



UNIVERSIDAD NACIONAL DE COLOMBIA SEDE MEDELLÍN

ESCUELA DE MATEMÁTICAS

TESIS DE DOCTORADO:

**Model Theory, Homological Conjectures, Frobenius  
Algebras and Cohomology of Twisted Graded G-Algebras**

EDISSON GALLEGO GONZÁLEZ

---

DIRECTOR:

JUAN D. VÉLEZ

CODIRECTOR:

MORDECHAI KATZMAN

Junio 11 de 2015

# Contents

<b>I</b>	<b>Introduction</b>	<b>iv</b>
<b>1</b>	<b>Some applications of ultraproducts and Lefschetz's principle to commutative and homological algebra.</b>	<b>1</b>
1.1	Preliminaries . . . . .	1
1.2	Ultraproducts . . . . .	2
1.3	Transfer principles . . . . .	3
1.4	Codes for polynomials, rings, and modules . . . . .	6
1.4.1	Equational criterion for flatness . . . . .	8
1.5	Asymptotic form of Koh's conjecture . . . . .	11
1.6	A non-Standard proof of a Theorem of Hochster . . . . .	16
<b>2</b>	<b>Frobenius Algebras</b>	<b>21</b>
2.1	Some preliminaries about Frobenius Algebras . . . . .	21
2.2	Openness of the finitely generated locus of the Frobenius Algebra . . . . .	23
<b>3</b>	<b>On the cohomology of <math>G</math>-Graded Twisted Algebras</b>	<b>28</b>
3.1	Some preliminaries on $G$ -graded twisted algebras . . . . .	28
3.2	Group Cohomology . . . . .	30
3.2.1	Some standard free resolutions . . . . .	31
3.2.2	Another way to compute the cohomology of groups . . . . .	33
3.3	The computation of $H^2(G, A)$ when $G$ is a finite abelian group and $A$ is a $G$ -module with the trivial action. . . . .	35

3.4 Graded Morphisms and the classification problem . . . . . 45

# Acknowledgements

I am deeply grateful to Professor Juan D. Vélez to whom am I in great debt for almost all my mathematical education. Without his contributions and guidance, this thesis could have not been possible. I am also in great debt to Professor Moty Katzman for his committed guidance and generosity at the moment of sharing his ideas and insights. I also want to thank him for his boundless hospitality during my visit to the University of Sheffield. Finally, I want to thank Juan Pablo Hernandez, my study partner, with whom I have discussed many of the results in this thesis.

## Part I

# Introduction

This thesis gravitates around several topics in commutative and homological algebra, as well as in the theory of noncommutative, nonassociative algebras.

1. The first chapter is devoted to applications of *Lefschetz's Principle* in Model Theory and the theory of ultraproducts of affine  $k$ -algebras to a series of questions in commutative and homological algebra. In particular, we will reformulate *Koh's Conjecture* [20] in this formalism. This will enable us to give an *asymptotic proof* of this conjecture in prime characteristic (Theorem 10). A further application of those methods also will allow us to give a new (non-standard) proof of a main metatheorem of Mel Hoschter (see [14]), a fundamental tool for reducing problems concerning  $k$ -algebras over fields of characteristic zero to problems about  $k$ -algebras over fields of prime characteristic. The book *The Use of Ultraproducts in Commutative Algebra* [30] is the main reference for this chapter. We will follow closely the notation in that book.
2. The second chapter focusses on the study of the Open Locus of the Frobenius Algebra. We will give a partial answer to a conjecture made by M. Katzman about the openness of the finitely generated locus of the Frobenius algebra. This conjecture can be formulated in a precise manner: Is the locus

$$U = \{P \in \text{Spec}(R) : \mathcal{F}(E_{R_p}) \text{ is a finitely generated } R_p\text{-algebra}\}$$

Where  $\mathcal{F}$  denotes the Frobenius functor and  $E_{R_p}$  the injective hull of the residual field of the local ring  $(R_p, pR_p)$  open in the Zariski Topology? This seems to be a very difficult question. However, in the case where  $R$  is a ring of the form  $R = K[x_1, \dots, x_n]/I$ , where  $I \subset K[x_1, \dots, x_n]$  is a *square-free monomial ideal*, we will show an open set in which  $\mathcal{F}(E_{R_p})$  is a finitely generated  $R_p$ -algebra.

3. The third chapter is devoted to a topic quite different from the previous ones. There, we tackle the problem of determining how many  $G$ - graded, twisted associative  $k$ -algebras exist up to graded isomorphisms, in case the group of graduation is a finitely generated abelian group. We solve that problem by computing the cohomology group  $H^2(G, A)$ , where  $A \subset k^*$  is certain multiplicative closed subset of  $k^*$ , viewed as a  $G$ -module via the trivial action. When  $G$  is given as a direct product  $G \simeq G_1 \times \dots \times G_k$ , with each  $G_i$  a

finite cyclic group of order  $n_i$ , we will show the following explicit formula holds (Theorem 22):

$$H^2(G, A) \cong \bigoplus_{i=1}^k \frac{A}{n_i A} \oplus \bigoplus_{i \neq j} \text{Ann}_A(n_i) \cap \text{Ann}_A(n_j).$$

Where  $\text{Ann}_A(n_j)$  denote the annihilator of  $n_j$  in  $A$ .

# Chapter 1

## Some applications of ultraproducts and Lefschetz's principle to commutative and homological algebra.

As it was mentioned in the introduction, in this chapter we will use some tools of model theory, mainly as they appear in the book *The Use of Ultraproducts in Commutative Algebra* [30] and the article *Bounds in Cohomology* [31] both of them written by H. Schoutens, in order to give a proof of a reformulated form of Koh's Conjecture and also a new proof of a (weaker form) classic result by M. Hoshcher, Theorem 10.

### 1.1 Preliminaries

In this section we introduce some basic notions that will be used throughout the first chapter. Most statements will not be proved. We will limit ourselves to give appropriate references. We start by defining the concept of a *filter*.



**Definition 1.** Let  $I$  be any non empty set. A filter on  $I$  is a subset  $\mathcal{U} \subset \mathcal{P}(I)$  such that:

1.  $I \in \mathcal{U}$  and  $\emptyset \notin \mathcal{U}$
2. If  $A, B \in \mathcal{U}$ , then  $A \cap B \in \mathcal{U}$
3. If  $A \in \mathcal{U}$  and  $A \subset B \subset I$ , then  $B \in \mathcal{U}$

**Example 1.** 1. Let us consider  $I = [0, 1]$ . Then the set  $\mathcal{U} = \{X \subset [0, 1] : \text{Lebesgue measure of } I - X \text{ is zero}\}$  is readily checked to be a filter.

2. If  $I$  is an infinite set, then  $\mathcal{U} = \{X \subset I : |I - X| < \infty\}$  is a filter. (Here,  $||$  denotes cardinality of a set.)

3. Let  $x \in I$  be a fixed element, and let  $\mathcal{U} = \{X \subset I : x \in X\}$ . Then  $\mathcal{U}$  is a filter called a principal filter.

**Definition 2.** A filter  $\mathcal{U}$  is called an ultrafilter on  $I$  if for every  $X \subset I$  we have  $X \in \mathcal{U}$  or  $I - X \in \mathcal{U}$ .

**Example 2.** 1. From the previous definition, it readily follows that every principal filter is an ultrafilter.

2. Using Zorn's Lemma, it is easy to show that for any filter  $\mathcal{D}$  on  $I$  there exists an ultrafilter  $\mathcal{U}$  on  $I$  such that  $\mathcal{D} \subset \mathcal{U}$ .

*Proof.* This is a standard result, see [24] Exercise 2.5.18 page 63. □

## 1.2 Ultraproducts

Now, let us introduce the notion of an ultraproduct.

Let  $\mathcal{L} = \{f \dots, R \dots, c \dots\}$  be any language (see [24], Definition 1.1.1), and let  $I$  be an infinite set. Let us suppose that  $\mathcal{M}_i$  is an  $\mathcal{L}$  structure for any  $i \in I$  (see [24], Definition 1.1.2). Let  $\mathcal{U}$  be a fixed ultrafilter on  $I$ . We may define a new  $\mathcal{L}$ -structure  $\mathcal{M}$  as follows: In the product  $\prod_{i \in I} \mathcal{M}_i$ , let us define an equivalence relation by declaring  $(a_i) \sim (b_i)$  if and only if the set  $\{i \in I : a_i = b_i\}$  is an element of  $\mathcal{U}$ . The set of equivalence classes will be denoted by  $\text{Ulim} \mathcal{M}_i$ ,

and the class of an element  $(a_i)$  as  $\text{Ulim}a_i$  or also as  $[\underline{a}_i]$ .

$\mathcal{M}$  is a  $\mathcal{L}$ -structure in the following way:

1. If  $c \in \mathcal{L}$  is a constant symbol, then we interpret it in  $\mathcal{M}$  as  $c^{\mathcal{M}} = \text{Ulim } c^{\mathcal{M}_i}$ , where  $c^{\mathcal{M}_i}$  is the interpretation of  $c$  in  $\mathcal{M}_i$ .
2. If  $f$  is a functional symbol in  $n$  variables, then its interpretation in  $\mathcal{M}$  is  $f^{\mathcal{M}} = \text{Ulim } f^{\mathcal{M}_i}$ , where  $f^{\mathcal{M}_i}$  is the interpretation of  $f$  in  $\mathcal{M}_i$ . In other words,  $f^{\mathcal{M}}([\underline{a}_i^1], \dots, [\underline{a}_i^n]) = \text{Ulim } f^{\mathcal{M}_i}(a_i^1, \dots, a_i^n)$ .
3. If  $R$  is a  $n$ -ary relation symbol in  $\mathcal{L}$ , then its interpretation in  $\mathcal{M}$  is given by:

$$R^{\mathcal{M}} = \{([\underline{a}_i^1], \dots, [\underline{a}_i^n]) / \{i : (a_i^1, \dots, a_i^n) \in R^{\mathcal{M}_i}\} \in \mathcal{U}\}$$

**Example 3.** Let  $\mathcal{R}_i$  be a ring with sum  $+_i$ , multiplication  $\cdot_i$  and constant symbols  $0_i, 1_i$  for all  $i \in I$ . Then Loś's theorem (see Theorem 1) guarantees that  $\text{Ulim}\mathcal{R}_i$  is a ring with sum  $+$  given by  $\text{Ulim}+_i$ , multiplication  $\cdot = \text{Ulim}\cdot_i$ , and constant symbols  $0 = \text{Ulim}0_i, 1 = \text{Ulim}1_i$ . This ring called an ultra-ring.

### 1.3 Transfer principles

In this section we will mention two principles which allow us to transfer algebraic properties from an ultraproduct of objects  $\text{Ulim}\mathcal{O}_i$  to each one of the objects  $\mathcal{O}_i$ , and vice versa.

One essential tool is Loś's Theorem. It states that any first-order formula is true in the ultraproduct if and only if the set of indices  $i$  such that the formula is true in  $\mathcal{M}_i$  is a member of  $\mathcal{U}$ . More precisely:

**Theorem 1** (Łoś). Let  $\Phi(v_1, \dots, v_n)$  be a formula in  $\mathcal{L}$ , and let  $\mathcal{U}$  be an ultrafilter on  $I$ . Then,  $\mathcal{M} \models \Phi([\underline{a}_1], \dots, [\underline{a}_n])$  if and only if  $\{i \in I : \mathcal{M}_i \models \Phi(a_1, \dots, a_n)\}$  is a set in  $\mathcal{U}$ , (see [24], Exercise 2.5.19, page 64).

**Example 4.** 1.

2. If each  $\mathcal{R}_i$  is an algebraically closed field, then  $R = \text{Ulim}\mathcal{R}_i$  is also an algebraically closed field.

*Proof.* Note that  $\text{Ulim}\mathcal{R}_i$  is a field by Łoś's theorem, since all field's axioms are first order sentences. Similarly, to prove that  $R$  is algebraically closed, it is enough to notice that this last condition can be stated in first order by means of a countable collection of sentences:

$$\sigma_n : (\forall a_0, \dots, a_n)(\exists x)(a_n = 0 \vee a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 = 0), \text{ with } n \geq 1.$$

□

3. If each  $\mathcal{R}_i$  is a local ring (not necessarily noetherian), then  $R = \text{Ulim}\mathcal{R}_i$  is also a local ring.

*Proof.*  $R$  is a local ring if and only if any sum of non units is again a non unit. Clearly, this condition can be expressed using a first order formula, and hence the result follows from Łoś's Theorem. □

Now we recall a standard result in the theory of fields.

**Theorem 2.** (Steinitz's Theorem) *If  $K$  and  $L$  are algebraically closed fields of the same characteristic and with the same (uncountable) cardinality, then they are isomorphic.*

With this result we are able to prove the following fundamental theorem.

**Theorem 3.** *Let  $I$  denote the set of all prime numbers, and let us choose any non-principal ultrafilter  $\mathcal{U}$  in  $I$ . Then, there is an isomorphism  $\text{Ulim } \mathbb{F}_p^{\text{alg}} \cong \mathbb{C}$ , where  $\mathbb{F}_p^{\text{alg}}$  denotes a fixed algebraic closure of the prime field  $\mathbb{Z}_p$ .*

*Proof.* The fact that  $\text{Ulim } \mathbb{F}_p^{\text{alg}}$  is an algebraic closed field follows from example 1. Moreover, it has characteristic 0 since for any fixed  $q > 0$  the sentence  $\phi_q : 1 + 1 + \dots + 1 \neq 0$  holds in  $\mathbb{F}_p^{\text{alg}}$ , for every  $p > q$ . Then, by Łoś's theorem, this ultraproduct must have characteristic 0.

On the other hand, the cardinality of this ultraproduct is equal to that of the continuum. Hence, both  $\mathbb{C}$  and  $\text{Ulim } \mathbb{F}_p^{\text{alg}}$  are algebraic closed fields of characteristic 0 with same uncountable cardinality. Then, by Steinitz's Theorem they are (non canonically) isomorphic. For more details, the reader may consult [30], Theorem 2.4.3.

□

**Remark 1.** By Loś's Theorem, a sentence  $\phi$  in the language of rings is true in  $\mathbb{C}$  if and only if it is true in  $\mathbb{F}_p^{\text{alg}}$ , for almost every  $p$ , i.e., for all primes in an element of the ultrafilter. Now, the set of prime numbers  $J$  in which  $\phi$  does not hold has to be finite. Otherwise, using example 1 (2) we could construct a non principal ultrafilter on  $J$ , and over this ultrafilter, an isomorphism  $\text{Ulim } \mathbb{F}_p^{\text{alg}} \cong \mathbb{C}$ , which would contradict Loś's Theorem.

On the other hand, any cofinite set such as  $L = \{p \mid \mathbb{F}_p^{\text{alg}} \models \phi\}$  which is cofinite on  $I$  must lie in the ultrafilter  $L \in \mathcal{U}$ . Then, the existence of an isomorphism  $\text{Ulim } \mathbb{F}_p^{\text{alg}} \cong \mathbb{C}$  is equivalent to the following theorem.

**Theorem 4. Lefschetz's Principle.** Let  $\phi$  be a sentence in the language of rings. The following statements are equivalent.

1.  $\phi$  is true in an algebraic closed field of characteristic zero.
2. There exists a natural number  $m$  such that for every  $p > m$ ,  $\phi$  is true for every algebraically closed field of characteristic  $p$ .

*Proof.* See ([24] Corollary 2.2.10, page 42). □

Now we are going to state without proof *The Compactness Theorem*, a cornerstone of Model Theory.

**Theorem 5.** Suppose  $T$  is a  $\mathcal{L}$ -theory. Then,  $T$  is satisfiable if and only if every finite subset of  $T$  is satisfiable

This theorem says that there exists a model for  $T$  if and only if there exists a model (not necessarily the same) for each finite subset of  $T$ . As an application of the Compactness Theorem we readily deduce the following proposition:

**Proposition 1.** Let  $\phi$  be a first order sentence which is true in every field  $k$  of characteristic zero. Then, there exists a prime number  $p_0$  such that  $\phi$  is true in each field  $F$  of characteristic  $q$ , for  $q > p_0$ .

*Proof.* Let us consider the theory whose sentences are the following:

$$T := \{\text{Axioms for fields, } q \neq 0 \text{ for all prime number } q, \neg\phi\}.$$

By hypothesis, this theory does not have a model. Henceforth, by the Compactness theorem, there must exist a finite set  $\Sigma \subset T$ , such that  $\Sigma$  does not have any models either. We may assume that in  $\Sigma$  are included all the (finite) field axioms,  $\neg\phi$ , and all the axioms  $q \neq 0$  for all  $q < p_0$  for some prime number  $p_0$ . Since  $\Sigma$  does not have model, each field  $F$  of characteristic  $q > p_0$  satisfies all the axioms in  $\Sigma$  except  $\neg\phi$ ; that is to say:  $F \models \phi$ .  $\square$

## 1.4 Codes for polynomials, rings, and modules

Throughout this discussion, we will fix a monomial order in the polynomial ring  $k[x_1, \dots, x_n]$ . We will also fix an ultrafilter on the set of all prime numbers.

**Definition 3.** *Let  $R$  be a finitely generated  $k$ -algebra.*

1. *Let  $I$  be an ideal of  $k[x_1, \dots, x_n]$ . We will say that  $I$  has **complexity at most  $d$** , if  $n \leq d$  and it is possible to choose generators for  $I$ ,  $f_1, \dots, f_s$ , with  $\deg f_i \leq d$ , for  $i = 1, \dots, s$ .*
2. *We say  $R$  has **complexity at most  $d$**  if there is a presentation of  $R$  as  $k[x_1, \dots, x_n]/I$ , with  $I$  of complexity at most  $d$ .*
3. *If  $J \subset R$  is an ideal, we will say that  $J$  **has complexity at most  $d$** , if  $R$  has complexity less than or equal to  $d$ , and there exists a lifting of  $J$  in  $k[x_1, \dots, x_n]$ , let us say  $J'$ , with complexity at most  $d$ .*
4. *If  $R$  is a local affine algebra, we say it has **complexity at most  $d$**  if  $R$  can be written as  $R = (k[x_1, \dots, x_n]/I)_p$ , for some prime ideal  $p \subset k[x_1, \dots, x_n]/I$  such that the complexity of  $R$  and  $p$  is at most  $d$ .*
5. *If  $M$  is any finitely generated  $R$ -module, we will say that  $M$  has **complexity at most  $d$**  if  $R$  is a  $k$ -algebra of complexity at most  $d$ , and there exists an exact sequence  $R^t \xrightarrow{\Gamma} R^s \rightarrow M \rightarrow 0$ , with  $s, t \leq d$ , where all the entries of the matrix  $\Gamma$  are polynomials (or quotients of polynomials, in the local case) with degree at most  $d$ .*
6. *Let  $M \subset R^d$  be  $R$ -submodule. We will say that  $M$  has **degree type at most  $d$**  (written as  $gt(M) \leq d$ ) if the complexity of  $R$  is at most  $d$ , and  $M$  is generated by  $d$ -tuples with*

all its entries of degree at most  $d$ . If  $M$  is a finitely generated  $R$ -module, we will say that  $M$  has **complexity degree at most  $d$**  if there exist submodules  $N_2 \subset N_1 \subset R^d$ , both of degree type at most  $d$ , such that  $M \cong N_1/N_2$ .

The notion of complexity degree and that of complexity of a module are closely related. In some sense, these are same, as we shall see below.

**Remark 2.** In (1), the number of generators of  $I$  may always be bounded in terms of  $d$ . In fact, without loss of generality we can assume that all the  $f_i$  are monic, and also that the leading terms of  $f_i$  and  $f_j$  are different from each other, when  $i \neq j$ . (If they have same leading term, we can change  $f_j$  by  $f_j - f_i$  and get a new set of generators for  $I$  satisfying this last property.) So,  $s \leq D$ , where  $D$  is the number of monomials of degree  $d$ ,  $D = |\{x_1^{r_1} \cdots x_n^{r_n} \mid \sum_{i=1}^n r_i \leq d\}|$ . It is then very easy to see that  $D = \binom{n+d}{n} \leq \binom{2d}{d}$ , since  $d \geq n$ .

Let  $A = k[x_1, \dots, x_n]$  be the polynomial ring with a fixed monomial order. For any polynomial  $f \in A$ , we will denote by  $a_f$  the tuple of all the coefficients of  $f$ . When the complexity of  $I$  is at most  $d$ , and  $I = (f_1, \dots, f_s)$ , by adding zeroes if necessary, we may always assume that  $s = D$ , where  $D$  is the number defined above. Then, the ideal  $I$  can be encoded by a tuple of the form

$$a_I = \left( n, \underset{\substack{\text{D coefficients} \\ \text{of } f_1}}{\text{-----}}, \dots, \underset{\substack{\text{D coefficients} \\ \text{of } f_s}}{\text{-----}} \right) \in \mathbb{N} \times k^{D^2},$$

where the monomials are listed according to the fixed monomial order. Conversely, given one of those tuples,  $a$ , we can always reconstruct the ideal it comes from. This ideal we shall denote by  $\mathcal{I}(a)$ . Similarly, if  $R$  is a  $k$ -algebra with complexity at most  $d$ , then  $R$  can be written as  $k[x_1, \dots, x_n]/\mathcal{I}(a)$ . We will express this fact as  $R = \mathcal{R}(a)$ .

Let  $M$  be an  $R$ -module. If the complexity degree of  $M$  is at most  $d$ , then the minimal number of generator for  $M$  is bounded in function of  $d$ . If the complexity degree of  $M$  is at most  $d$ , then  $M$  can be encoded by a tuple  $v = (n_1, n_2)$ , where  $n_1$  is a code for  $N_1$  and  $n_2$  is a code for  $N_2$ . We will write this as  $M \cong \mathcal{M}(v)$ . Note that the complexity degree of  $M$  is smaller than or equal to its complexity (as it was defined in 5), when  $M$  is a finitely generated  $R$ -module. In fact, if  $M$  has complexity at most  $d$ , then exists an exact sequence  $R^t \xrightarrow{\Gamma} R^s \rightarrow M \rightarrow 0$ , with  $s, t \leq d$ , where all the entries of the matrix  $\Gamma$  are polynomials (or quotients of polynomials, in the local

case) with degree at most  $d$ . So,  $M$  is a quotient  $R^s/N$  with  $N = \text{im}(\Gamma)$ , both of them free  $R$ -modules with degree type at most  $d$ .

Reciprocally, if  $M$  has complexity degree at most  $d$ , then there exists a number  $D$  that only depends on  $d$  such that  $M$  has complexity at most  $D$ . We then say that both complexities are mutually bounded, and we may use one notion or the other.

### 1.4.1 Equational criterion for flatness

First, let us recall the definition of flatness. An  $R$ -module  $S$  is *flat* if for every monomorphism  $M' \rightarrow M$  of  $R$ -modules, the induced map  $S \otimes_R M' \rightarrow S \otimes_R M$  is again a monomorphism. Now, an  $R$ -module  $S$  is *faithfully flat* if it is *flat* and for any non-zero  $R$ -module  $N$ ,  $S \otimes_R N$  is non-zero. A ring homomorphism  $R \rightarrow S$  is called *flat*, respectively *faithfully flat*, if  $S$  is flat, respectively faithfully flat, as  $R$ -module.

We will need an equational criterion for flatness that we discuss next.

Let us first introduce the following notation. Given an  $R$ -module  $M$ , and tuples  $\underline{b}_i$  in  $R^n$ , an  $M$ -linear combination of the  $\underline{b}_i$  is a tuple in  $M^n$  of the form  $m_1 \underline{b}_1 + \cdots + m_n \underline{b}_n$ , where  $m_i \in M$ . We will denote by  $\text{gen}(\underline{b}_i)_M$  the set of such a linear combinations. Given a linear equation (or a system of linear equations)  $\mathcal{L}: a_{i1}Y_1 + \cdots + a_{in}Y_n = a_i$  with  $a_{ij}, a_i \in R$ , let us denote  $\text{Sol}_M(\mathcal{L})$  the  $R$ -submodule of  $M^n$  of all the solutions in  $M$  of  $\mathcal{L}$ .

**Theorem 6.** *An extension of rings  $R \rightarrow S$  is faithfully flat if and only if for every equation  $\mathcal{L}: a_1Y_1 + \cdots + a_nY_n = a$ , with  $a_i, a \in R$  we have that  $\text{Sol}_S(\mathcal{L}) = \text{Sol}_R(\mathcal{L}) + \text{gen}(\underline{b}_i : i = 1, \dots, l)_S$ , and thus  $\text{Sol}_R(\mathcal{L}) \neq \emptyset$ , if  $\text{Sol}_S(\mathcal{L}) \neq \emptyset$ , where  $\underline{b}_i$  with  $i = 1, \dots, l$  is a set of generators for  $\text{Sol}_R(\mathcal{L}')$ , where  $\mathcal{L}'$  is the homogeneous equation associated to  $\mathcal{L}$ .*

*Proof.* See ([5] Proposition 13, page 36 ) or ( [30] Theorem 3.3.1, page 39). □

This theorem is also true if we replace  $\mathcal{L}$  by a finite system of linear equations.

Now, let  $K$  be an ultrafield, i.e., a field of the form  $K = \text{Ulim } k_w$ . Let us denote by  $\underline{X} = (x_1, \dots, x_n)$  an  $n$ -tuple of indeterminates. *The ultraproduct of the  $k_w[\underline{X}]$  is called an ultra-hull of  $K[\underline{X}]$ , and it is denoted as  $U(K[\underline{X}])$  [30]. There exists a natural embedding of  $(\text{Ulim } k_w)[\underline{X}]$  into  $U(K[\underline{X}])$ , by sending  $(\text{Ulim } a_w)(\underline{X}) \mapsto \text{Ulim}(a_w \underline{X})$  [30]. With this notation, we can state the*

following fundamental result which can be regarded as a form of the *Van Den-Dries-Schmidt's Theorem* (see [27] and [30], Theorem 4.2.2, page 55).

**Theorem 7.** *The ring extension  $K[\underline{X}] \rightarrow U(K[\underline{X}])$  is faithfully flat. Moreover, the expansion of any prime ideal  $P \subset K[\underline{X}]$  into  $U(K[\underline{X}])$  is again a prime ideal.*

This theorem can be generalized to the case of a  $K$ -algebra essentially of finite type, i.e., a localization at a prime ideal of a finitely generated  $K$ -algebra [30]. As an application of this theorem one can obtain the following corollary.

**Corollary 1.** *Given  $d > 0$ , there exists a formula  $IdMem_d$  such that for any field  $k$ , any ideal  $I \subset k[x_1, \dots, x_n]$  and any  $k$ -algebra  $R$ , both of complexity at most  $d$  over  $k$ , it holds that  $f \in IR$  if and only if  $k \models IdMem_d(a_f, a_I)$ . Here  $a_f$ , and  $a_I$  denotes codes for  $f$  and  $I$  respectively.*

We recall that if  $\phi(\xi)$  is a formula with free variable  $\xi$  and parameters from a ring  $R$ , then  $a \in |\phi|_R$  means  $R \models \phi(a)$ , see [24], Definition 1.1.6.

For the convenience of the reader, we present the proof of this corollary as given in [31], Remark 2.3. and [30], Theorem 4.4.1, page 59.

*Proof.* The following assertion imply immediately the result.

**Assertion.** *There exists  $D \geq 0$ , that only depends on  $d$ , such that for any field  $k$ , any ideal  $I \subset k[x_1, \dots, x_n]$  and any  $k$ -algebra  $R$ , both of complexity at most  $d$  over  $k$ , if  $f$  is a polynomial of complexity less than  $d$  with  $f \in I$ , then it is possible to write  $f = h_1 f_1 + \dots + h_s f_s$ , with each  $h_i$  of complexity less than  $D$ . In fact, let us suppose on the contrary that we cannot find such a bound. Then, for each  $w$  there would exist a field  $k_w$ ,  $I_w = (f_{1w}, \dots, f_{sw}) \subset k_w[x_1, \dots, x_n]$ , an ideal of complexity less than  $d$  over  $k_w$ , and  $f_w \in I_w$  also of complexity smaller than  $d$ , such that, if  $f_w = h_{1w} f_{1w} + \dots + h_{sw} f_{sw}$ . Then some  $h_{iw}$  must have complexity bigger than  $w$ . Let us denote by  $f, h_{i\infty}$ , and by  $f_i$  the respective ultraproducts of  $f_w, h_{iw}$ , and  $f_{iw}$ . We note that  $f, f_i, i = 1, \dots, s$  may be regarded as polynomials (of bounded degree by  $d$ ) in  $K[x_1, \dots, x_n]$ , where  $K = \text{Ulim} k_w$ .*

*Then, the following equation holds in  $U(K[\underline{x}])$ :  $f = h_{1\infty} f_1 + \dots + h_{s\infty} f_s$ , with  $h_{i\infty} \in U(K[\underline{x}])$ . That is, the linear equation  $f_1 Y_1 + \dots + f_s Y_s = f$  has a solution in  $U(K[\underline{x}])$ . By Theorems 6 and 7, there must exist a solution  $h_1, \dots, h_s \in K[\underline{x}]$ . By taking  $D = \max\{\text{complexity}(h_i) : i = 1, \dots, s\}$*



we get from Loś's Theorem a solution for  $f_1Y_1 + \dots + f_sY_s = f$  of complexity bounded by  $D$  for almost every  $w$ , which is a contradiction.

So,  $f \in IR$  if and only if there exist polynomials  $h_i$  of complexity at most  $D$ , such that  $f = h_1f_1 + \dots + h_sf_s$ . This can be expressed using a first order formula in the language of rings.  $\square$

**Remark 3.** Using Corollary 1, it is easy to get for each  $d$ , formulas  $Inc_d$  and  $Equal_d$  such that if  $R$  is a finitely generated  $K$ -algebra with complexity at most  $d$ , and if  $J$  and  $I$  are ideals of  $R$  with complexity less than  $d$ , then  $(a_I, a_J) \in |Inc_d|_K$  (resp.  $(a_I, a_J) \in |Equal_d|_K$ ) if and only if  $I$  is included in  $J$ ,  $I \subset J$ , (resp.  $I = J$ ).

Also from theorem 7, may be deduced the following theorem.

**Theorem 8.** ([30] Theorem 4.4.4) For any pair of integers  $d, n > 0$ , there exists a bound  $b = b(d, n)$  such that for any field  $k$  and any ideal  $P \subset k[x_1, \dots, x_n]$  of complexity at most  $d$  we have:  $P$  is a prime ideal if and only if for any two polynomials  $f, g$  of complexity at most  $b$  which do not belong to  $P$  then neither does their product.

**Remark 4.** Given  $d, n > 0$  there exists a formula  $Prime_d$  such that for any field  $k$  and any ideal  $P \subset k[x_1, \dots, x_n]$  of complexity at most  $d$  we have:  $P$  is a prime ideal if and only if  $k \models Prime_d(a_P)$ . Where  $a_P$  is a code for  $P$ .

The existence of this formula follows from the last theorem, and from Corollary 1.

**Example 5.** Let  $K$  be an algebraic closed field of characteristic 0,  $P \subset K[x_1, \dots, x_n]$  a prime ideal of complexity at most  $d$ , and  $a_P$  a code for  $P$ . So,  $K \models \exists(\xi)Prime_d(\xi)$ ; namely,  $Prime_d(a_P)$  holds in  $K$ . By Lefschetz's Principle  $\mathbb{F}_p^{alg} \models \exists(\xi)Prime_d(\xi)$  for all  $p > m$ , for some  $m$ .

On the other hand, If  $a'_{P'}$  a tuple in  $\mathbb{F}_p^{alg}$  for which the sentence  $\exists(\xi)Prime_d(\xi)$  is true in  $\mathbb{F}_p^{alg}$ , for a fix prime number  $p > m$ , then, by decoding  $a'_{P'}$ , we may find a prime ideal  $P' \subset \mathbb{F}_p^{alg}[x_1, \dots, x_n]$  with complexity at most  $d$ .

**Example 6.** Given  $d, n > 0$  there exists a formula  $MaxIdeal_{d,n}$  such that for any algebraic closed field  $K$  and any ideal  $m \subset K[x_1, \dots, x_n]$  of complexity at most  $d$  we have:

$m$  is a maximal ideal if and only if  $K \models MaxIdeal_{d,n}(a_m)$ , where  $a_m$  is a code for  $m$ . In

fact, by the Nullstellensatz  $m$  is maximal if and only if there exist  $b_1, \dots, b_n \in K$  such that  $m = (x_1 - b_1, \dots, x_n - b_n)$ . Let us call  $J = (x_1 - b_1, \dots, x_n - b_n)$ . Then, the required formula is:

$$\text{MaxIdeal}(\xi) : (\exists b_1, \dots, b_n)(\text{Equal}_d(\xi, a_J)),$$

where  $\xi$  and  $a_J$  must be replaced by the codes  $a_m$  of  $m$ , and  $a_J$  of  $J$ , respectively.

**Theorem 9.** ([30] Theorem 4.4.6) For any pair of integers  $d, n > 0$ , there exists a bound  $b = b(d, n)$  such that for any field  $k$ , and any ideal  $I \subset k[x_1, \dots, x_n]$  of complexity at most  $d$ , its radical  $J = \text{Rad}(I)$  has complexity at most  $b$ . Moreover,  $J^b \subset I$ , and  $I$  has at most  $b$  distinct minimal primes all of which are generated by polynomials of degree at most  $b$ .

**Example 7.** Given  $d, n > 0$ , there exists a formula  $\text{Rad}_d$  such that for any field  $k$  and any pair of ideals  $P, I \subset k[x_1, \dots, x_n]$  of complexity at most  $d$ , with  $P$  a prime ideal containing  $I$ , we have: the radical of  $I$  is  $P$ ,  $\text{Rad}(I) = P$  if and only if  $k \models \text{Rad}_d(a_I, a_P)$ . Here  $a_I, a_P$  are codes for  $I$  and  $P$  respectively.

In fact, by last theorem we know there exists a bound  $b = b(d, n)$  that only depends on  $d$  and  $n$  such that  $P^b \subset I$ . But this is equivalent to saying that  $\text{Rad}(I) = P$ , since  $\text{Rad}(I)$  is the intersection of all prime ideals containing  $I$ . It is then sufficient for the formula  $\text{Rad}_d$  to express that the product of any set of  $b$  elements between the bounded generators of  $P$  lies in  $I$ . This can be done by means of a first order formula, by using Corollary 1.

**Lemma 1.** ([31] Lemma 3.2) For each  $d > 0$ , there is a bound  $D = D(d)$  with the following property. Let  $T$  be an affine (local) ring of complexity at most  $d$ . Let  $M$  and  $M'$  be submodules of  $T^d$  of degree type at most  $d$ . Then the degree type of  $(M :_T M') = \{t \in T \mid tM' \subset M\}$  is bounded by  $D$ .

In particular, if  $T$  is an affine (local) ring of complexity at most  $d$ , and  $J \subset T$  is an ideal of complexity at most  $d$ , then we deduce that  $\text{Ann}_T J := (0 :_T J)$  has complexity at most  $D = D(d)$ , that only depends of  $d$ .

## 1.5 Asymptotic form of Koh's conjecture

In this section we will give an *asymptotic* proof of Koh's Conjecture in prime characteristic. This conjecture states the following (see [20] where it originally appeared):

**Conjecture.** *Let  $R$  be a Noetherian ring,  $R \subset S$  a module-finite extension of rings such that the projective dimension of  $S$  as an  $R$ -module is finite,  $\text{Pd}_R(S) < \infty$ . Then, there exists a retraction  $\rho : S \rightarrow R$ . By a retraction we mean an  $R$ -linear homomorphism satisfying  $\rho(1) = 1$ .*

When  $R$  contains a field of characteristic 0, it is known that this conjecture is true (see [34]). There are counterexamples for local equicharacteristic rings of prime characteristic, and for rings of mixed characteristic (see [34]). However, at the end of this section *we will prove that the set of prime numbers for which there are counterexamples of a fixed bounded complexity is finite*. More precisely:

**Theorem 10.** *Given  $d > 0$ , there exists a prime  $p_d$  such that for any field  $k$  of characteristic  $p > p_d$ , and any module finite extension  $R \subset S$  of local  $k$ -algebras with complexity at most  $d$  over  $k$ , minimal number of generators of  $S$  as  $R$ -module less than  $d$  and  $\text{Pd}_R(S) < d$ , the extension has a retraction  $\rho : S \rightarrow R$ .*

First, we start by recalling the following definition.

**Definition 4.** *A local ring  $(R, m)$  is called Gorenstein if:*

1.  *$R$  is Cohen Macaulay (CM), see [11], page 456.*
2. *If  $\{x_1, \dots, x_d\}$  is any system of parameters for  $R$ , and  $\overline{R} = R/(x_1, \dots, x_d)$ , then the socle of  $\overline{R}$ ,  $\text{Soc}(\overline{R})$ , defined as  $\text{Ann}_{\overline{R}}(m)$ , is 1-dimensional as an  $R/m$ -vector space, see [11], page 526.*

**Observation 1.** *If  $R$  is a Gorenstein ring, and if  $J \subset \overline{R}$  is an ideal, then any generator  $\overline{u}$  of  $\text{Soc}(\overline{R})$  is in  $J$ .*

*Proof.* Since  $J \subset \overline{m}$ , there is a minimal number  $t$  such that  $m^t J = 0$  in  $\overline{R}$ . If  $z \in m^{t-1} J$  with  $z \neq 0$  then, obviously,  $mz = 0$ . Therefore,  $z = \alpha u$ , with  $\alpha$  invertible, because  $R$  is Gorenstein. In this way, we obtain that  $u = \alpha^{-1} z \in m^{t-1} J \subset J$ . □

**Notation.** *If  $M$  is an  $R$ -module, we will denote its dual,  $\text{Hom}_R(M, R)$ , by  $M^*$ .*

**Theorem 11.** *([13], page 67) Let  $(R, m) \hookrightarrow (T, \eta)$  be an module-finite extension of local rings with  $T$  a free  $R$ -module. If  $T/mT$  is Gorenstein, and  $J \subset T$  is an ideal, there exists a retraction  $\rho : T/J \rightarrow R$  if and only if  $\text{Ann}_T(J) \not\subseteq mT$ .*

*Proof.* This result appears in the thesis of Danny Gomez [13]. However, for the convenience of the reader we include the complete proof. We divide the proof in three steps.

1. Let us note that  $T^*$  is both an  $R$ -module and a  $T$ -module, with  $t\lambda(x) = \lambda(tx)$ , for  $t \in T$ , and  $\lambda \in T^*$ . Let  $u_0 \in T$  be any lifting of a generator of  $Soc(T/mT)$ ; that is,  $\bar{u}_0 \in T/mT$  is a generator of  $Soc(T/mT)$ .

Obviously,  $u_0 \notin mT$ . Since  $T$  is a free  $R$ -module, there exist elements  $u_1, \dots, u_n \in T$  such that  $\beta = \{u_0, u_1, \dots, u_n\}$  is a basis for  $T$  as an  $R$ -module. Let  $\phi : T \rightarrow T^*$  be the  $T$ -homomorphism, defined as  $\phi(t) = tu_0^*$ , where  $\{u_0^*, u_1^*, \dots, u_n^*\}$  is the dual basis associated to  $\beta$ .

**Assertion.**  $\phi$  is an isomorphism of  $T$  modules.

Recall the following fact. If  $\phi : F_0 \rightarrow F_1$  is an  $R$  homomorphism between free  $R$ -modules with the same rank, and  $\bar{\phi} : F_0/mF_0 \rightarrow F_1/mF_1$  is an isomorphism, then  $\phi$  is also an isomorphism. Therefore, it is enough to show that  $\bar{\phi}$  is an isomorphism. For this purpose, we can show that  $\bar{\phi}$  is injective, because both  $T/mT$  and  $T^*/mT^*$  are free modules of the same rank.

If  $\bar{\phi}$  were not injective, then  $Ker(\bar{\phi})$  would be a non-zero ideal of  $\bar{T}$ , then  $\bar{u}_0 \in Ker(\bar{\phi})$ . So  $u_0 u_0^* \in mT^*$ . Then  $u_0 u_0^* = a_0 u_0^* + \dots + a_n u_n^*$ , with  $a_i \in m$ . Evaluating at the value 1 we would have  $u_0 u_0^*(1) = u_0 = a_0 u_0^*(1) + \dots + a_n u_n^*(1) \in mR$ , which is a contradiction!

2. Let us consider the sequence  $0 \rightarrow J \rightarrow T \rightarrow T/J \rightarrow 0$ . Applying  $*$  we get

$$\begin{array}{ccccccc} 0 & \longrightarrow & (T/J)^* & \longrightarrow & T^* & \longrightarrow & J^* \\ & & \downarrow & & \psi = \phi^{-1} \downarrow & & \\ & & Ann_T(J) & \longrightarrow & T & & \end{array}$$

**Assertion.**  $\psi((T/J)^*) = Ann_T(J)$  or, equivalently,  $\phi(Ann_T(J)) = (T/J)^*$

If  $t \in Ann_T(J)$ , then  $\phi(t) = tu_0^*$ . Now, if  $j \in J$  then  $tu_0^*(j) = u_0^*(tj) = u_0^*(0) = 0$ . That is,  $\phi(t)$  restricted to  $J$  is equal to 0. Therefore, if  $\lambda = \phi(t)|_J$ , then  $\lambda$  may be viewed as an element of  $(T/J)^*$ .

Conversely, let  $\lambda : T \rightarrow R$  be a morphism such that  $\lambda(J) = (0)$ . Since  $\phi : T \rightarrow T^*$  is an isomorphism, then, there exist  $t_\lambda \in T$  such that  $\phi(t_\lambda) = \lambda$ , i.e. ,  $\lambda = t_\lambda u_0^*$ . Inasmuch as  $\lambda(j) = 0$ , for every  $j \in J$ , we see that  $t_\lambda u_0^*(jt') = 0$ , for all  $t' \in T$  and  $j \in J$ . Then,  $jt_\lambda u_0^*(t') = 0$ , for all  $t' \in T$ , since  $J$  is an ideal of  $T$ . Now,  $(jt_\lambda)u_0^* \equiv 0$  in  $T^*$ ; but given that  $\phi$  is an isomorphism, then it must be that  $jt_\lambda = 0$ . In this way,  $t_\lambda \in \text{Ann}_T(J)$ .

3. Let us see that there exists an  $R$ -linear homomorphism  $\rho : T/J \rightarrow R$  if and only if  $\text{Ann}_T(J) \not\subseteq mT$ .

“ $\Rightarrow$ ” Suppose that there exists  $\rho : T/J \rightarrow R$  with  $1 \mapsto 1$ . Let  $t_\rho \in T$  be the unique element such that  $t_\rho u_0^* = \rho$ . Given that  $\rho \in (T/J)^*$ , then we have  $t_\rho \in \text{Ann}_T(J)$ .

**Assertion.**  $t_\rho \notin mT$ .

Arguing by contradiction: Suppose that this were not the case. Then,  $t_\rho = a_0 u_0 + \cdots + a_n u_n$  with  $a_j \in m$ . So,  $t_\rho u_0^* = a_0 u_0 u_0^* + \cdots + a_n u_n u_0^*$ ; evaluating at 1 we get  $1 = \rho(1) = t_\rho u_0^*(1) = \sum_j a_j u_j u_0^*(1) \in m$ , which is a contradiction!

“ $\Leftarrow$ ” Now, suppose that the image of  $\text{Ann}_T(J)$  in  $T/mT$ ,  $\overline{\text{Ann}_T(J)}$ , is different from zero. As  $\bar{u}_0 \in \overline{\text{Ann}_T(J)}$ , there exists  $t_0 \in \text{Ann}_T(J)$  such that  $\bar{u}_0 = \bar{t}_0$ . Therefore,  $u_0 = t_0 + \sum_{i=0} a_i u_i$ , and obviously,  $t_0 = u_0 - \sum_{i=0} a_i u_i$ . Define  $\tilde{\rho} := t_0 u_0^* \in (T/J)^*$ . It follows that  $\tilde{\rho} = u_0 u_0^* - \sum_{i=0} a_i u_i u_0^*$ , and  $\tilde{\rho}(1) = 1 - b$ , with  $b \in m$ . Thus,  $\rho := \frac{1}{1-b} \tilde{\rho}$  satisfies the required conditions.

□

**Theorem 12** (Koh in characteristic zero). *Let  $R$  be a ring containing  $\mathbb{Q}$ , and let  $R \subset S$  be a module-finite extension of rings such that the projective dimension of  $S$  as an  $R$ -module is finite,  $\text{Pd}_R(S) < \infty$ . Then, there exists a retraction  $\rho : S \rightarrow R$ .*

*Proof.* See [34]

□

**Observation 2.** *Let us consider a local ring  $(R, m)$ ,  $R \hookrightarrow S$  a module-finite extension, and let  $s_1, \dots, s_n \in S$  be generators of  $S$  as an  $R$ -module, i.e.,  $S = Rs_1 + \cdots + Rs_n$ . For each  $s_i \in S$  choose any monic polynomial with coefficients in  $R$  that  $s_i$  satisfies, say  $f_i(t) = t^{d_i} + r_{i1}t^{d_i-1} + \cdots + r_{id_i}$ , with  $r_{ij} \in R$ . Let  $T = R[T_1, \dots, T_n]/(f_1(T_1), \dots, f_n(T_n))$ , and let  $\phi$  be the induced homomorphism  $\phi : T \rightarrow S$ . Denote by  $J$  the kernel of  $\phi$ . Then clearly  $S \cong T/J$ .*

Using the above notation, it is possible to give a criterion for the existence of retractions in module-finite extensions.

**Theorem 13.** *Let  $(R, m)$  be a local ring and  $R \hookrightarrow S$  a module-finite extension, given as above. The homomorphism  $R \hookrightarrow T/J$  given by the inclusion  $R \hookrightarrow S$  splits (i.e., there exists a retraction) if and only if  $\text{Ann}_T(J)$  is not contained in  $mT$ .*

*Proof.* It follows immediately from Theorem 11. □

The following theorem states that given  $i \geq 0$  and  $d > 0$ , then there exists a formula  $(\text{Tor}_i)_d$  such that for any field  $k$ ,  $k$ -algebra  $R$  and  $R$ -modules  $M, N, V$  all of them of complexities at most  $d$ , then  $\text{Tor}_i^R(M, N) \cong V$  if and only if  $(\text{Tor}_i)_d$  evaluated in codes of  $R, M, N$  and  $V$  is true over  $k$ . And also an analogue for  $\text{Ext}$ .

**Theorem 14.** *Given  $i \geq 0, d > 0$ , there exist formulas  $(\text{Tor}_i)_d$  and  $(\text{Ext}^i)_d$  with the following properties: let  $k$  be any field; then, if a tuple  $(a, m, n, v)$  is in  $|(\text{Tor}_i)_d|_k$  (respectively, in  $|(\text{Ext}^i)_d|_k$ ), then  $\mathcal{M}(v)$  is isomorphic to  $\text{Tor}_i^{A(a)}(\mathcal{M}(m), \mathcal{M}(n))$  (respectively to  $\text{Ext}_{A(a)}^i(\mathcal{M}(m), \mathcal{M}(n))$ ). Moreover, for each tuple  $(a, m, n)$  we can find at least one  $v$  such that  $(a, m, n, v)$  belongs to  $|(\text{Tor}_i)_d|_k$  (respectively, to  $|(\text{Ext}^i)_d|_k$ ).*

*Proof.* See [31] Corollary 4.4, page 150. □

We recall the following standard result.

**Theorem 15.** *Let  $(R, m)$  be a local ring, and denote by  $K$  the residue field  $R/m$ . If  $M$  is a finitely generated  $R$ -module, then  $\text{Pd}_R(M) \leq n$  if and only if  $\text{Tor}_{n+1}^R(M, K) = 0$ .*

It is clear from the previous theorems that there exists a formula  $(\text{Pd}_{<n})_d$  such that, if  $M = \mathcal{M}(v)$  is an  $R = \mathcal{R}(a)$ -module with complexity less than  $d$ , where  $(R, m)$  is a finitely generated local affine  $K$ -algebra with complexity less than  $d$ , then  $K \models (\text{Pd}_{<n})_d(a, v)$ , if and only if,  $\text{Pd}_R(M) \leq n$ .

Now, we state one of our main results:

**Theorem 16.** *For each  $d > 0$  there exists a first order formula  $\text{Koh}_d$  such that if  $(R, m, k)$  is a local, finitely generated  $k$ -algebra with  $k$ -complexity at most  $d$ , and if  $S$  is a module-finite extension of  $R$  with minimal number of generator as  $R$ -module less than  $d$  and projective dimension  $\text{Pd}_R(S) < d$ , with  $k$ -complexity at most  $d$ , then, Koh's conjecture is true for  $R$  and  $S$  (i.e., there exists a retraction  $\rho : S \rightarrow R$ ) if and only if  $k \models \text{Koh}_d(a, b)$ , where  $R \cong \mathcal{R}(a)$  and  $S \cong \mathcal{S}(b)$ .*

*Proof.* From the last observation we may suppose that  $S \cong T/J$ , where the complexity of  $J$  and  $T$  is less than  $d$ . Moreover, in view of the characterization for the existence of retractions, we know that there is a retraction  $\rho$  if and only if  $\text{Ann}_T(J) \not\subseteq mT$ .

As we already discussed, there is a formula  $(\text{Pd}_{<n})_d$  such that if  $R = \mathcal{R}(a)$ , and  $S = \mathcal{R}(b)$ . Then,  $k \models \text{Pd}_{<n}(a, b)$  if and only if  $\text{Pd}_R(S) < n$ .

Let  $\text{Koh}_d$  be the formula which establishes: if  $\text{Pd}_R(S) < d$ , then  $\text{Ann}_T(J) \not\subseteq mT$ , i.e.,

$$\text{Koh}_d(\xi, \xi', \nu, \nu') : \bigvee_{i=0}^{d-1} \text{Pd}_R(\xi, \nu) = i \longrightarrow \neg \text{Inc}_d(\nu', \xi').$$

Where  $\nu'$  and  $\xi'$  are reserved for a code to  $\text{Ann}_T(J)$ , and  $mT$ , respectively.

It is clear that  $k \models \text{Koh}_d(a, a', b, b')$  if and only if there exist a retraction  $\rho : S \rightarrow R$ .  $\square$

*Proof.* (Of Theorem 10.)

From Theorem 12, we see that  $k \models \text{Koh}_d(a, b)$  for any zero characteristic field  $k$ . Then, by Proposition 1, we deduce that  $\mathbb{F}_p \models \text{Koh}_d(a, b)$ , for every field  $\mathbb{F}_p$  of prime characteristic  $p$  sufficiently large. More precisely, we have: Given  $d > 0$ , there exists a prime number  $p_d$  such that for any field  $k$  of characteristic  $p > p_d$ , and any modulo-finite extension  $R \subseteq S$  of local  $k$ -algebras with complexity at most  $d$  over  $k$ , with minimal number of generators of  $S$  as  $R$ -modulo less than  $d$ , and with  $\text{Pd}_R(S) < d$ , there exists a retraction  $\rho : S \rightarrow R$ .  $\square$

## 1.6 A non-Standard proof of a Theorem of Hochster

In this section we give a non-standard proof of the following theorem, see [14].

**Theorem 17.** *Let  $S$  be a finitely generated  $K$ -algebra domain, where  $K$  is any field of characteristic zero. Let  $m \subset S$  be a maximal ideal with height  $n$ . Suppose  $\{F_\alpha(\underline{x}, \underline{y})\}$ , with  $\alpha = 1, \dots, l$ , is a polynomial system of equations with coefficients in  $\mathbb{Z}$ , and that  $(\underline{x}, \underline{y}) = (x_1, \dots, x_n, y_1, \dots, y_m)$  is a tuple of elements in  $S$  such that:*

1.  $\text{Rad}(\underline{x}) = m$ .
2.  $F_\alpha(\underline{x}, \underline{y}) = 0$ , for every  $\alpha$ .
3.  $K \subset S \xrightarrow{\pi} S/m$  is an isomorphisms.

Then, there exists a field  $L$  of prime characteristic, a finitely generated  $L$ -algebra  $S'$ ,  $m'$  a maximal ideal of  $S'$  of height  $n$ , and elements  $(\underline{x}', \underline{y}') = (x'_1, \dots, x'_n, y'_1, \dots, y'_m)$  in  $S'$  such that:

1.  $\text{Rad}(\underline{x}') = m'$ .
2.  $F_\alpha(\underline{x}', \underline{y}') = 0$ , for all  $\alpha$ .
3.  $L \xrightarrow{i} S' \xrightarrow{\pi} S'/m'$ , with  $\pi \circ i$  an isomorphism.

Moreover, the characteristic  $p > 0$  of  $L$  can be chosen equal to any prime number not contained in some finite set.

This Theorem was proved by M. Hochster, ([14]).

Let us start with a result taken from [31].

**Theorem 18.** ([31], Proposition 5.1.) For each  $d, h > 0$ , there exists a formula  $\text{Height}_d = h$  such that for any field  $k$ , any finitely generated  $k$ -algebra  $R$  of complexity at most  $d$ , and any ideal  $I \subset R$  of complexity at most  $d$ , it holds that: The height of  $I$  is equal to  $h$  if and only if  $(a, b) \in |\text{Height}_d = h|_k$ , where  $a, b$  are codes for  $R$  and  $I$  respectively.

**Example 8.** Let  $K$  be an algebraic closed field of characteristic 0, let  $I \subset K[x_1, \dots, x_n]$  be an ideal of height  $h$  and complexity at most  $d$ . Let  $a_I$  be a code for  $I$  (so that,  $K \models \exists(\xi)(\text{Height}_d(\xi) = h)$ , namely  $\text{Height}_d(a_I) = h$ , holds in  $K$ ). By Lefschetz's Principle  $\mathbb{F}_p^{\text{alg}} \models \exists(\xi)(\text{Height}_d(\xi) = h)$ , for all  $p > m$ , for some integer  $m$ . Let  $a'_I$  be a tuple in  $\mathbb{F}_p^{\text{alg}}$  for which, after substitution, the sentence  $\exists(\xi)(\text{Height}_d(\xi) = h)$  holds true in  $\mathbb{F}_p^{\text{alg}}$  for  $p > m$ . Then, by decoding  $a'_I$ , we may find an ideal  $I' \subset \mathbb{F}_p^{\text{alg}}[x_1, \dots, x_n]$  of height  $h$  and with complexity at most  $d$ .

**Lemma 2.** Let  $S = K[T_1, \dots, T_\nu]/I$  be a integral domain over an algebraic closed field  $K$  of characteristic 0, where  $I \subset K[T_1, \dots, T_\nu]$  is a prime ideal of  $K$ -complexity at most  $d$ . Let  $m \subset K[T_1, \dots, T_\nu]$  be a maximal ideal with  $K$ -complexity at most  $d$  and height  $n$  in  $S$ . That is,



$I \subset m$ , and  $ht(m) = \nu = n + ht(I)$  in  $K[T_1, \dots, T_\nu]$ . Suppose  $\{F_\alpha(\underline{x}, \underline{y})\}_{\alpha=1, \dots, l}$  is a polynomial system of equations with coefficients in  $\mathbb{Z}$ , and that  $(\underline{x}, \underline{y}) = (x_1, \dots, x_n, y_1, \dots, y_m)$  is a tuple of elements in  $S$  such that:

1.  $\text{Rad}(\underline{x}) = m$  in  $S$ .
2.  $F_\alpha(\underline{x}, \underline{y}) = 0$ , for all  $\alpha = 1, \dots, l$ .

Then, we can always construct a  $\mathbb{F}_p^{\text{alg}}$ -algebra  $S' = \mathbb{F}_p^{\text{alg}}[T_1, \dots, T_\nu]/I'$ , with  $I' \subset \mathbb{F}_p^{\text{alg}}[T_1, \dots, T_\nu]$  a prime ideal of  $\mathbb{F}_p^{\text{alg}}$ -complexity at most  $d$ , such that:

1. There exists  $m' \subset \mathbb{F}_p^{\text{alg}}[T_1, \dots, T_\nu]$ , a maximal ideal with  $\mathbb{F}_p^{\text{alg}}$ -complexity at most  $d$  and height  $n$  in  $S'$ , i.e.,  $I' \subset m'$  and  $ht(m') = \nu = n + ht(I')$  in  $\mathbb{F}_p^{\text{alg}}[T_1, \dots, T_\nu]$ .

There exists  $(\underline{x}', \underline{y}') = (x'_1, \dots, x'_n, y'_1, \dots, y'_m)$ , a tuple of elements in  $S'$  such that:

1.  $\text{Rad}(\underline{x}') = m'$  in  $S'$ .
2.  $F_\alpha(\underline{x}', \underline{y}') = 0$ , for all  $\alpha = 1, \dots, l$ .

*Proof.* The hypothesis above may be expressed by means of a first order formula  $\Phi_d$  such that when we evaluate on the codes of  $S, m, (\underline{x}, \underline{y}), \dots$ , respectively, it is true that  $K \models \Phi_d$  if and only if  $m$  is a maximal ideal of height  $n$  in  $S$ ,  $I$  is a prime ideal content in  $m$ , and (1), (2) are satisfied. This formula may be explicitly given as:

$$\Phi_d : (\exists a_m, a_I, a_{(\underline{x}, \underline{y})})((\text{Prime}_d(a_I) \wedge \text{MaxIdeal}_d(a_m) \wedge \text{Inc}_d(a_I, a_m) \wedge \text{Height}_d(a_m) = \nu \wedge \text{Height}_d(a_I) = \nu - n \wedge \text{Rad}_d(a_{\underline{x}}, a_m) \wedge \text{IdMem}_d(F_\alpha(\underline{x}, \underline{y}), a_I))$$

Now, by Leftchetz's principle,  $K \models \Phi_d$ , if and only if  $\mathbb{F}_p^{\text{alg}} \models \Phi_d$ , for all prime number  $p$  large enough. As we discussed in Examples 7,6, 5, 8 and Remark 3 there are tuples in  $\mathbb{F}_p^{\text{alg}}$   $a'_m, a'_I, a'_{(\underline{x}, \underline{y})}, \dots$  which codify a maximal ideal  $m'$ , a prime ideal  $I'$ , and a system of elements  $\underline{x}, \underline{y}$  that satisfy in  $\mathbb{F}_p^{\text{alg}}[T_1, \dots, T_\nu]/I'$  all the required conditions. Then,  $S' = \mathbb{F}_p^{\text{alg}}[T_1, \dots, T_\nu]/I'$  is the required  $\mathbb{F}_p^{\text{alg}}$ -algebra. Moreover, it is clear from the above that  $S'$  may be constructed of characteristic equal to  $p$ , for all prime number large enough.

□

*Proof.* (Of Theorem 17.)

**First step:** Reduction to the case where  $K$  is algebraically closed.

Let  $R$  be a finitely generated  $K$ -algebra domain, where  $K$  is any field of characteristic zero. Let  $m \subset R$  a maximal ideal of height  $n$ , and let  $x_1, \dots, x_n$  be elements in  $R$  such that  $\text{Rad}(x_1, \dots, x_n) = m$ , and such that conditions 1-3 hold in  $R$ . Let  $\overline{K}$  be an algebraic closure of  $K$ , and define  $R' = \overline{K} \otimes_K R$ . We notice that  $R \rightarrow R'$  is a faithfully flat extension, and therefore  $R$  injects into  $R'$ . Moreover,  $mR' \cap R = m$  ([25] Theorem 7.5, (2), page 49). Consequently, there is a prime ideal  $q \subset R'$  such that  $q \cap R = m$ . We notice that  $q$  has to be maximal: Since  $R$  is a finitely generated  $K$ -algebra domain, all its maximal ideal have the same height, equal to the Krull dimension of  $R$ . Hence, by Noether Normalization Theorem, there are algebraically independent elements  $a_1, \dots, a_n$  in  $R$  such that  $A = K[a_1, \dots, a_n] \subset R$  is a module-finite extension. But this implies that  $R' \subset \overline{K} \otimes_K R$  is also module-finite extension, and consequently  $\dim(\overline{K} \otimes_K R) = \dim R$ . From this, we see that  $q$  has to be a maximal ideal in  $R'$ .

Now, in  $R'_q$ , the ideal  $mR'_q$  is  $qR'_q$ -primary. Thus, there is a power  $n > 0$  such that  $q^n R'_q \subset mR'_q$ . On the other hand, there is a power  $l > 0$ , such that  $m^l R \subset (x_1, \dots, x_n)R$ . Thus,  $q^{n+l} R'_q \subset (x_1, \dots, x_n)R'_q$ . After inverting a finite number of elements in  $R'$  we may assume that by localizing at a single element  $u \in R' - q$ , the inclusion  $q^{n+l} R'_u \subset (x_1, \dots, x_n)R'_u$  still holds. We let  $R''$  be the localized ring  $R'_u$ .

This ring is a finitely generated  $\overline{K}$ -algebra extension of  $R$  of the same dimension. Moreover, the ideal  $m'' = qR''$  is maximal, and  $q^{n+l} R'' \subset (x_1, \dots, x_n)R''$ . Therefore,  $\text{Rad}(x_1, \dots, x_n)R'' = m''R''$ . Let  $Q \subset R''$  be a minimal prime ideal of  $R''$  included in  $m''$ , and such that  $\dim(R''/Q) = \dim R''$ . Thus, if we let  $S$  be the ring  $R''/Q$ , and let  $\eta = m''S$ , then,  $S$  is a f.g.  $\overline{K}$ -algebra domain, with  $ht(\eta) = n$ , and  $\text{Rad}(x_1, \dots, x_n)S = \eta S$ . Thus, condition 1 holds in  $S$ .

Besides, since there is a ring homomorphism  $R \rightarrow S$ , it is then clear that condition 2 also holds in  $S$ . Finally, the Nullstellensatz implies that condition 3 is true in  $S$ . So, we may replace  $R$  by  $S$ .

**Second step:**

Let us take a presentation for  $S$ , say  $S = K[T_1, \dots, T_\nu]/I$ . Since  $S$  is a integer domain, we have that  $I \subset K[T_1, \dots, T_\nu]$  is a prime ideal. By the hypothesis, there exists a maximal ideal  $m \subset K[T_1, \dots, T_\nu]$  with height  $n$  in  $S$ . That is,  $ht(m) = \nu = n + ht(I)$  in  $K[T_1, \dots, T_\nu]$ , and

there exists a tuple of elements in  $S$ ,  $(\underline{x}, \underline{y}) = (x_1(\underline{t}), \dots, x_n(\underline{t}), y_1, \dots, y_m(\underline{t}))$  such that:

1.  $Rad(\underline{x}) = m$
2.  $F_\alpha(\underline{x}, \underline{y}) = 0$ , for all  $\alpha = 1, \dots, l$
3. Let us note that the condition that  $K \subset S \xrightarrow{\pi} S/m$  is an isomorphism is trivially satisfied, since we are supposing that  $K$  is algebraically closed.

Let  $d > 0$  be an integer that bounds all the complexities of the objects mentioned above.

The proof follows from Lemma 2.

□

## Chapter 2

# Frobenius Algebras

In this chapter we will adhere to techniques very close to those developed in [1]. In that article, the authors, working within the setting of the formal power series ring in  $n$  variables, were able to prove several cases in which the Frobenius algebra is principal, or infinitely generated. Their work was very much inspired by that of M. Katzman ([18]). We will deal with the same problem in the context of polynomial rings.

### 2.1 Some preliminaries about Frobenius Algebras

Let  $R$  be a ring of characteristic  $p$ , and  $e \geq 0$  be any integer. For any  $R$ -module  $M$  we define  $\mathcal{F}^e(M) = \text{Hom}^e(M, M)$ , the set of maps from  $M$  to  $M$  which are  $r^{p^e}$ -linear; that is,  $\varphi$  is in  $\mathcal{F}^e(M)$  if it satisfies  $\varphi(rx) = r^{p^e}\varphi(x)$ , for all  $r \in R$ ,  $x \in M$ .

Consider the  $e$ -th Frobenius homomorphism  $f^e : R \rightarrow R$ , given by  $f^e(r) = r^{p^e}$ , and let  $F_*^e R$  denote the ring  $R$  with the product given by the Frobenius morphism. That is,  $x \cdot r = r^{p^e}x$ , for  $r \in R$ ,  $x \in F_*^e R$ .

When  $e = 1$ , the *Frobenius skew polynomial ring* over  $R$ ,  $R[x, f]$ , is the left  $R$ -module freely generated by  $(x^i)_{i \in \mathbb{N}}$ . That is, it consists of all polynomial  $\sum r_i x^i$ , but with multiplication given by the rule:  $xr = f(r)x = r^p x$  for all  $r \in R$ , see [26]. For any  $R$ -module  $M$ , we define  $F^e(M) = F_*^e R \otimes_R M$ , where  $F_*^e R$  is regarded as a right  $R$ -module. For example,

$$r^{p^e} x \otimes m = x \cdot r \otimes m = x \otimes rm.$$

We think of  $F^e(M)$  as a left  $R$ -module with the product  $r \cdot (s \otimes m) = rs \otimes m$ . The functor  $F^e(-)$  is called *the  $e$ -th Frobenius functor*.

In what follows, we will use the following natural identification:

$$\boxed{\mathcal{F}^e(M) \cong \text{Hom}_R(F^e(M), M)} \quad (2.1)$$

Given  $\varphi \in \mathcal{F}^e(M)$ , we may consider  $\psi \in \text{Hom}_R(F^e(M), M)$ , defined as  $\psi(r \otimes m) = r\varphi(m)$ . And, reciprocally, if we have  $\psi \in \text{Hom}_R(F^e(M), M)$ , we may define  $\varphi \in \mathcal{F}^e(M)$  as  $\varphi(m) = \psi(1 \otimes m)$ .

**Definition 5.** Let  $(R, m)$  be a local ring of characteristic  $p > 0$ , and let us denote by  $E = E_R(R/m)$  the injective hull of the residue field [11]. We define the Frobenius algebra of  $E$  as

$$\boxed{\mathcal{F}(E) = \bigoplus_{e \geq 0} \mathcal{F}^e(E)}$$

We note that  $\mathcal{F}(E)$  is a  $\mathbb{N}$ -graded algebra over  $F^0(E)$ , where given  $\varphi \in \mathcal{F}^e(E)$ , and  $\psi \in \mathcal{F}^{e'}(E)$ , the map  $\varphi \cdot \psi = \varphi \circ \psi$  is an element of  $\mathcal{F}^{e+e'}(E)$ , since  $\varphi \circ \psi(rx) = \varphi(r^{p^{e'}} \psi(x)) = r^{p^{e+e'}} \varphi \circ \psi(x)$ .

Now,  $\mathcal{F}^0(E) = \text{Hom}^0(E, E) = \text{Hom}_R(E, E) = E^\vee$ . It is well known that when  $(R, m)$  is a complete local ring, the Matlis dual of  $E$  is isomorphic to  $R$ , see [45]. Therefore, when  $(R, m)$  is a complete local ring we have that  $F^0(E) = R$ , and, hence,  $\mathcal{F}(E)$  is an  $R$ -algebra.

The following theorem is taken from [18]. We include it for the sake of completeness. First, we need the following definitions: Let  $A$  be a commutative ring of characteristic  $p$ , and  $I \subset A$  be an ideal. Let us define

$$F = \bigoplus_{e \geq 0} (I^{[p^e]} : I) f^e = \bigoplus_{e \geq 0} F_e f^e,$$

the  $\mathbb{N}$ -graded  $A$ -algebra with the following product: for  $u f^e \in F_e f^e$ , and  $u' f^{e'} \in F_{e'} f^{e'}$ , then,  $u f^e u' f^{e'} = u(u'^{p^e} f^{e+e'})$ . Let  $L_e = \sum F_{e_1} F_{e_2}^{[p^{e_1}]} \dots F_{e_s}^{[p^{e_1+\dots+e_{s-1}}]}$ , with  $1 \leq e_1, \dots, e_s < e$  and  $e_1 + \dots + e_s = e$ , and let us define  $F_{<e}$  as the subalgebra of  $F$  generated by  $F_0 f^0, \dots, F_{e-1} f^{e-1}$ .

With those notations we have:

**Theorem 19.** (*Katzman Criterion*)  $(F_{<e}) \cap F_e f^e = L_e f^e$ .

*Proof.* Let  $u \in F_{<e} \cap F_e f^e$  be an element. Then  $u$  is a sum of products of the form  $u_{e_1} \cdots u_{e_s}$ , where  $u_{e_j} \in F_{e_j} f^{e_j}$ , and  $e_1 + \cdots + e_s = e$ , i.e.,  $u_{e_j} = a_{e_j} f^{e_j}$ . Therefore,

$$u = a_{e_1} f^{e_1} a_{e_2} f^{e_2} \cdots a_{e_s} f^{e_s} = a_{e_1} a_{e_2}^{p^{e_1}} \cdots a_{e_s}^{p^{e_1 + \cdots + e_{s-1}}} f^{e_1 + \cdots + e_s}$$

which clearly lies in  $L_e f^e$ .

Conversely, if  $a_{e_1} \in F_{e_1}$ ,  $a_{e_2}^{p^{e_1}} \in F_{e_2}^{p^{e_1}}$ , and  $x \in I$  then, for some  $u_{ij} \in I$  we have

$$x a_{e_1} a_{e_2}^{p^{e_1}} = \left( \sum r_i u_i^{p^{e_1}} \right) a_{e_2}^{p^{e_1}} = \sum r_i (u_i a_{e_2})^{p^{e_1}} = \sum r_i \left( \sum r_j u_{ij}^{p^{e_2}} \right)^{p^{e_1}} = \sum r_{ij} u_{ij}^{p^{e_1 + e_2}} \in I^{p^{e_1 + e_2}}.$$

Inductively, if  $a_{e_1} a_{e_2}^{p^{e_1}} \cdots a_{e_s}^{p^{e_1 + \cdots + e_{s-1}}} \in F_{e_1} F_{e_2}^{[p^{e_1}]} \cdots F_{e_s}^{p^{e_1 + \cdots + e_{s-1}}}$ , and  $x \in I$ , it follows that

$$x a_{e_1} a_{e_2}^{p^{e_1}} \cdots a_{e_s}^{p^{e_1 + \cdots + e_{s-1}}} \in I^{p^{e_1 + \cdots + e_s}}.$$

That is,

$$F_{e_1} F_{e_2}^{[p^{e_1}]} \cdots F_{e_s}^{[p^{e_1 + \cdots + e_{s-1}}]} \subseteq (I^{[p^{e_1 + \cdots + e_s}]} : I) = (I^{[p^e]} : I)$$

Then,  $L_e f^e \subseteq F_e f^e$ . On the other hand, if  $u = u_{e_1} \cdots u_{e_s} \in L_e$ , with  $u_{e_j} \in F_{e_j}^{[p^{e_1 + \cdots + e_{j-1}}]}$ , then,  $u_{e_j} = (u'_{e_j})^{p^{e_1 + \cdots + e_{j-1}}}$ , therefore,  $u f^e = u'_{e_1} f^{e_1} u'_{e_2} f^{e_2} \cdots u'_{e_s} f^{e_s} \in F_{<e}$ . □

## 2.2 Openness of the finitely generated locus of the Frobenius Algebra

The following natural question arises: For a complete local ring  $(R, m)$ , is the Frobenius algebra  $\mathcal{F}(E)$  a finitely generated  $R$ -algebra? The answer in general is *no*, as shown in [18].

There, it is shown that for the complete local ring  $R = K[[x, y, z]]/(xy, xz)$ , where  $K$  is a field of prime characteristic, the Frobenius algebra  $\mathcal{F}(E)$  is not finitely generated as an  $R$ -algebra.

In spite of that negative result, another interesting question may be posed: Is the locus

$$U = \{P \in \text{Spec}(R) : \mathcal{F}(E_{R_p}) \text{ is a finitely generated } R_p\text{-algebra}\}$$

open in the Zariski Topology? This seems to be a very difficult question. *We will prove the above conjecture in the case of a ring of the form  $R = K[x_1, \dots, x_n]/I$ , where  $I \subset K[x_1, \dots, x_n]$  is a square-free monomial ideal.*

Before we tackle this problem, we first recall the following standard fact: Let  $(R, m)$  be a complete local ring of prime characteristic  $p$ , and let  $S = R/I$  be a quotient by some ideal  $I \subset R$ . We denote  $E_R = E_R(R/m)$ , and  $E_S = E_S(S/mS)$ . Then, the injective hull of  $S/mS$  can be obtained as  $\text{Hom}_R(S, E_R) \cong \text{Ann}_{E_R} I$ . Therefore,  $E_S = \text{Ann}_{E_R} I \subset E_R$ , see [15], Lemma 3.2.

**Proposition 2.** ([19], Proposition 4.1) *With the above notation.*

$$\mathcal{F}^e(E_S) \cong \frac{(I^{[p^e]} : I)}{I^{[p^e]}}$$

and therefore

$$\mathcal{F}(E_S) = \bigoplus_{e \geq 0} \frac{(I^{[p^e]} : I)}{I^{[p^e]}} f^e$$

Where the multiplication on the right hand side is given by  $xf^e \cdot yf^{e'} = xy^{p^e} f^{e+e'}$ .

*Proof.* Take  $\varphi \in \mathcal{F}^e(E_S)$ . By (2.1), we may think of  $\varphi$  as an element of  $\text{Hom}_R(F^e(E_S), E_S)$ . Applying the duality functor  $\vee = \text{Hom}_R(\_, E_R)$  to  $\varphi$ , we get  $\varphi^\vee : E_S^\vee \rightarrow F^e(E_S)^\vee \cong F^e(E_S^\vee)$ , (see [23], Lemma 4.1, for the last isomorphism). But by Matlis duality we have  $E_S^\vee = (S^\vee)^\vee \cong S$ . Moreover, it is not difficult to see that  $F^e(S) = F^e(R/I) \cong R/I^{[p^e]}$ .

Therefore, we may identify  $\varphi^\vee$  with a map  $\varphi^\vee : R/I \rightarrow R/I^{[p^e]}$ . Now, if  $\bar{u} = \varphi^\vee(\bar{1})$  then the homomorphism  $\varphi^\vee$  is just multiplication by  $u$ . We note that since  $\varphi^\vee$  is well defined, this implies that  $u \in (I^{[p^e]} : I)$ .

Define the  $R$ -homomorphism  $\lambda : (I^{[p^e]} : I) \rightarrow \mathcal{F}^e(E_S)$  as  $\lambda(u) = \psi^\vee$ , where  $\psi : R/I \rightarrow R/I^{[p^e]}$  is the homomorphism given by multiplication by  $u$ .

The  $R$ -homomorphism  $\lambda$  is surjective as we saw above; and clearly,  $\text{Ker}(\lambda) = I^{[p^e]}$ .

Therefore,  $\mathcal{F}^e(E_S) \cong (I^{[p^e]} : I)/I^{[p^e]}$ . □

**Lemma 3.** ([1], Lemma 2.2) *With the same notation as above. Suppose there is an element  $u \in R$  such that for all  $e \geq 0$*

$$(I^{[p^e]} :_R I) = I^{[p^e]} + (u^{p^e-1}).$$

*Then, there is an isomorphism of  $S$  algebras  $\mathcal{F}(E_S) \cong S[u^{p-1}\theta, f]$ . Here,  $S[u^{p-1}\theta, f]$  denotes the 1-th skew polynomial ring in the variable  $u^{p-1}\theta$ , (see [26], page 285).*

*Proof.* We have:

$$\mathcal{F}(E_S) = \bigoplus_{e \geq 0} \frac{(I^{[p^e]} : I)}{I^{[p^e]}} f^e = \bigoplus_{e \geq 0} \frac{I^{[p^e]} + (u^{p^e-1})}{I^{[p^e]}} f^e = \bigoplus_{e \geq 0} (u^{p^e-1}) f^e$$

On the other hand:

$$S[u^{p-1}\theta, f] := S \oplus Su^{p-1}\theta \oplus S(u^{p-1}\theta)^2 \oplus (Su^{p-1}\theta)^3 \oplus \dots = S \oplus Su^{p-1}\theta \oplus Su^{p^2-1}\theta^2 \oplus Su^{p^3-1}\theta^3 \oplus \dots$$

Define the  $S$  homomorphism

$$\Psi : \bigoplus_{e \geq 0} (u^{p^e-1}) f^e \longrightarrow \bigoplus_{e \geq 0} S(u^{p-1}\theta)^e$$

by  $\Psi(su^{p^e-1}f^e) = s(u^{p-1}\theta)^e$ . This is clearly an isomorphism of  $S$ -algebras. □

Now, let  $R = k[[x_1, \dots, x_n]]$  be the formal power series ring where  $k$  denotes a field of characteristic  $p > 0$  and  $I \subset R$  is a square-free monomial ideal. Then, its minimal primary decomposition  $I = I_{\alpha_1} \cap \dots \cap I_{\alpha_s}$  is given in terms of face ideals. That is, if  $\alpha = (a_1, \dots, a_n) \in \{0, 1\}^n$ , then  $I_\alpha = (x_i | a_i \neq 0)$ . Suppose that the sum of ideals  $\sum_{1 \leq i \leq s} I_{\alpha_i}$  is equal to  $(x_1^{b_1}, x_2^{b_2}, \dots, x_n^{b_n})$ , where  $\beta = (b_1, \dots, b_n) \in \{0, 1\}^n$ . Let us abbreviate  $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n}$  by  $x^\beta$ . In ([1], Proposition 3.2) the authors showed that

$$(I^{[p^e]} :_R I) = I^{[p^e]} + J_{p^e} + (x^\beta)^{p^e-1}, \quad (2.2)$$

for any  $e \geq 0$ , where  $J_{p^e}$  is either the zero ideal, or its generators are monomials  $x^\zeta = x_1^{c_1} \dots x_n^{c_n}$  which satisfy  $c_i \in \{0, p^e - 1, p^e\}$ , for some  $c_i = p^e$ ,  $c_j = p^e - 1$ ,  $c_k = 0$ ,  $1 \leq i, j, k \leq n$ .

Notice that by knowing  $(I^{[p]} :_R I)$  we will readily know  $(I^{[p^e]} :_R I)$ , for any  $e \geq 0$ .

**Theorem 20.** ([1], Theorem 3.5) *With the previous notation and assumptions:*

*Let  $I \subset R$  be a square-free monomial ideal, let  $u = x^\beta$ , and let  $S = R/I$ . Then,*

1.  $\mathcal{F}(E_S) \cong S[u^{p-1}\theta, f]$  is principally generated when  $J_p = 0$ .
2.  $\mathcal{F}(E_S)$  is infinitely generated when  $J_p \neq 0$ .



*Proof.* The first statement is clear by Lemma 3. For the second part, we will assume, without loss of generality, and only with the purpose of simplifying the presentation, that  $\beta = (1, \dots, 1)$  and  $J_p$  has a generator of the form  $x^\zeta = x_1^p x_2^{p-1} x_4^{c_4} \dots x_n^{c_n}$  with  $c_i \in \{0, p-1, p\}$ . Let  $e \geq 1$  be any integer and  $1 \leq e_1, \dots, e_s < e$  such that  $e_1 + \dots + e_s = e$ . Then,

$$x^{\zeta_e} = x_1^{p^e} x_2^{p^e-1} x_4^{C_4} \dots x_n^{C_n} \in J_{p^e} \subseteq \mathcal{F}_e(E_S) := (I^{[p^e]} :_R I)$$

with  $C_i \in \{0, p^e - 1, p^e\}$ ,  $i = 4, \dots, n$  (and obviously,  $x^{\zeta_e} \in \mathcal{F}_{<e}$ ). We will show that  $x^{\zeta_e} \notin L_e$ , so by Katzman's criterion  $\mathcal{F}(E_S)$  cannot be finitely generated.

With this purpose, let us see that

$$x^{\zeta_e} \notin \mathcal{F}_{e_1} \mathcal{F}_{e_2}^{[p^{e_1}]} \mathcal{F}_{e_3}^{[p^{e_1+e_2}]} \dots \mathcal{F}_{e_s}^{[p^{e_1+e_2+\dots+e_{s-1}}]}.$$

From (2.2) it is enough to show that

$$x^{\zeta_e} \notin G_{e_1} G_{e_2}^{[p^{e_1}]} G_{e_3}^{[p^{e_1+e_2}]} \dots G_{e_s}^{[p^{e_1+e_2+\dots+e_{s-1}}]},$$

where  $G_e := (x_1^{p^e} x_2^{p^e-1} x_4^{C_4} \dots x_n^{C_n})$ . But, let us note that the exponent of  $x_1$  in the generator of this product is

$$p^{e_1+(e_1+e_2)+\dots+(e_1+e_2+\dots+e_s)} > p^{e_1+e_2+\dots+e_s} = p^e,$$

which is certainly impossible. □

Now we are in position to prove our main theorem.

**Theorem 21.** *Let  $R = k[x_1, \dots, x_n]$  be the polynomial ring in  $n$  variables, where  $k$  is a field of prime characteristic  $p > 0$ . Let us define  $S = R/I$ , where  $I \subset R$  is a square-free monomial ideal. Then the locus  $U' = \{Q \in \text{Spec}(S) : \mathcal{F}(E_{S_Q}) \text{ is a finitely generated } S_Q\text{-algebra}\}$  contain the open  $U = \text{Spec}(S) \setminus V((I^{[p]} + J_p)/I^{[p]})$ .*

*Proof.* In fact, we will show that  $U = \text{Spec}(S) \setminus V((I^{[p]} + J_p)/I^{[p]})$ .

Let  $Q \in \text{spec}(S) \setminus V((I^{[p]} + J_p)/I^{[p]})$  be a prime ideal. Let  $E_{\widehat{S_Q}}$  denote the injective hull of the residue field of  $\widehat{S_Q}$ , where  $\widehat{S_Q}$  is the completion of  $S_Q$  with respect to its maximal ideal  $QS_Q$ . A basic theoretical result, see [45], says that  $E_{\widehat{S_Q}} \cong E_{S_Q}$ . Let us define  $M := (I^{[p]} + J_p)/I^{[p]}$ . Note

that if  $Q \notin \text{supp}(M)$ , then  $0 = M_Q = (I^{[p]} + J_p)/I^{[p]} \otimes_S S_Q$ , therefore  $(I^{[p]} : I)/I^{[p]} \otimes_S S_Q \cong (x^\beta)_Q^{p-1}$ . So we can write

$$\begin{aligned} \mathcal{F}(E_{S_Q}) &\cong \mathcal{F}(E_{\widehat{S}_Q}) \cong \bigoplus_{e \geq 0} \frac{(I^{[p^e]} \widehat{S}_Q : I \widehat{S}_Q)}{I^{[p^e]} \widehat{S}_Q} f^e \cong \bigoplus_{e \geq 0} \frac{(I^{[p^e]} : I)}{I^{[p^e]}} f^e \otimes_S \widehat{S}_Q \\ &\cong \bigoplus_{e \geq 0} (x^\beta)^{p^e - 1} f^e \end{aligned}$$

Which is finitely generated, by Lemma 3.

□

## Chapter 3

# On the cohomology of $G$ -Graded Twisted Algebras

In this chapter we will present an explicit formula to compute the exact number of graded isomorphism classes of associative  $G$ -graded twisted algebras over a field  $k$ , when  $G$  is a finite abelian group. We achieve this by computing the cohomology group  $H^2(G, A)$ , where  $A \subset k^*$  is certain multiplicative closed subset of  $k^*$ , viewed as a  $G$ -module via the trivial action, when  $G$  is given as a direct product  $G \simeq G_1 \times \cdots \times G_k$ , with each  $G_i$  a finite cyclic group of order  $n_i$ .

### 3.1 Some preliminaries on $G$ -graded twisted algebras

The standard reference for this material is [35]. Since this is a relatively new area of research, not very well known in the literature, we have included in this section all the main definitions and theorems (without proof) as they appear in [35].

The motivation for the study of  $G$ -graded twisted algebras arise in theoretical physics [40], [41], [42], [43], [44], and [10]. These algebras were introduced in [9], and also in [39]. To put the material of this chapter in perspective, the reader may consult [8], [28], [29], [36], and [37] for a more general study of nonassociative algebras, generalizations of Lie algebras and  $G$ -graded twisted *division* algebras.

We shall be interested only in the case of algebras over a field, that in our case will be  $\mathbb{R}$  or  $\mathbb{C}$ . Thus, we start from the following definition (in [35],  $k$  is taken more generally to be a commutative ring).

**Definition 6.** ([35]) Let  $G$  denote a group. Let  $W$  be an algebra over a commutative field  $k$ . We will say that  $W$  is a  $G$ -graded twisted algebra (not necessarily commutative neither associative) if there exists a  $G$ -grading  $W = \bigoplus_{g \in G} W_g$ , with  $W_a W_b \subset W_{ab}$ , where each summand  $W_g$  is a one dimensional vector space over  $k$ . We demand that  $W$  has no monomial zero divisors. This last condition means that for each pair of nonzero elements  $w_a \in W_a$  and  $w_b \in W_b$ ,  $w_a w_b \neq 0$ . We also assume that  $W$  has an identity element  $1 = w_e \in W_e$ , where by  $e$  we denote the identity element of the group  $G$ .

We observe that since each graded component  $W_g$  is a one dimensional vector space over  $k$ , we may choose a basis  $B = \{w_g : g \in G\}$  for  $W$  as a  $k$ -vector space. In [35], page 2, the authors introduced the following definition.

**Definition 7.** For any fixed basis  $B$  as above define the structure constant with respect to  $B$ ,  $C_B : G \times G \rightarrow k^*$ , where  $k^* = k - \{0\}$ , as the function that for any pair of elements  $w_a \in W_a$ ,  $w_b \in W_b$ , satisfies  $w_a w_b = C_B(a, b) w_{ab}$ .

Some properties that may easily verified follow immediately from this definition:

1.  $w_a w_e = C_B(a, e) w_a$ , implies  $C_B(a, e) = 1$ , for all elements  $a$  in  $G$ .
2.  $C_B$  must take values in a subgroup  $A$  of the multiplicative group  $k^*$ , since  $W$  has no monomial zero divisors. We will omit the subscript  $B$ , it is clear from the context.
3. If  $q : G \times G \rightarrow A^*$ , and  $r : G \times G \times G \rightarrow A^*$  are functions defined as:

$$\begin{aligned} q(a, b) &= C(a, b)C(b, a)^{-1} \\ r(a, b, c) &= C(b, c)C(ab, c)^{-1}C(a, bc)C(a, b)^{-1} \end{aligned} \tag{3.1}$$

then, for all  $a, b, c$  in  $G$  it holds that  $w_a(w_b w_c) = r(a, b, c)(w_a w_b)w_c$ ; and that  $w_a w_b = q(a, b)w_b w_a$ , if  $G$  is abelian. Notice that  $W$  is commutative or associative if and only if  $q \equiv 1$ , respectively,  $r \equiv 1$ . The authors in [35] showed that  $\partial_2 C = r$ . Taking advantage

of this fact, they managed to identify graded isomorphism classes of associative  $G$ -graded twisted algebras with elements in the second cohomology group  $H_2(G, A)$ , see Remark 5, and Theorem 24.

**Definition 8.** ([35], Definition 2) A morphism between two  $G$ -graded twisted algebras  $W = \bigoplus_{g \in G} W_g$  and  $V = \bigoplus_{g \in G} V_g$  we mean an unitarian homomorphism of  $k$ -algebras  $\phi : W \rightarrow V$ . If it also preserves the grading, i.e.,  $\phi(W_g) \subset V_g$ , we say the morphism is graded.

Moreover,  $W$  and  $V$  are isomorphic as *graded* algebras, if there are *graded* morphisms  $\phi : W \rightarrow V$  and  $\psi : V \rightarrow W$  such that  $\phi\psi$  and  $\psi\phi$  are both the identity.

Throughout this chapter *it will be assumed that  $G$  is a finite group.*

Our next objective is to count how many isomorphism classes (under graded homomorphisms) of associative, graduate twisted algebras over a field are there when  $G$  is a finite *abelian* group. We introduce the fundamental tool.

## 3.2 Group Cohomology

For this section the reader may consult [3], [4]. We start by recalling some basic definitions.

Let  $G$  be a group and  $A$  a  $G$ -module. Consider the left exact functor from the category of  $G$ -modules,  $G\text{-mod}$ , to the category  $Ab$  of abelian groups, defined as  $A \rightarrow A^G$ , where  $A^G = \{a \in A : g \cdot a = a \text{ for all } g \in G\}$ . For a given a morphism of  $G$ -modules  $f : A \rightarrow B$ ,  $f^G : A^G \rightarrow B^G$  is defined as the morphism of abelian groups given by  $f^G(a) = f(a)$ .

We write  $H^*(G, A)$  for its right derived functor.  $H^*(G, A)$  is called the *cohomology groups of  $G$  with coefficients in  $A$* , see [3] and [4]. It is not difficult to see that if we consider  $\mathbb{Z}$  as a trivial  $G$ -module then we then have that  $A^G \cong \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ , and therefore  $H^*(G, A) \cong \text{Ext}_{\mathbb{Z}[G]}^*(\mathbb{Z}, A)$  (see [6], Chapter III).

We recall the following material concerning the standard projective resolution of  $\mathbb{Z}[G]$ -modules, when  $\mathbb{Z}$  is viewed as a  $G$ -module with the trivial action. This resolution is used to compute  $\text{Ext}_{\mathbb{Z}[G]}^*(\mathbb{Z}, A)$ , and hence it is a valuable tool for computing the cohomology groups of  $G$  with coefficients in  $A$ .

### 3.2.1 Some standard free resolutions

For the sake of completeness, we have included some standard results, as presented in [6].

Define  $F_n$  as the free abelian group generated by the elements  $(g_0, g_1, \dots, g_n) \in G^{n+1}$ , and consider the boundary  $\mathbb{Z}$ -homomorphisms  $\partial_n : F_n \rightarrow F_{n-1}$  given by

$$\partial_n(g_0, \dots, g_n) = \sum_{i=0}^n (-1)^i (g_0, \dots, g_{i-1}, \widehat{g_i}, g_{i+1}, \dots, g_n).$$

An straightforward computation shows that  $\partial_{n-1} \circ \partial_n = 0$ . Thus, there is a complex of free  $\mathbb{Z}$ -modules

$$\cdots \longrightarrow F_n \xrightarrow{\partial_n} F_{n-1} \xrightarrow{\partial_{n-1}} F_{n-2} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\partial_1} F_0 \longrightarrow 0 \quad (3.2)$$

Note that  $F_0 = \mathbb{Z}[G]$ . Now, let  $\mathcal{E} : F_0 = \mathbb{Z}[G] \rightarrow \mathbb{Z}$  be the map given as the  $\mathbb{Z}$ -homomorphism that sends every  $g \in G$  to  $1 \in \mathbb{Z}$  (3.2). Consider the augmented complex

$$\cdots \longrightarrow F_n \xrightarrow{\partial_n} F_{n-1} \xrightarrow{\partial_{n-1}} F_{n-2} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\mathcal{E}} \mathbb{Z} \longrightarrow 0 \quad (3.3)$$

We claim that (3.3) is a resolution of free  $\mathbb{Z}$ -modules for  $\mathbb{Z}$ .

Indeed, if  $F_\bullet$  denotes the complex (3.3), let us see that the morphisms of complexes  $id : F_\bullet \rightarrow F_\bullet$  and  $0 : F_\bullet \rightarrow F_\bullet$  are homotopic.

Define  $h_{-1} : \mathbb{Z} \rightarrow F_0$  as  $h_{-1}(1) = e \in G$ , and for  $n = 0, 1, \dots$  define

$$h_n : F_n \rightarrow F_{n+1} \text{ as } h_n(g_0, \dots, g_n) = (e, g_0, \dots, g_n).$$

$$\begin{array}{ccccccc} \cdots & \longrightarrow & F_{n+1} & \xrightarrow{\partial_{n+1}} & F_n & \xrightarrow{\partial_n} & F_{n-1} & \longrightarrow & \cdots & \longrightarrow & F_1 & \xrightarrow{\partial_1} & F_0 & \xrightarrow{\mathcal{E}} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \scriptstyle{0, id} & \swarrow \scriptstyle{h_n} & \downarrow \scriptstyle{0, id} & \swarrow \scriptstyle{h_{n-1}} & \downarrow \scriptstyle{0, id} & & & & \downarrow \scriptstyle{0, id} & \swarrow \scriptstyle{h_0} & \downarrow \scriptstyle{0, id} & \swarrow \scriptstyle{h_{-1}} & \downarrow \scriptstyle{0, id} & & & \\ \cdots & \longrightarrow & F_{n+1} & \xrightarrow{\partial_{n+1}} & F_n & \xrightarrow{\partial_n} & F_{n-1} & \longrightarrow & \cdots & \longrightarrow & F_1 & \xrightarrow{\partial_1} & F_0 & \xrightarrow{\mathcal{E}} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

It is an easy exercise to check that

$$id - 0 = id = \partial_{n+1} \circ h_n + h_{n-1} \circ \partial_n,$$

for  $n = 0, 1, 2, \dots$ , where  $\partial_0 = \mathcal{E}$ .

Therefore, the induced maps in the homologies are the same, i.e.,  $id : \ker(\partial_n)/\text{im}(\partial_{n+1}) \rightarrow \ker(\partial_n)/\text{im}(\partial_{n+1})$  and

$0 : \ker(\partial_n)/\text{im}(\partial_{n+1}) \rightarrow \ker(\partial_n)/\text{im}(\partial_{n+1})$  are the same maps. Hence,  $\ker(\partial_n)/\text{im}(\partial_{n+1}) = 0$ .

Thus, the complex (3.3) is indeed a resolution of free  $\mathbb{Z}$ -modules for  $\mathbb{Z}$ .

On the other hand, note that each  $F_n$  is a  $G$ -module with the action  $g \cdot (g_0, \dots, g_n) = (gg_0, \dots, gg_n)$ , where  $\mathbb{Z}$  is regarded as a  $G$ -module with the trivial action. Let us see that each  $F_n$  is a free  $\mathbb{Z}[G]$ -module.

We have a natural action of  $G$  over  $G^{n+1}$  (by multiplication on the left). Note that  $(g_0, g_1, \dots, g_n) = g_0 \cdot (e, g_0^{-1}g_1, \dots, g_0^{-1}g_n)$ , and  $(e, g_1, \dots, g_n) \neq g \cdot (e, g'_1, \dots, g'_n)$ , for all  $g \neq e$ .

Therefore, if the orbits are denoted by  $\mathcal{O}_{(e, g_1, \dots, g_n)}$ , with  $g_i \in G$ , for  $i = 1, 2, \dots, n$  it is clear that:

$$G^{n+1} = \bigsqcup_{(g_1, \dots, g_n) \in G^n} \mathcal{O}_{(e, g_1, \dots, g_n)}.$$

Hence,

$$F_n = \mathbb{Z}[G^{n+1}] = \mathbb{Z}[\bigsqcup_{(g_1, \dots, g_n) \in G^n} \mathcal{O}_{(e, g_1, \dots, g_n)}] \cong \bigoplus_{(g_1, \dots, g_n) \in G^n} \mathbb{Z}[\mathcal{O}_{(e, g_1, \dots, g_n)}].$$

But  $\mathcal{O}_{(e, g_1, \dots, g_n)} \cong G/G_{(e, g_1, \dots, g_n)}$ , where

$$G_{(e, g_1, \dots, g_n)} = \{g \in G : g \cdot (e, g_1, \dots, g_n) = (e, g_1, \dots, g_n)\} = \{e\}.$$

Thus,  $\mathcal{O}_{(e, g_1, \dots, g_n)} \cong G$ . We conclude then that

$$F_n \cong \bigoplus_{(g_1, \dots, g_n) \in G^n} \mathbb{Z}[G].$$

Also note that the set  $\{(e, g_1, \dots, g_n) : (g_1, \dots, g_n) \in G^n\}$  is a basis for  $F_n$  as a  $\mathbb{Z}[G]$ -module since each  $(e, g_1, \dots, g_n)$  generates its own orbit  $\mathcal{O}_{(e, g_1, \dots, g_n)}$  and these elements are linear independent.

Finally, what we conclude is that the resolution of free  $\mathbb{Z}$ -modules for  $\mathbb{Z}$  given in (3.3) is actually a resolution of free  $\mathbb{Z}[G]$ -modules for  $\mathbb{Z}$ , viewed as a  $G$ -module with the trivial action.

### The Bar Resolution for $\mathbb{Z}$

We saw above that  $\{(e, g_1, \dots, g_n) : (g_1, \dots, g_n) \in G^n\}$  is a basis for  $F_n$ , as a  $\mathbb{Z}[G]$ -module.

Now, we change this basis for another very useful basis that we will call *the bar basis* for  $F_n$ .

Define  $[g_1|g_2|\dots|g_n] = (e, g_1, g_1g_2, \dots, g_1g_2 \dots g_n)$ .

We claim that the set  $\{[g_1|g_2|\dots|g_n] : (g_1, \dots, g_n) \in G^n\}$  is also a basis for  $F_n$ . In fact, this set is clearly linear independent. On the other hand, there is a bijection between the old

basis  $\{(e, g_1, \dots, g_n) : (g_1, \dots, g_n) \in G^n\}$  and the set  $\{[g_1|g_2|\dots|g_n] : (g_1, \dots, g_n) \in G^n\}$ , since

$$(e, g_1, g_2, \dots, g_n) = (e, g'_1, g'_1 g'_2, \dots, g'_1 g'_2 \dots g'_n) = [g'_1|g'_2|\dots|g'_n],$$

where  $g'_i = g_{i-1}^{-1} g_i$ , for  $i = 1, 2, \dots, n$ .

Therefore  $\{[g_1|g_2|\dots|g_n] : (g_1, \dots, g_n) \in G^n\}$  is a basis for  $F_n$  as a  $\mathbb{Z}[G]$ -module. This base is usually called the *bar basis* for  $F_n$ .

Now, if we compute the boundary homomorphisms  $\partial_n : F_n \rightarrow F_{n-1}$  given in (3.3) in terms of the bar basis, we get the following equation:

$$\begin{aligned} \partial_n([g_1|g_2|\dots|g_n]) &= \partial_n(e, g_1, g_1 g_2, \dots, g_1 g_2 \dots g_n) = (g_1, g_1 g_2, \dots, g_1 g_2 \dots g_n) + \\ &+ \sum_{i=1}^{n-1} (-1)^i (e, g_1, \dots, g_1 g_2 \dots g_{i-1}, \widehat{g_1 g_2 \dots g_i}, g_1 g_2 \dots g_{i+1}, \dots, g_1 g_2 \dots g_n) \\ &+ (-1)^n (e, g_1, g_1 g_2, \dots, g_1 g_2 \dots g_{n-1}) \\ &= g_1 [g_2|\dots|g_n] + \sum_{i=1}^{n-1} (-1)^i [g_1|\dots|g_{i-1}|g_i g_{i+1}|g_{i+2}|\dots|g_n] + \\ &+ (-1)^n [g_1|\dots|g_{n-1}]. \end{aligned}$$

Thus, we have that the boundary operator  $\partial_n : F_n \rightarrow F_{n-1}$  in the bar resolution is given by

$$\partial_n([g_1|\dots|g_n]) = g_1 [g_2|\dots|g_n] + \sum_{i=1}^{n-1} (-1)^i [g_1|\dots|g_{i-1}|g_i g_{i+1}|g_{i+2}|\dots|g_n] + (-1)^n [g_1|\dots|g_{n-1}]. \quad (3.4)$$

The resolution given in (3.3)

$$\dots \longrightarrow F_n \xrightarrow{\partial_n} F_{n-1} \xrightarrow{\partial_{n-1}} F_{n-2} \longrightarrow \dots \longrightarrow F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \quad (3.5)$$

will be called *the bar resolution for  $\mathbb{Z}$* . (Note that  $\{[e] = (e)\}$  is the bar basis for  $F_0$ .)

### 3.2.2 Another way to compute the cohomology of groups

From now on, we consider each  $F_n$  endowed with the bar basis.

For  $n = 0, 1, 2, \dots$  define  $C^n(G, A) = \{\varphi : G^n \rightarrow A\}$ , the set of functions from  $G^n$  to  $A$ , here  $G^0 = \{e\}$ .

$C^n(G, A)$  is an abelian group, since  $A$  is an abelian group and also  $C^n(G, A)$  has a structure of  $G$ -module where  $(g\varphi)(x) = g\varphi(x)$ , for  $g \in G$ , and  $\varphi \in C^n(G, A)$ . Let us see



that  $C^n(G, A)$  is isomorphic to  $\text{Hom}_{\mathbb{Z}[G]}(F_n, A)$  as  $G$ -modules.

Indeed, define

$$\begin{aligned} \mu : C^n(G, A) &\rightarrow \text{Hom}_{\mathbb{Z}[G]}(F_n, A) \\ \varphi &\mapsto \mu(\varphi) \end{aligned}$$

where  $\mu(\varphi)([g_1 | \cdots | g_n]) = \varphi(g_1, \dots, g_n)$ .

It is a  $\mathbb{Z}[G]$ -homomorphism with inverse

$$\begin{aligned} \mu^{-1} : \text{Hom}_{\mathbb{Z}[G]}(F_n, A) &\rightarrow C^n(G, A) \\ \psi &\mapsto \mu^{-1}(\psi) \end{aligned}$$

where  $\mu^{-1}(\psi)(g_1, \dots, g_n) = \psi([g_1 | \cdots | g_n])$ .

Therefore, we have the following commutative diagram:

$$\begin{array}{ccc} \text{Hom}_{\mathbb{Z}[G]}(F_n, A) & \xrightarrow{\partial_{n+1}^*} & \text{Hom}_{\mathbb{Z}[G]}(F_{n+1}, A) \\ \mu \downarrow & & \downarrow \mu \\ C^n(G, A) & \xrightarrow{\partial^n} & C^{n+1}(G, A) \end{array}$$

where  $\partial_{n+1}^*(\psi) = \psi \circ \partial_{n+1}$ ,  $\mu$  is an isomorphism and  $\partial^n = \mu \circ \partial_{n+1}^* \circ \mu^{-1}$ .

If we compute explicitly the morphism  $\partial^n$  we have:

$$\begin{aligned} \partial^n(\varphi)(g_1, \dots, g_{n+1}) &= \mu \circ \partial_{n+1}^* \circ \mu^{-1}(\varphi)(g_1, \dots, g_{n+1}) = \mu \circ \partial_{n+1}^* \circ \varphi([g_1 | \cdots | g_{n+1}]) \\ &= \mu \circ \varphi(\partial_{n+1}([g_1 | \cdots | g_{n+1}])) \end{aligned}$$

and by (3.4)

$$\partial_n([g_1 | \cdots | g_n]) = g_1[g_2 | \cdots | g_n] + \sum_{i=1}^{n-1} (-1)^i [g_1 | \cdots | g_{i-1} | g_i g_{i+1} | g_{i+2} | \cdots | g_n] + (-1)^n [g_1 | \cdots | g_{n-1}].$$

Hence,

$$\begin{aligned} \partial^n(\varphi)(g_1, \dots, g_{n+1}) &= \mu \circ \varphi(\partial_{n+1}([g_1 | \cdots | g_{n+1}])) \\ &= \mu \circ \varphi(\partial_n([g_1 | \cdots | g_{n+1}])) = g_1[g_2 | \cdots | g_{n+1}] + \sum_{i=1}^n (-1)^i [g_1 | \cdots | g_{i-1} | g_i g_{i+1} | g_{i+2} | \cdots | g_{n+1}] + (-1)^{n+1} [g_1 | \cdots | g_n] \\ &= \mu(g_1 \varphi([g_2 | \cdots | g_{n+1}])) + \sum_{i=1}^n (-1)^i \varphi([g_1 | \cdots | g_{i-1} | g_i g_{i+1} | g_{i+2} | \cdots | g_{n+1}]) + (-1)^{n+1} \varphi([g_1 | \cdots | g_n]) \\ &= g_1 \varphi(g_2, \dots, g_{n+1}) + \sum_{i=1}^n (-1)^i \varphi(g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_{n+1}) + (-1)^{n+1} \varphi(g_1, \dots, g_n). \end{aligned} \tag{3.6}$$

As  $H^n(G, A)$  is isomorphic to  $\text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, A)$ , we may compute  $H^n(G, A)$  by taking a resolution of projective  $\mathbb{Z}[G]$ -modules for  $\mathbb{Z}$ , then applying the functor  $\text{Hom}_{\mathbb{Z}[G]}(-, A)$  and finally taking homology.

Using the bar resolution for  $\mathbb{Z}$  we obtain

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \xrightarrow{\partial_{n-1}^*} & \text{Hom}_{\mathbb{Z}[G]}(F_{n-1}, A) & \xrightarrow{\partial_n^*} & \text{Hom}_{\mathbb{Z}[G]}(F_n, A) & \xrightarrow{\partial_{n+1}^*} & \text{Hom}_{\mathbb{Z}[G]}(F_{n+1}, A) & \longrightarrow & \cdots \\ & & & \mu \downarrow & & \mu \downarrow & & \mu \downarrow & & \\ \cdots & \xrightarrow{\partial^{n-2}} & C^{n-1}(G, A) & \xrightarrow{\partial^{n-1}} & C^n(G, A) & \xrightarrow{\partial^n} & C^{n+1}(G, A) & \longrightarrow & \cdots \end{array}$$

where the squares commutes.

Thus,  $\{C^\bullet(G, A), \partial^\bullet\}$  is a complex with

$$\partial^n(\varphi)(g_1, \dots, g_{n+1}) = g_1\varphi(g_2, \dots, g_{n+1}) + \sum_{i=1}^n (-1)^i \varphi(g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_{n+1}) + (-1)^{n+1} \varphi(g_1, \dots, g_n),$$

and consequently

$$H^n(G, A) \cong \text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, A) \cong \frac{\ker(\partial^n)}{\text{im}(\partial^{n-1})}.$$

### 3.3 The computation of $H^2(G, A)$ when $G$ is a finite abelian group and $A$ is a $G$ -module with the trivial action.

When  $G$  is a finite cyclic group we have a particular free resolution of  $\mathbb{Z}[G]$ -modules for  $\mathbb{Z}$ , viewed as a  $G$ -module with the trivial action.

First, we notice that  $\mathbb{Z}[G] \cong \mathbb{Z}[T]/(T^n - 1)$ , where  $n$  is the order of  $G$ . Let us denote this quotient by  $\mathbb{Z}[t]$ , and by  $N$  denote the polynomial  $N = 1 + t + t^2 + \dots + t^{n-1}$ . Then,  $\mathbb{Z} \cong \mathbb{Z}[t]/(t - 1)$  and we there is a free resolution:

$$\cdots \xrightarrow{N} \mathbb{Z}[t] \xrightarrow{t-1} \mathbb{Z}[t] \xrightarrow{N} \mathbb{Z}[t] \xrightarrow{t-1} \mathbb{Z}[t] \xrightarrow{\pi} \mathbb{Z} \longrightarrow 0 \quad (3.7)$$

Omitting  $\mathbb{Z}$ , and applying the contravariant functor  $\text{Hom}_{\mathbb{Z}[t]}(\_, A)$ , where  $A$  is a  $G$ -module with the trivial action ( $g \cdot a = a$ ), we get the following commutative diagram:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & \text{Hom}_{\mathbb{Z}[t]}(\mathbb{Z}[t], A) & \xrightarrow{t-1} & \text{Hom}_{\mathbb{Z}[t]}(\mathbb{Z}[t], A) & \xrightarrow{N} & \text{Hom}_{\mathbb{Z}[t]}(\mathbb{Z}[t], A) & \xrightarrow{t-1} & \text{Hom}_{\mathbb{Z}[t]}(\mathbb{Z}[t], A) & \longrightarrow & \dots \\
& & \lambda_0 \downarrow & & \lambda_1 \downarrow & & \lambda_2 \downarrow & & \lambda_3 \downarrow & & \\
0 & \longrightarrow & A & \xrightarrow{D^0} & A & \xrightarrow{D^1} & A & \xrightarrow{D^2} & A & \longrightarrow & \dots
\end{array} \tag{3.8}$$

where  $\lambda_i : \text{Hom}_{\mathbb{Z}[t]}(\mathbb{Z}[t], A) \rightarrow A$  is the isomorphism given by  $\lambda_i(\varphi) = \varphi(1)$  with inverse  $\lambda_i^{-1} : A \rightarrow \text{Hom}_{\mathbb{Z}[t]}(\mathbb{Z}[t], A)$  give by  $\lambda_i^{-1}(a) = \varphi_a$  with  $\varphi_a(1) = a$  and  $D^j = \lambda_{j+1} \circ \delta_j \circ \lambda_j^{-1}$ , with  $\delta_0 = t-1$ ,  $\delta_1 = N$ ,  $\delta_2 = t-1$ ,  $\delta_3 = N$ ,  $\dots$

Thus,

$$D^1(a) = N\varphi_a(1) = N \cdot a = na.$$

and  $D^2(a) = (t-1)\varphi_a(1) = (t-1) \cdot a = 0$ . Therefore, taking the second homology we obtain:

$$H^2(G, A) \cong \frac{\ker(D^2)}{\text{im}(D^1)} = \frac{A}{nA}.$$

For the general case of a finite abelian group  $G$  we will use the following lemma, see [6]:

**Lemma 4.** *If  $F_\bullet \xrightarrow{\delta_\bullet} \mathbb{Z} \longrightarrow 0$  is a free resolution of  $\mathbb{Z}[G_1]$ -modules, and  $F'_\bullet \xrightarrow{\delta'_\bullet} \mathbb{Z} \longrightarrow 0$  is a free resolution of  $\mathbb{Z}[G_2]$ -modules, the tensor product of these two resolutions, defined as*

$$H_\bullet \xrightarrow{D_\bullet} \mathbb{Z} \longrightarrow 0,$$

where  $H_n = \bigoplus_{i=0}^n F_{n-i} \otimes F'_i$  and if  $a \otimes b \in F_{n-i} \otimes F'_i$

$$D_n(a \otimes b) = \delta_{n-i}(a) \otimes b + (-1)^{n-i} a \otimes \delta'_i(b),$$

is a free resolution of  $\mathbb{Z}[G_1 \times G_2] \cong \mathbb{Z}[G_1] \otimes \mathbb{Z}[G_2]$ -modules.

Suppose that we have  $G = G_1 \times G_2$  where  $G_1$  and  $G_2$  are cyclic groups of orders  $n$  and  $m$  respectively. With the same notation we used above, we have a free resolution of  $\mathbb{Z}[G_1]$ -modules:

$$\dots \xrightarrow{\Delta_3^1} \mathbb{Z}[t] \xrightarrow{\Delta_2^1} \mathbb{Z}[t] \xrightarrow{\Delta_1^1} \mathbb{Z}[t] \xrightarrow{\Delta_0^1} \mathbb{Z}[t] \xrightarrow{\pi} \mathbb{Z} \longrightarrow 0, \tag{3.9}$$

where  $\Delta_{2i}^1 = t-1$  for  $i = 0, 1, 2, \dots$ , and  $\Delta_{2i+1}^1 = N = 1+t+\dots+t^{n-1}$ , for  $i = 0, 1, 2, \dots$ , and a free resolution of  $\mathbb{Z}[G_2]$ -modules

$$\dots \xrightarrow{\delta_3^2} \mathbb{Z}[s] \xrightarrow{\delta_2^2} \mathbb{Z}[s] \xrightarrow{\delta_1^2} \mathbb{Z}[s] \xrightarrow{\delta_0^2} \mathbb{Z}[s] \xrightarrow{\pi} \mathbb{Z} \longrightarrow 0, \tag{3.10}$$

where  $\delta_{2i}^2 = s - 1$  for  $i = 0, 1, 2, \dots$ , and  $\delta_{2i+1}^2 = M = 1 + s + \dots + s^{m-1}$ , for  $i = 0, 1, 2, \dots$ .

By the previous lemma, the tensor product of (4.9) and (4.10), which is

$$\dots \longrightarrow \mathbb{Z}[t, s]^4 \xrightarrow{\Delta_2^2} \mathbb{Z}[t, s]^3 \xrightarrow{\Delta_1^2} \mathbb{Z}[t, s]^2 \xrightarrow{\Delta_0^2} \mathbb{Z}[t, s] \longrightarrow \mathbb{Z} \longrightarrow 0, \quad (3.11)$$

where  $\mathbb{Z}[t, s]$  denotes  $\mathbb{Z}[t] \otimes \mathbb{Z}[s] \cong \mathbb{Z}[G_1 \times G_2]$ , and the morphisms  $D_i$  are given by

$$\begin{aligned} \Delta_0^2(p_1, p_2) &= \Delta_0^1(p_1) + \delta_0^2(p_2) = (t-1)p_1 + (s-1)p_2 \\ \Delta_1^2(p_1, p_2, p_3) &= (\Delta_1^1(p_1) - \delta_0^2(p_2), \Delta_0^1(p_2) + \delta_1^2(p_3)) = (Np_1 - (s-1)p_2, (t-1)p_2 + Mp_3) \\ \Delta_2^2(p_1, p_2, p_3, p_4) &= (\Delta_2^1(p_1) + \delta_0^2(p_2), \Delta_1^1(p_2) - \delta_1^2(p_3), \Delta_0^1(p_3) + \delta_2^2(p_4)) \\ &= ((t-1)p_1 + (s-1)p_2, Np_2 - Mp_3, (t-1)p_3 + (s-1)p_4) \end{aligned} \quad (3.12)$$

is a free resolution of  $\mathbb{Z}[G_1 \times G_2]$ -modules.

We highlight the following equations since they will play an important role in the general case.

$$\boxed{\begin{aligned} \Delta_0^2(p_1, p_2) &= \Delta_0^1(p_1) + \delta_0^2(p_2) \\ \Delta_1^2(p_1, p_2, p_3) &= (\Delta_1^1(p_1) - \delta_0^2(p_2), \Delta_0^1(p_2) + \delta_1^2(p_3)) \\ \Delta_2^2(p_1, p_2, p_3, p_4) &= (\Delta_2^1(p_1) + \delta_0^2(p_2), \Delta_1^1(p_2) - \delta_1^2(p_3), \Delta_0^1(p_3) + \delta_2^2(p_4)) \end{aligned}} \quad (3.13)$$

In the same way, as in (3.8), using resolution (3.11), we get a complex

$$0 \longrightarrow A \xrightarrow{D^0} A^2 \xrightarrow{D^1} A^3 \xrightarrow{D^2} A^4 \longrightarrow \dots$$

such that the homologies of this complex are precisely the cohomology groups  $H^i(G, A)$ , where  $A$  is a  $G$ -module with the trivial action and  $D^i$  are the morphisms induced by the morphisms  $D_i$ .

That is,

$$\begin{aligned} D_2^0(a) &= (\Delta_0^2(e_1) \cdot a, \Delta_0^2(e_2) \cdot a) = ((t-1)a, (s-1)a) = (0, 0) \\ D_2^1(a, b) &= (\Delta_1^2(e_1) \cdot (a, b), \Delta_1^2(e_2) \cdot (a, b), \Delta_1^2(e_3) \cdot (a, b)) \\ &= ((N, 0) \cdot (a, b), (-(s-1), (t-1)) \cdot (a, b), (0, M) \cdot (a, b)) = (na, 0, mb) \\ D_2^2(a, b, c) &= (\Delta_2^2(e_1) \cdot (a, b, c), \Delta_2^2(e_2) \cdot (a, b, c), \Delta_2^2(e_3) \cdot (a, b, c), \Delta_2^2(e_4) \cdot (a, b, c)) \\ &= ((t-1, 0, 0) \cdot (a, b, c), (s-1, N, 0) \cdot (a, b, c), (0, -M, t-1) \cdot (a, b, c), (0, 0, s-1) \cdot (a, b, c)) \\ &= (0, nb, -mb, 0) \end{aligned} \quad (3.14)$$

Therefore,  $\ker(D_2^2) = A \oplus \text{Ann}_A(n) \cap \text{Ann}_A(m) \oplus A$ , and  $\text{im}(D_2^1) = nA \oplus 0 \oplus mA$ .

Hence,

$$H^2(G_1 \times G_2, A) \cong \frac{A}{nA} \oplus \text{Ann}_A(n) \cap \text{Ann}_A(m) \oplus \frac{A}{mA}$$

Note that the following equations are all what we need in order to compute the above morphisms.

$$\begin{aligned} \Delta_0^2(e_1) &= \Delta_0^1(1) \\ \Delta_0^2(e_2) &= \delta_0^2(1) \\ \Delta_1^2(e_1) &= (\Delta_1^1(1), 0) \\ \Delta_1^2(e_2) &= (-\delta_0^2(1), \Delta_0^1(1)) \\ \Delta_1^2(e_3) &= (0, \delta_1^2(1)) \\ \Delta_2^2(e_1) &= (\Delta_2^1(1), 0, 0) \\ \Delta_2^2(e_2) &= (\delta_0^2(1), \Delta_1^1(1), 0) \\ \Delta_2^2(e_3) &= (0, -\delta_1^2(1), \Delta_0^1(1)) \\ \Delta_2^2(e_4) &= (0, 0, \delta_2^2(1)) \end{aligned} \tag{3.15}$$

Now, let us consider  $G = G_1 \times \cdots \times G_k$ , where  $G_i$  is a cyclic group of order  $n_i$ . We obtain as a consequence of Lemma (4), after tensoring the free resolutions  $\mathbb{Z}[t_i] \rightarrow \mathbb{Z} \rightarrow 0$ , a free resolution of

$$\begin{aligned} \mathbb{Z}[G_1 \times \cdots \times G_k] &\cong \mathbb{Z}[T_1, \dots, T_k] / (T_1^{n_1} - 1, \dots, T_k^{n_k} - 1) \\ &= \mathbb{Z}[t_1, \dots, t_k] - \text{modules.} \end{aligned}$$

$$\begin{aligned} \longrightarrow \mathbb{Z}[t_1, \dots, t_k]^{a_k} &\xrightarrow{\Delta_2^k} \mathbb{Z}[t_1, \dots, t_k]^{b_k} \xrightarrow{\Delta_1^k} \mathbb{Z}[t_1, \dots, t_k]^{c_k} \xrightarrow{\Delta_0^k} \mathbb{Z}[t_1, \dots, t_k] \longrightarrow \mathbb{Z} \longrightarrow 0 \end{aligned} \tag{3.16}$$

Note that when  $k = 1$ , we have  $a_1 = 1$ ,  $b_1 = 1$  and  $c_1 = 1$ .

**Lemma 5.** *In the above resolution  $c_k = k = c_{k-1} + 1$ ,  $b_k = \binom{k+1}{2} = b_{k-1} + c_{k-1} + 1$ , and  $a_k = a_{k-1} + b_{k-1} + c_{k-1} + 1 = a_{k-1} + \binom{k}{2} + (k-1) + 1$ , for  $k \geq 2$ , where  $a_1 = b_1 = c_1 = 1$ .*

Furthermore, the morphisms  $\Delta_0^k$ ,  $\Delta_1^k$  and  $\Delta_2^k$  are given recursively by

$$\Delta_0^k((p_1, \dots, p_{k-1}), q) = \Delta_0^{k-1}(p_1, \dots, p_{k-1}) + \delta_0^k(q)$$

$$\Delta_1^k((p_1, \dots, p_{\binom{k}{2}}), (q_1, \dots, q_{k-1}), r) = (\Delta_1^{k-1}(p_1, \dots, p_{\binom{k}{2}}) - \delta_0^k(q_1, \dots, q_{k-1}), \Delta_0^{k-1}(q_1, \dots, q_{k-1}) + \delta_1^k(r))$$

$$\begin{aligned} \Delta_2^k((p_1, \dots, p_{a_{k-1}}), (q_1, \dots, q_{\binom{k}{2}}), (r_1, \dots, r_{k-1}), l) = \\ = (\Delta_2^{k-1}(p_1, \dots, p_{a_{k-1}}) + \delta_0^k(q_1, \dots, q_{\binom{k}{2}}), \Delta_1^{k-1}(q_1, \dots, q_{\binom{k}{2}}) - \delta_1^k(r_1, \dots, r_{k-1}), \Delta_0^{k-1}(r_1, \dots, r_{k-1}) + \delta_2^k(l)) \end{aligned}$$

where  $\delta_i^k(a_1, \dots, a_n) = (\delta_i^k(a_1), \dots, \delta_i^k(a_n))$ .

*Proof.* We argue by induction on  $k$ .

If  $k = 2$ , by (3.11), we have  $a_2 = 4$ ,  $b_2 = 3$  and  $c_2 = 2$ . Hence,  $a_2 = a_1 + \binom{2}{2} + 1 + 1$ ,  $b_2 = \binom{3}{2}$ , and  $c_2 = 2$ .

Suppose this is true for  $n < k$ . For a product of  $k$  finite cyclic groups  $G = G_1 \times \dots \times G_k$ , tensoring the free resolution of  $\mathbb{Z}[G_1 \times \dots \times G_{k-1}]$ -modules

$$\begin{array}{ccccccc} & F_3 & & F_2 & & F_1 & & F_0 \\ & \parallel & & \parallel & & \parallel & & \parallel \\ \longrightarrow & \mathbb{Z}[t_1, \dots, t_{k-1}]^{a_{k-1}} & \xrightarrow{\Delta_2^{k-1}} & \mathbb{Z}[t_1, \dots, t_{k-1}]^{b_{k-1}} & \xrightarrow{\Delta_1^{k-1}} & \mathbb{Z}[t_1, \dots, t_{k-1}]^{c_{k-1}} & \xrightarrow{\Delta_0^{k-1}} & \mathbb{Z}[t_1, \dots, t_{k-1}] \longrightarrow \mathbb{Z} \longrightarrow 0 \end{array} \quad (3.17)$$

with the free resolution of  $\mathbb{Z}[G_k]$ -modules

$$\begin{array}{ccccccc} & F'_3 & & F'_2 & & F'_1 & & F'_0 \\ & \parallel & & \parallel & & \parallel & & \parallel \\ \longrightarrow & \mathbb{Z}[t_k] & \xrightarrow{\delta_2^k} & \mathbb{Z}[t_k] & \xrightarrow{\delta_1^k} & \mathbb{Z}[t_k] & \xrightarrow{\delta_0^k} & \mathbb{Z}[t_k] \longrightarrow \mathbb{Z} \longrightarrow 0, \end{array} \quad (3.18)$$

where  $\delta_0^k = t_k - 1$ ,  $\delta_1^k = N_k = 1 + t_k + \dots + t_k^{k-1}$ , we get the respective free resolution of  $\mathbb{Z}[G_1 \times \dots \times G_k]$ -modules

$$\longrightarrow \mathbb{Z}[t_1, \dots, t_k]^{a_k} \xrightarrow{\Delta_2^k} \mathbb{Z}[t_1, \dots, t_k]^{b_k} \xrightarrow{\Delta_1^k} \mathbb{Z}[t_1, \dots, t_k]^{c_k} \xrightarrow{\Delta_0^k} \mathbb{Z}[t_1, \dots, t_k] \longrightarrow \mathbb{Z} \longrightarrow 0 \quad (3.19)$$

where

$$\mathbb{Z}[t_1, \dots, t_k]^{a_k} = \bigoplus_{i=0}^3 F_{3-i} \otimes F'_i = \mathbb{Z}[t_1, \dots, t_k]^{a_{k-1}} \bigoplus \mathbb{Z}[t_1, \dots, t_k]^{b_{k-1}} \bigoplus \mathbb{Z}[t_1, \dots, t_k]^{c_{k-1}} \bigoplus \mathbb{Z}[t_1, \dots, t_k]$$

hence  $a_k = a_{k-1} + b_{k-1} + c_{k-1} + 1 = a_{k-1} + \binom{k}{2} + (k-1) + 1$ .

$$\mathbb{Z}[t_1, \dots, t_k]^{b_k} = \bigoplus_{i=0}^2 F_{2-i} \otimes F'_i = \mathbb{Z}[t_1, \dots, t_k]^{b_{k-1}} \oplus \mathbb{Z}[t_1, \dots, t_k]^{c_{k-1}} \oplus \mathbb{Z}[t_1, \dots, t_k]$$

hence  $b_k = b_{k-1} + c_{k-1} + 1 = \binom{k}{2} + (k-1) + 1 = \binom{k+1}{2}$ .

$$\mathbb{Z}[t_1, \dots, t_k]^{c_k} = \bigoplus_{i=0}^1 F_{1-i} \otimes F'_i = \mathbb{Z}[t_1, \dots, t_k]^{c_{k-1}} \oplus \mathbb{Z}[t_1, \dots, t_k]$$

and therefore  $c_k = c_{k-1} + 1 = (k-1) + 1 = k$ .

Finally, as we saw in (3.13), the tensor of the resolutions (3.17) and (3.18) is the resolution (3.16) where the morphisms are given by

$$\Delta_0^k((p_1, \dots, p_{k-1}), q) = \Delta_0^{k-1}(p_1, \dots, p_{k-1}) + \delta_0^k(q)$$

$$\Delta_1^k((p_1, \dots, p_{\binom{k}{2}}), (q_1, \dots, q_{k-1}), r) = (\Delta_1^{k-1}(p_1, \dots, p_{\binom{k}{2}}) - \delta_0^k(q_1, \dots, q_{k-1}), \Delta_0^{k-1}(q_1, \dots, q_{k-1}) + \delta_1^k(r))$$

$$\begin{aligned} \Delta_2^k((p_1, \dots, p_{a_{k-1}}), (q_1, \dots, q_{\binom{k}{2}}), (r_1, \dots, r_{k-1}), l) = \\ = (\Delta_2^{k-1}(p_1, \dots, p_{a_{k-1}}) + \delta_0^k(q_1, \dots, q_{\binom{k}{2}}), \Delta_1^{k-1}(q_1, \dots, q_{\binom{k}{2}}) - \delta_1^k(r_1, \dots, r_{k-1}), \Delta_0^{k-1}(r_1, \dots, r_{k-1}) + \delta_2^k(l)) \end{aligned} \quad (3.20)$$

where  $\delta_i^k(a_1, \dots, a_n) = (\delta_i^k(a_1), \dots, \delta_i^k(a_n))$ .  $\square$

Now we are ready to prove that for  $G = G_1 \times \dots \times G_k$  where  $G_i$  is a cyclic group of order  $n_i$ ,

$$H^2(G, A) \cong \bigoplus_{i=1}^k \frac{A}{n_i A} \oplus \left( \bigoplus_{i \neq j} \text{Ann}_A(n_i) \cap \text{Ann}_A(n_j) \right),$$

where  $A$  is a  $G$ -module with the trivial action.

As we saw in (3.8), after omitting  $\mathbb{Z}$  in the resolution (3.16), and then applying the functor  $\text{Hom}_{\mathbb{Z}[G]}(-, A)$ , we get a complex which is isomorphic to the complex

$$0 \longrightarrow A \xrightarrow{D_k^0} A^{k-1} \oplus A \xrightarrow{D_k^1} A^{\binom{k}{2}} \oplus A^{k-1} \oplus A \xrightarrow{D_k^2} A^{a_{k-1}} \oplus A^{\binom{k}{2}} \oplus A^{k-1} \oplus A \longrightarrow \dots, \quad (3.21)$$

where the morphisms  $D_k^1$  and  $D_k^2$  are the morphisms induced by the morphisms (3.20), very much in the same way as in (3.14). That is,

$$\begin{aligned}
D_k^0(a) &= (\Delta_0^k(e_1) \cdot a, \Delta_0^k(e_2) \cdot a, \dots, \Delta_0^k(e_k) \cdot a), \quad a \in A \\
D_k^1(a, b) &= (\Delta_1^k(e_1) \cdot (a, b), \Delta_1^k(e_2) \cdot (a, b), \dots, \Delta_1^k(e_{b_k}) \cdot (a, b)), \quad (a, b) \in A^{k-1} \oplus A \\
D_k^2(a, b, c) &= (\Delta_2^k(e_1) \cdot (a, b, c), \Delta_2^k(e_2) \cdot (a, b, c), \dots, \Delta_2^k(e_{a_k}) \cdot (a, b, c)), \quad (a, b, c) \in A^{\binom{k}{2}} \oplus A^{k-1} \oplus A
\end{aligned} \tag{3.22}$$

where  $e_j$  denotes the canonical vector  $(0, \dots, 0, 1, 0, \dots, 0)$ .

In order to compute the morphisms  $D_k^1$  and  $D_k^2$  we need to know the values of  $\Delta_1^k(e_j)$ , with  $j = 1, \dots, b_k$ , and  $\Delta_2^k(e_j)$ , with  $j = 1, \dots, a_k$ . Using the equations (3.20) we have:

$$\begin{aligned}
\Delta_0^k(e_1) &= \Delta_0^{k-1}(e_1) \\
\Delta_0^k(e_2) &= \Delta_0^{k-1}(e_2) \\
&\vdots \\
\Delta_0^k(e_{k-1}) &= \Delta_0^{k-1}(e_{k-1}) \\
\Delta_0^k(e_k) &= \delta_0^k(1)
\end{aligned}$$

$$\begin{aligned}
\Delta_1^k(e_1) &= (\Delta_1^{k-1}(e_1), 0) \\
\Delta_1^k(e_2) &= (\Delta_1^{k-1}(e_2), 0) \\
&\vdots \\
\Delta_1^k(e_{b_{k-1}}) &= (\Delta_1^{k-1}(e_{b_{k-1}}), 0)
\end{aligned} \tag{3.23}$$

$$\begin{aligned}
\Delta_1^k(e_{(b_{k-1})+1}) &= (-\delta_0^k(e_1), \Delta_0^{k-1}(e_1)) \\
\Delta_1^k(e_{(b_{k-1})+2}) &= (-\delta_0^k(e_2), \Delta_0^{k-1}(e_2)) \\
&\vdots \\
\Delta_1^k(e_{(b_{k-1})+(k-1)}) &= (-\delta_0^k(e_{k-1}), \Delta_0^{k-1}(e_{k-1})) \\
\Delta_1^k(e_{(b_{k-1})+(k-1)+1}) &= \delta_1^k(e_{b_k}) = (0, \delta_1^k(1)).
\end{aligned} \tag{3.24}$$

We note that (3.23) applied to a vector

$$(a, b) = (a_1, a_2, b) \in A^{k-2} \oplus A \oplus A = A^{k-1} \oplus A$$



produces the vector

$$\begin{aligned} & (\Delta_1^{k-1}(e_1) \cdot (a_1, a_2), \Delta_1^{k-1}(e_2) \cdot (a_1, a_2), \dots, \Delta_1^{k-1}(e_{b_{k-1}}) \cdot (a_1, a_2)) \\ &= D_{k-1}^1(a_1, a_2) = D_{k-1}^1(a). \end{aligned}$$

On the other hand, using equation (3.20), it is easy to check by induction that  $\Delta_0^k(e_i) \cdot (a_1, \dots, a_k) = 0$ , for all  $k \geq 2$ . Therefore, as  $\delta_0^k(e_i) = (0, \dots, 0, t_k - 1, 0, \dots, 0)$ , we see that (3.24) applied to a vector  $(a_1, \dots, a_k)$  produce the vector  $(0, 0, \dots, 0)$ .

Finally, as

$$(0, \delta_1^k(1)) \cdot (a, b) = \delta_1^k(1) \cdot b = N_k \cdot b = n_k b,$$

we conclude that

$$\text{im}(D_k^1) = \text{im}(D_{k-1}^1) \oplus 0 \oplus 0 \oplus \dots \oplus 0 \oplus n_k A \subset A^{\binom{k}{2}} \oplus A^{k-1} \oplus A = A^{\binom{k+1}{2}}.$$

Therefore,

$$\begin{aligned} D_k^1((x_1, \dots, x_{k-1}), y) &= (D_{k-1}^1(x_1, \dots, x_{k-1}), 0, 0, \dots, 0, \delta_1^k(1) \cdot y) \\ &= (D_{k-1}^1(x_1, \dots, x_{k-1}), 0, 0, \dots, 0, n_k \cdot y) \end{aligned} \quad (3.25)$$

From (3.14), we obtain  $D_2^1(x, y) = (n_1 x, 0, n_2 y)$ .

Hence by equation (3.25)

$$\begin{aligned} D_3^1((x_1, x_2), y) &= (n_1 x_1, 0, n_2 x_2, 0, 0, n_3 y) \\ D_4^1((x_1, x_2, x_3), y) &= (n_1 x_1, 0, n_2 x_2, 0, 0, n_3 x_3, 0, 0, 0, n_4 y) \\ &\vdots \end{aligned}$$

$$D_k^1((x_1, \dots, x_{k-1}), y) =$$

$$(n_1 x_1, 0, n_2 x_2, 0, 0, n_3 x_3, 0, 0, 0, n_4 x_4, 0, 0, 0, 0, n_5 x_5, 0, 0, 0, 0, 0, n_6 x_6, \dots, n_{k-1} x_{k-1}, 0, 0, \dots, 0, n_k z). \quad (3.26)$$

Now, using again equations (3.20) we obtain:

$$\begin{aligned} \Delta_2^k(e_1) &= (\Delta_2^{k-1}(e_1), 0, 0) \\ \Delta_2^k(e_2) &= (\Delta_2^{k-1}(e_2), 0, 0) \\ &\vdots \\ \Delta_2^k(e_{a_{k-1}}) &= (\Delta_2^{k-1}(e_{a_{k-1}}), 0, 0) \end{aligned} \quad (3.27)$$

$$\begin{aligned}
\Delta_2^k(e_{(a_{k-1})+1}) &= (\delta_0^k(e_1), \Delta_1^{k-1}(e_1), 0) \\
\Delta_2^k(e_{(a_{k-1})+2}) &= (\delta_0^k(e_2), \Delta_1^{k-1}(e_2), 0) \\
&\vdots \\
\Delta_2^k(e_{(a_{k-1})+b_{k-1}}) &= (\delta_0^k(e_{b_{k-1}}), \Delta_1^{k-1}(e_{b_{k-1}}), 0)
\end{aligned} \tag{3.28}$$

$$\begin{aligned}
\Delta_2^k(e_{(a_{k-1})+(b_{k-1})+1}) &= (0, -\delta_1^k(e_1), \Delta_0^{k-1}(e_1)) \\
\Delta_2^k(e_{(a_{k-1})+(b_{k-1})+2}) &= (0, -\delta_1^k(e_2), \Delta_0^{k-1}(e_2)) \\
&\vdots \\
\Delta_2^k(e_{(a_{k-1})+(b_{k-1})+(k-1)}) &= (0, -\delta_1^k(e_{k-1}), \Delta_0^{k-1}(e_{k-1})) \\
\Delta_2^k(e_{(a_{k-1})+(b_{k-1})+(k-1)+1}) &= \Delta_2^k(e_{a_k}) = (0, 0, \delta_2^k(1)).
\end{aligned} \tag{3.29}$$

We notice that

$$\begin{aligned}
\delta_0^k(e_j) \cdot (x_1, \dots, x_{b_{k-1}}) &= 0, \quad \delta_2^k(1) \cdot z = 0, \\
\delta_1^k(e_j) \cdot (y_1, \dots, y_{k-1}) &= N_k e_j \cdot (y_1, \dots, y_{k-1}) = n_k y_j.
\end{aligned}$$

As we saw before,  $\Delta_0^{k-1}(e_j) \cdot (y_1, \dots, y_{k-1}) = 0$ .

Thus from equations (3.27), (3.28) and (3.29) we deduce:

$$\begin{aligned}
D_k^2((x_1, \dots, x_{b_{k-1}}), (y_1, \dots, y_{k-1}), z) &= \\
&= (\Delta_2^k(e_1) \cdot ((x_1, \dots, x_{b_{k-1}}), (y_1, \dots, y_{k-1}), z), \dots, \Delta_2^k(e_{a_k}) \cdot ((x_1, \dots, x_{b_{k-1}}), (y_1, \dots, y_{k-1}), z)) \\
&= (D_{k-1}^2(x_1, \dots, x_{b_{k-1}}), D_{k-1}^1(y_1, \dots, y_{k-1}), -n_k y_1, \dots, -n_k y_{k-1}, 0).
\end{aligned}$$

Now, from (3.26) we know that

$$\begin{aligned}
D_{k-1}^1(y_1, \dots, y_{k-2}, y_{k-1}) &= \\
&= (n_1 y_1, 0, n_2 y_2, 0, 0, n_3 y_3, 0, 0, 0, n_4 y_4, 0, 0, 0, 0, n_5 y_5, 0, 0, 0, 0, n_6 y_6, \dots, n_{k-2} y_{k-2}, 0, 0, \dots, 0, n_{k-1} y_{k-1})
\end{aligned}$$

Hence,

$$\begin{aligned}
D_k^2((x_1, \dots, x_{b_{k-1}}), (y_1, \dots, y_{k-1}), z) &= \\
&= (D_{k-1}^2(x_1, \dots, x_{b_{k-1}}), n_1 y_1, 0, n_2 y_2, 0, 0, n_3 y_3, 0, 0, 0, n_4 y_4, 0, 0, 0, 0, n_5 y_5, 0, 0, 0, 0, n_6 y_6, \dots, \\
&\dots, n_{k-2} y_{k-2}, 0, 0, \dots, 0, n_{k-1} y_{k-1}, \dots, y_{k-1}), -n_k y_1, \dots, -n_k y_{k-1}, 0).
\end{aligned}$$

Thus, we conclude that

$$\ker(D_k^2) = \ker(D_{k-1}^2) \oplus \text{Ann}_A(n_1) \cap \text{Ann}_A(n_k) \oplus \cdots \oplus \text{Ann}_A(n_{k-1}) \cap \text{Ann}_A(n_k) \oplus A.$$

**Theorem 22.** *Suppose that  $G$  is a finite abelian group, written as  $G = G_1 \times \cdots \times G_k$ , where  $G_i$  is a finite cyclic group of order  $n_i$ . Suppose that  $A$  is a  $G$ -module with the trivial action. Then*

$$H^2(G, A) \cong \bigoplus_{i=1}^k \frac{A}{n_i A} \oplus \bigoplus_{i \neq j} \text{Ann}_A(n_i) \cap \text{Ann}_A(n_j).$$

Eventhough this theorem is true for any  $G$ -module  $A$  with the trivial action, we will only use it in the case when  $A \subset k^*$  is a subgroup of the units of a field  $k$  (see theorem 25).

*Proof.* As we saw above

$$\ker(D_k^2) = \ker(D_{k-1}^2) \oplus \text{Ann}_A(n_1) \cap \text{Ann}_A(n_k) \oplus \cdots \oplus \text{Ann}_A(n_{k-1}) \cap \text{Ann}_A(n_k) \oplus A$$

and

$$\text{im}(D_k^1) = \text{im}(D_{k-1}^1) \oplus 0 \oplus 0 \oplus \cdots \oplus 0 \oplus n_k A.$$

Therefore,

$$H^2(G, A) \cong \frac{\ker(D_{k-1}^2)}{\text{im}(D_{k-1}^1)} \oplus \text{Ann}_A(n_1) \cap \text{Ann}_A(n_k) \oplus \cdots \oplus \text{Ann}_A(n_{k-1}) \cap \text{Ann}_A(n_k) \oplus \frac{A}{n_k A}.$$

But if  $H = G_1 \times \cdots \times G_{k-1}$ . Then,

$$\frac{\ker(D_{k-1}^2)}{\text{im}(D_{k-1}^1)} \cong H^2(H, A).$$

Hence,

$$H^2(G_1 \times \cdots \times G_k, A) \cong H^2(G_1 \times \cdots \times G_{k-1}, A) \oplus \text{Ann}_A(n_1) \cap \text{Ann}_A(n_k) \oplus \cdots \oplus \text{Ann}_A(n_{k-1}) \cap \text{Ann}_A(n_k) \oplus \frac{A}{n_k A}.$$

When  $k = 2$  we saw that the result is true:

$$H^2(G_1 \times G_2, A) \cong \frac{A}{n_1 A} \oplus \frac{A}{n_2 A} \oplus \text{Ann}_A(n_1) \cap \text{Ann}_A(n_2).$$

Therefore, by the inductive hypothesis, if

$$H^2(G_1 \times \cdots \times G_{k-1}, A) \cong \bigoplus_{i=1}^{k-1} \frac{A}{n_i A} \oplus \bigoplus_{i \neq j} \text{Ann}_A(n_i) \cap \text{Ann}_A(n_j).$$

Then

$$H^2(G_1 \times \cdots \times G_k, A) \cong \bigoplus_{i=1}^k \frac{A}{n_i A} \oplus \bigoplus_{i \neq j} \text{Ann}_A(n_i) \cap \text{Ann}_A(n_j).$$

□

### 3.4 Graded Morphisms and the classification problem

In this section we collect some results from [35] that provide necessary and sufficient conditions for two algebras to be graded-isomorphic (under a graded isomorphism) in terms of the second group of cohomology  $H^2(G, k^*)$ . After that we show as an application of theorem 22 a formula to compute how many  $G$ - graded, twisted associative  $k$ -algebras exist up to graded isomorphisms, in case the group of graduation  $G \simeq G_1 \times \cdots \times G_k$ , is a finitely generated abelian group.

The reader may consult the proof of the following two theorems in [35], Theorem 4 and Theorem 5.

**Theorem 23.** *Let  $V = \bigoplus_{g \in G} V_g$  and  $W = \bigoplus_{g \in G} W_g$  two  $G$ -graded  $k$ -algebras. Let us fix bases  $B_1$  and  $B_2$  for  $V$  and  $W$ , respectively, and let  $C_1$  and  $C_2$  be the associated structure constants. Then  $V$  is isomorphic to  $W$  if and only if the function  $C_1 C_2^{-1}$  is in the kernel of  $d^2 : C^2(G, k^*) \rightarrow C^3(G, k^*)$  and the class  $[C_1 C_2^{-1}]$  is trivial in  $H^2(G, k^*)$ .*

When  $C_1$  and  $C_2$  take values in a subgroup  $A \subset k^*$ , then  $C_1 C_2^{-1} \in C^2(G, A)$ . Authors in [35] present the following theorem that gives a criterion in terms of  $H^2(G, A)$  to determine when  $V$  and  $W$  are isomorphic.

**Theorem 24.**  *$\phi : V \rightarrow W$  is a (graded) isomorphism if and only if  $d^2(C_1 C_2^{-1}) = 1$ , and  $[C_1 C_2^{-1}] \in \ker(i_2)$ , where  $i_2 : H^2(G, A) \rightarrow H^2(G, k^*)$  denotes the homomorphism in cohomology induced by the inclusion  $i : A \rightarrow k^*$ .*

The following remark allows to identify the elements of  $H^2(G, A)$  with associative  $G$ -graded twisted  $K$ -algebras with structure constants taking values in  $A$ , where  $A \subset K^*$  is a multiplicative subgroup.

**Remark 5.** If  $V$  and  $W$  are associative, then  $d^2 C_1 = d^2 C_2 = 1$ , since each of these terms are equal to the associativity function in (3.1). In this case, the class of each  $C_i$  is an element of  $H^2(G, A)$  and the condition  $[C_1 C_2^{-1}] = 1$  is equivalent to  $[C_1] = [C_2]$  in  $H^2(G, A)$ .

See [35], Remark 2.

Let us notice that two associative  $G$ -graded  $k$ -algebras are isomorphic  $V \cong W$  if and only if  $\overline{[C_1]} = \overline{[C_2]}$  in  $H^2(G, A)/\ker(i_2)$  (by remark 5 and theorem 24.) if and only if  $[C_1 C_2^{-1}] \in \ker(i_2)$ .

Then, the number of associative  $G$ -graded  $k$ -algebras with associated structure constants taking values on  $A$  is  $|H^2(G, A)/\ker(i_2)|$

As an application of Theorem 22, using the same notation, we are able to prove our main result.

**Theorem 25.** *Let  $G$  be a finite abelian group,  $A$  a  $G$ -module with the trivial action. Then the number of  $G$ -graded twisted associative algebras on  $A$ , up to graded isomorphisms, is at most*

$$\prod_{i=1}^k \left| \frac{A}{n_i A} \right| \cdot \prod_{i \neq j} |Ann_A(n_i) \cap Ann_A(n_j)|.$$

*Proof.* The number of  $G$ -graded twisted associative  $k$ -algebras on  $A$  is a quotient of  $|H^2(G_1 \times \cdots \times G_k, A)|$ . Hence, the result follows from the formula obtained in Theorem 22.  $\square$

# Bibliography

- [1] Álvarez, M., J., Boix, A. F., and Zarzuela, S. Frobenius and Cartier algebras of Stanley–Reisner rings. *Journal of Algebra*, 358 (2012), 162-177.
- [2] Atiyah, M. F. and Macdonald, I.G., *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Mass, 1969.
- [3] Atiyah, M. and Wall C., *Cohomology of Groups*, from J. W. S. Cassel and A. Fröhlich, *Algebraic Number Theory*, Thompson Book Company, Washington D. C, (1967).
- [4] Babakhanian A., *Cohomological methods in group theory*, Marcel Dekker Inc., (1972).
- [5] Bourbaki, N., *Commutative Algebra Chapters 1-7*, Springer-Verlag, New York, 1989.
- [6] Brown, K. S. (1982). *Cohomology of groups* (No. 87). Springer Science and Business Media.
- [7] Craven T., Velez J., and Wills–Toro L., *Cohomology of deformation parameters of diagonal noncommutative nonassociative graded algebras*. *Acta Mathematica Academiae Paedagogicae Nyíregyháziensis* **24** , 271–277 (2008), and ICM 2008.
- [8] Craven T., Velez J., and Wills–Toro L., *Graded Lie algebras and  $q$ -commutative and  $r$ -associative parameters*, *São Paulo Journal of Mathematical Sciences* **3**, 1 , 263—280 (2009).
- [9] Edwards C. and Lewis J., *Twisted Group Algebras I*, *Commun. math. Phys.* **13**, 119–130 (1969).
- [10] Edwards C. and Lewis J., *Twisted Group Algebras II*, *Commun. math. Phys.* **13**, 131–141 (1969).

- [11] Eisenbud, D., *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, Vol. 150, Springer-Verlag, New York, 1995.
- [12] Grothendieck, A., *Local Cohomology: A Seminar Given by A. Grothendieck*, Harvard University, Fall, 1961 (Vol. 41). Springer.
- [13] Gomez-Ramirez, D. 2013. *Homological Conjectures, Clousure Operations, Vector Bundles and Forcing Algebras*, Ph.D. thesis, Universidad Nacional de Colombia.
- [14] Hochster, M., *Expository Lectures from the CBMS Regional Conference (U. of Nebraska) June 24-28, 1974* (p. 32, Lemma 5.7).
- [15] Hochster, M. (2011). *Local cohomology*. unpublished notes.
- [16] Karpilovsky, Gregory, *Projective representations of finite groups*. Monographs and Textbooks in Pure and Applied Mathematics, 94. Marcel Dekker, Inc., New York, 1985.
- [17] Karpilovsky, Gregory, *Group representations*. Vol. 2, 3. North-Holland Mathematics Studies, 177, 180. North-Holland Publishing Co., Amsterdam, 1993.
- [18] Katzman, M., *A non-finitely generated algebra of Frobenius maps*. Proceedings of the American Mathematical Society, 138(7), 2381-2383, (2010).
- [19] Katzman, M., *Parameter-test-ideals of Cohen–Macaulay rings*. Compositio Mathematica, 144(04), 933-948, (2008).
- [20] Koh, J. H. (1983). *The direct summand conjecture and behavior of codimension in graded extensions* (Doctoral dissertation, Ph. D. Thesis, University of Michigan).
- [21] Kunz, E., *Introduction to Commutative Algebra and Algebraic Geometry*, Birkh user, Boston, 1985.
- [22] Kunz, E., *Characterizations of regular local rings of characteristic p*, Amer. J. Math., 91 (1969), 772-784.
- [23] Lyubeznik, G., *F-modules: applications to local cohomology and D-modules in characteristic  $p > 0$* . J. reine angew. Math. 491 (1997),65-130

- [24] Marker, D., *Model Theory: An Introduction*, Graduate texts in Mathematics, Vol 217, Springer-Verlag, New York, 2002.
- [25] Matsumura, H. (1980) *Commutative Algebra*, (Mathematics Lecture Note Series, 56).
- [26] Sharp, R. Y. (2012). Big tight closure test elements for some non-reduced excellent rings. *Journal of Algebra*, 349(1), 284-316.
- [27] Schmidt, K. and Vanden Dries, L., *Bounds in the Theory of Polynomial Rings Over Fields. A Non-standard Approach*, *Invent. Math.*, 116 (2000), 125-169.
- [28] Schafer R., *An Introduction to Nonassociative Algebras*. New York: Dover, p. 13, (1996).
- [29] Scheunert M., *Generalized Lie Algebras*, *J. Math. Phys.* **20**(4), 712-720, April (1979).
- [30] Schoutens, H., *The Use of Ultraproducts in Commutative Algebra*, *Lecture Notes in Mathematics*, 1999, 204p, Springer (2010).
- [31] Schoutens, H., *Bounds in Cohomology*, *Israel J. Math.* 116 (2000), 125-169.
- [32] Schoutens, H., *Lefschetz principle applied to symbolic powers*, <http://www.math.ohio-state.edu/~schoutens>, 2001.
- [33] Smith, K., *Tight Closure of Parameter Ideals*, *Inv. Math.* 115 (1994), 41-60.
- [34] Velez, J., *Openness of the F-rational locus, smooth base change and Koh's conjecture*, University of Michigan.,(Doctoral dissertation) 1993.
- [35] Velez, J. D., Wills, L. A., and Agudelo, N., *On the classification of G-graded twisted algebras*, *Journal for Algebra and Number Theory Academia* Volume 4, Issue 1, February 2014, Pages 1-20.
- [36] Wills-Toro L. A., *Classification of some graded division algebras I*, submitted for publication (arXiv:1007.3730v3[math.RA]).
- [37] Wills-Toro L. A., *Classification of some graded division algebras II*, submitted to publication.
- [38] Wills-Toro L. A., *Classification of some graded division algebras III*, in preparation.



- [39] Wills-Toro L. A., *Finite group graded Lie algebraic extensions and Trefoil symmetric relativity, Standard Model, Yang-Mills and gravity theories*, University of Hawaii Manoa, Ph.D. Thesis (2004).
- [40] Wills-Toro L. A., *Trefoil Symmetry I: Clover Extensions Beyond Coleman-Mandula Theorem*, Journal of Mathematical Physics, **42**, 3915 (2001).
- [41] Wills-Toro L. A., Sánchez L., Osorio J., and Jaramillo D., *Trefoil Symmetry II: Another Clover Extension*, Journal of Mathematical Physics, **42**, 3935 (2001).
- [42] Wills-Toro L. A., *Trefoil Symmetry III: The full Clover Extension*, Journal of Mathematical Physics, **42**, 3947 (2001).
- [43] Wills-Toro L. A., Sánchez L., and Leleu X., *Trefoil Symmetry IV: Basic Enhanced Superspace for the Minimal Vector Clover Extension*, International Journal of Theoretical Physics, Volume **42**, No. 1, 57–72 (2003).
- [44] Wills-Toro L. A., Sánchez L., Leleu X., and Bleeker D., *Trefoil Symmetry V: Class Representations for the Minimal Clover Extension*, International Journal of Theoretical Physics, Volume **42**, No. 1, 73–83 (2003).
- [45] Winfried Bruns, Jürgen Herzog, H., (1998). Cohen-macaulay rings. Cambridge University Press.