \leq 2d - 1$,
- $D = s(1 + deg(F)) \leq \beta_2(1 + 2d)$,

thus we end up with

$$0 \to R^s \xrightarrow{F} R^r \xrightarrow{G} Syz(a_1, a_2, a_3, a_4)\ (\subset R^4) \to 0. \tag{3.12}$$

Since this sequence splits, there exists a matrix $H \in R^{r\times s}$ with $HF = I_s$ and so the matrix F is unimodular. We can apply the previous *Corollary* 3.34 and from now on $M \in R^{r\times r}$ will denote a matrix that satisfies *(i), (ii), (iii)* from 3.34.

In 3.12 we know that there exists an R-module $V \cong Syz(a_1, a_2, a_3, a_4)$, such that R^r is the direct sum of $Im(F)$ and V, that is

$$R^r = Im(F) \oplus V. \tag{3.13}$$

Making a more careful treatment we can find that

$$Syz(a_1, a_2, a_3, a_4) = Im(G) = G(V),$$

because $Ker(G) = Im(F)$. Finally we are ready to find a basis for $Syz(a_1, a_2, a_3, a_4)$.

Theorem 3.35. *There exist a basis for $Syz(a_1, a_2, a_3, a_4)$ formed by the three vectors $\mathbf{p}, \mathbf{q}, \mathbf{r} \in R^4$, with the polynomial entries bounded in degree by*

$$\max(deg(\mathbf{p}), deg(\mathbf{q}), deg(\mathbf{r})) \leq (2d-1)(r-1)2D(1+2D)(1+D^4)(1+D)^4.$$

Proof. Let $N \in R^{r\times r}$ be the inverse matrix of M, then we have that

$$deg(N) \leq (r-1)deg(M), \tag{3.14}$$

because the determinant of every $(r-1)\times(r-1)$-minor is a polynomial of degree at most $r-1$ in terms of the entries of M. Also, from the item (ii) of *Corollary* 3.34 we have that

$$F = N \begin{bmatrix} I_s \\ 0 \end{bmatrix}.$$

We know that N is an automorphism for $R^r = N(span(e_1, \ldots, e_s, e_{s+1}, e_{s+2}, e_{s+3}))$ and that

$$Ker(G) = Im(F) = N(span(e_1, \ldots, e_s)),$$

where e_i is the i-th column vector of R^r. Hence we have[2]

$$Syz(a_1, a_2, a_3, a_4) = Im(G) = G(R^r) = GN(span(e_1, \ldots, e_r)) = GN(span(e_{s+1}, e_{s+2}, e_{s+3})),$$

and we define the basis for $Syz(a_1, a_2, a_3, a_4)$ as

$$\mathbf{p} = GNe_{s+1},$$
$$\mathbf{q} = GNe_{s+2},$$
$$\mathbf{r} = GNe_{s+3}.$$

[2]In contrast to the proof of *Theorem* 2.30, here we don't need to fully identify the module $V \cong Syz(a_1, a_2, a_3, a_4)$ as a direct summand inside R^r.

Finally, using the previous bounds $deg(G) \leq 2d-1$ and 3.14, we obtain the result

$$\max(deg(\mathbf{p}), deg(\mathbf{q}), deg(\mathbf{r})) \leq deg(G)deg(N) \leq (2d-1)(r-1)deg(M)$$
$$\leq (2d-1)(r-1)2D(1+2D)(1+D^4)(1+D)^4.$$

■

Substituting in terms of d and the Betti number β_2 we have the bound

$$2(2d-1)(\beta_2+2)\beta_2(1+2d)(1+2\beta_2(1+2d))(1+(\beta_2(1+2d))^4)(1+\beta_2(1+2d))^4 \quad (3.15)$$

and substituting the previous result $\beta_2 \leq 4\binom{2d+2}{2} \in O(d^2)$ we can find a bound for the degree of a minimal μ-basis that completely depends on d. We can compute that the result in 3.15 is in the order of

$$O(d^{33}).$$

In the end of this section we put some of our thoughts about the results obtained throughout this chapter.

- We have found a family of rational surfaces with a minimal μ-basis bounded in degree by the linear term $\leq 2d-1$.
- We have given an explicit bound for the degree of a minimal μ-basis for any rational surface as in 3.1. The result of the bound is in the order of $O(d^{33})$.
- This big and not so attractive bound comes mostly from the solution of the *Quillen-Suslin Theorem*. Therefore could be interesting to find better bounds for an "effective" solution of the *Quillen-Suslin Theorem*.
- The result that we found for the regularity is linear with $reg(\hat{I}) \leq 3d-2$, so it is a pretty good bound and optimal from a complexity point of view.
- The formula 3.15 is given also in terms of β_2 in case that we already know who is β_2. The bound for β_2 is in the order of $O(d^2)$, but having a small knowledge of the ideal $\hat{I}$ and its Hilbert function this result could be improved drastically.
- Perhaps, for *"aesthetic purposes"* it could be better to follow the *"philosophy"* of [21] and just say: *"we have proven that the degree of a minimal μ-basis for any rational surface is bounded by a single exponential bound $d^{O(1)}$"*.[3]

[3] Clearly we have that $O(2) = O(1)$

3.7 Appendix

The main result we shall follow from [21] is the following theorem.

Theorem 3.36. ***(Theorem 3.1,*** [21]***)*** *Let $R = \mathbb{K}[x_1, \ldots, x_n]$ and assume that $F \in R^{r\times s}$ $(r < s)$ is unimodular. Then there exists a square matrix $M \in R^{s\times s}$ such that*

(i) *M is unimodular,*

(ii) *$FM = [I_r, 0] \in R^{r\times s}$,*

(iii) *$deg(M) = (r(1 + deg(F))^{O(n)}$.*

With the pioneering work of *Mayr* and *Meyer* [12], we know that the general problem of solving linear equation systems in polynomial rings involves necessarily a doubly exponential bound for the degree of the polynomials appearing in the solution. Also from [12], we know that the best possible bound for the regularity of an ideal in the general case is double exponential as in 3.8. Therefore the previous result has important theoretical consequences because it proofs that a solution for the *Serre's conjecture* exists with a single exponential bound for the degree.

In our case $n = 2$ and we will have to make some small *"adjustments"* to find an actual constant instead of the complexity class $O(2)$. We will follow exactly the same proof as in [21], and in certain steps we will substitute phrases like $n + 3n \in O(n)$ by the exact computation $n + 3n = 4n$.

Proposition 3.37. ***(Proposition 4.1,*** [21]***)*** *Assume that $F \in R^{r\times s}$ $(R = \mathbb{K}[x_1, \ldots, x_n]$, $r < s)$ is unimodular. Then there exists a square matrix $M \in R^{s\times s}$ such that:*

(i) *M is unimodular,*

(ii) *$FM = [f_{ij}(x_1, \ldots, x_{n-1}, 0)]$ (i.e., FM is equal to the $r \times s$ matrix obtained by specializing the indeterminate x_n to zero in the matrix F),*

(iii) *$deg(M) \leq D(1 + 2D)(1 + D^{2n})(1 + D)^{2n}$, with $D = r(1 + deg(F))$.*

Proof. We denote $F(t)$ as the matrix $F(t) = [f_{ij}(x_1, \ldots, x_{n-1}, t)]$ and inside this proposition $d = 1 + deg(F)$.

<u>*Claim 1.*</u> (*Procedure 4.6, Step 1 and Step 2,* [21]) There exists elements $c_1, \ldots, c_N \in \mathbb{K}[x_1, \ldots, x_{n-1}]$ with $N \leq (1+rd)^{2n}$ such that $x_n \in (c_1, \ldots, c_N)$. Also we can find elements

$a_1, \ldots, a_N \in x_n\mathbb{K}[x_1, \ldots, x_{n-1}]$, such that

$$x_n = a_1c_1 + \ldots + a_Nc_N$$

and with

$$\max_{1\leq k\leq N}\{deg(a_kc_k)\} \leq 1 + (rd)^{2n}.$$

Claim 2. (*Procedure 4.6, Step 3 and Step 4,* [21]) For $1 \leq k \leq N$ let

$$b_k = \sum_{h=1}^{k} a_hc_h,$$

then there exist unimodular matrices E_k with the properties

- $F(b_k)E_k = F(b_{k-1})$,
- $deg(E_k) \leq rd(1 + 2rd)\max\{deg(b_k), deg(b_{k-1})\} \leq rd(1 + 2rd)(1 + (rd)^{2n})$ (here we substituted the original $(rd)^{O(n)}$ by obtained bound, because $\max\{deg(b_k), deg(b_{k-1})\} \leq 1 + (rd)^{2n}$).

Therefore we define $M = E_NE_{N-1}\ldots E_1$ and we have $F(x_n)M = F(0)$, with the bound

$$deg(M) \leq Nrd(1 + 2rd)(1 + (rd)^{2n}) \leq rd(1 + 2rd)(1 + (rd)^{2n})(1 + rd)^{2n}.$$
$$deg(M) \leq D(1 + 2D)(1 + D^{2n})(1 + D)^{2n}$$

■

Proof. (of *Theorem* 3.36) For a matrix $F = [f_{ij}(x_1, \ldots, x_n)]$ the substitution of a variable x_i for 0 does not increase the degree of the matrix, and keeps the unimodularity because the condition of being unimodular is equivalent to the fact that the $(r \times r)$-minors have no common zeros. Therefore, applying the previous proposition n times we can find a unimodular square $R^{s\times s}$ matrix M' with

$$FM' = [f_{ij}(0, 0, \ldots, 0)]$$

and degree bounded by

$$deg(M') \leq nD(1 + 2D)(1 + D^{2n})(1 + D)^{2n}.$$

Since the matrix $[f_{ij}(0, 0, \ldots, 0)]$ has rank r, we can find an elementary matrix $E \in \mathbb{K}^{s\times s}$ with $[f_{ij}(0, 0, \ldots, 0)]E = [I_r, 0]$. Making $M = M'E$, we get $FM = [I_r, 0]$ and the same inequality

$$deg(M) \leq nD(1+2D)(1+D^{2n})(1+D)^{2n}.$$

■

Bibliography

[1] Falai Chen, David Cox, and Yang Liu, *The μ-basis and implicitization of a rational parametric surface*, Journal of Symbolic Computation **39** (2005), no. 6, 689–706.

[2] David Eisenbud, Daniel R. Grayson, Mike Stillman, Bernd Sturmfels (Eds.), *Computations in algebraic geometry with macaulay 2*, 1st ed., Vol. 8, Springer, 2002.

[3] David Eisenbud, *Commutative algebra with a view towards algebraic geometry*, Graduate Texts in Mathematics, 150, Springer-Verlag, 1995.

[4] Daniel R. Grayson and Michael E. Stillman, *Macaulay2, a software system for research in algebraic geometry*. Available at http://www.math.uiuc.edu/Macaulay2/.

[5] E. Graham Evans, Phillip Griffith, *Syzygies*, London Mathematical Society Lecture Note Series, 106, Cambridge University Press, 1985.

[6] Winfried Bruns, H. Jürgen Herzog, *Cohen-macaulay rings*, 2nd ed., Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1998.

[7] David Hilbert, *Über die theorie der algebraischen formen*, Math. Ann. **36** (1890), 473–534.

[8] T. Y. Lam, *Serre's problem on projective modules*, Springer Monographs in Mathematics, Springer Verlag, 2006.

[9] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics 211, Springer-Verlag New York, 2002.

[10] M. F. Atiyah, I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley Publishing, 1969.

[11] Hideyuki Matsumura, *Commutative ring theory*, 1st ed., Cambridge Studies in Advanced Mathematics volume 8, Cambridge University Press, 1989.

[12] Ernst W. Mayr, Albert R. Meyer, *The complexity of the word problems for commutative semigroups and polynomial ideals*, Advances in mathematics **46** (1982), no. 3, 305–329.

[13] James R. Munkres, *Elements of algebraic topology*, Addison-Wesley, 1984.

[14] nLab, *Category of chain complexes*. https://ncatlab.org/nlab/show/category+of+chain+complexes.

[15] David A. Cox, John Little, Donal O'Shea, *Using algebraic geometry*, 2nd ed., Graduate texts in mathematics, 185, Springer Verlag, 2005.

[16] Irena Peeva, *Syzygies and hilbert functions*, CRC Press, 2007.

[17] ———, *Graded syzygies*, Vol. 14, Springer Science & Business Media, 2010.

[18] D. C. Youla, P. F. Pickel, *The quillen-suslin theorem and the structure of n-dimensional elementary polynomial matrices*, IEEE transactions on circuits and systems **31** (1984), no. 6, 513–518.

[19] Joseph J. Rotman, *An introduction to homological algebra*, Academic Press, 1979.

[20] Giulio Caviglia, Enrico Sbarra, *Characteristic-free bounds for the castelnuovo-mumford regularity*, Compos. Math **141** (2005), no. 6, 1365–1373.

[21] Leandro Caniglia, Guillermo Cortiñas, Silvia Danón, Joos Heintz, Teresa Krick, Pablo Solernó, *Algorithmic aspects of suslin's proof of serre's conjecture*, computational complexity **3** (1993), no. 1, 31–55.