LIMITS OF QUOTIENTS OF RATIONAL POLYNOMIAL FUNCTIONS OF THREE VARIABLES, CLASSIFICATION OF G-GRADED TWISTED ALGEBRAS AND THE COMPUTATION OF THE F-RATIONAL LOCUS

Juan Pablo Hernández Rodas

A thesis submitted in partial fulfillment for the
degree of Doctor of Philosophy

in the

Faculty of Science
Universidad Nacional de Colombia
Medellín

Supervisor: Prof. Juan Diego Vélez Caicedo

June 2015

CONTENTS

ACKNOWLEDGEMENTS

I would like to thank my parents for all their help during the development of this thesis. I want to express my deepest gratitude to my advisor, Dr. Juan Diego Vélez, for accepting to develop this work together with me, for his excellent guidance and for his love to Mathematics. I would also thank my friend and colleague, Edisson Gallego, who spent so many hours discussing with me about topics related with this thesis. I thank all those people who made this thesis possible. I am very grateful with the fellowship for outstanding students granted by the Universidad Nacional de Colombia, since it was my financial support. Unfortunately, this scholarship is not awarded anymore.

ABSTRACT

This thesis is divided in three main parts. In the first part we provide a theoretical method to determine the existence of the limit of a quotient of polynomial functions of three variables. An algorithm to compute such limits in the case where the polynomials have rational coefficients, or more generally, coefficients in a real finite extension of the rational numbers is also described.
In the second part, for any finite abelian group G, we present an exact formula to count the G-graded twisted algebras satisfying certain symmetry condition.
Finally, in the third part we describe an algorithm to compute the F-rational locus of an affine algebra over a field of prime characteristic $p > 0$ by computing first its global test ideal. As a consequence we deduce the Openness of the F-rational locus, a result originally proved in [27].

Part I

LIMITS OF QUOTIENTS OF RATIONAL POLYNOMIAL FUNCTIONS OF THREE VARIABLES

1. INTRODUCTION

Algorithms for computing limits of functions in one variable are studied in [15]. Similar algorithms have been developed in [13], [14]. On the other hand, computational methods dealing with classical objects like power series and algebraic curves have been developed by several authors during the last two decades [6], [11]. In [5] a symbolic computation algorithm for computing local parametrization of analytic branches and real analytic branches of a curve in n-dimensional space is proposed. Necessary and sufficient conditions for the existence of limits of the form $\lim_{(x,y)\to(a,b)} f(x,y)/g(x,y)$ are given in [1], under the hypothesis that f and g are real analytic functions near the point (a,b), and g has an isolated zero at (a,b). The authors give a criterion which could be implemented in a computer algebra system in the case where f and g are polynomials with rational coefficients, or more generally, with coefficients in a real finite extension of the rationals.

We generalize the methods developed in [1]. A theoretical method for determining the existence of limits of the form $\lim_{(x,y,z)\to(a,b,c)} f(x,y,z)/g(x,y,z)$, where f and g are polynomials with rational coefficients, or more generally, with coefficients in a real extension field of $\mathbb{Q}$, defined as in [1], page 203 is developed. The problem is solved by reducing to the case of functions of two variables. We use Lagrange multipliers, as it appears in Proposition 1, pag 199 of [1], but for the case of functions defined on a hypersurface. The final reduction to the two dimensional case is achieved by using the fact that any algebraic curve is birational to a plane curve, and therefore locally isomorphic. For this, we need a constructive version of this theorem.

A high level description of an algorithm for determining the existence of the limit as well as its computation is provided. The main result is summarized in Theorem 2. Proofs are provided in a constructive manner making it possible to implement the method in an algorithmic way.

2. PRELIMINARIES

2.1 Dimension of algebraic sets and the singular locus

Given an ideal $I \subset \mathbb{R}[x_1, \ldots, x_n]$, $V(I)$ will be denote the complex affine variety cut by I, in other words, it is the set of complex zeros of polynomials of I.

However, in this thesis when we talk about the dimension of $V(I)$, we are actually taking about the dimension of $V(I)$ as an algebraic set, that is to say,

$$\dim(V(I)) = \dim(\mathbb{R}[x_1, \ldots, x_n]/I).$$

When $P \subset \mathbb{R}[x_1, \ldots, x_n]$ is a prime ideal, it is well known that the dimension of the integer domain $\mathbb{R}[x_1, \ldots, x_n]/P$ coincides with the transcendence degree of the field extension $\mathbb{R} \subset \mathbb{R}(x, y, z)$, where $\mathbb{R}(x, y, z)$ denotes the fraction field of $\mathbb{R}[x, y, z]/P$. The transcendence degree of a field extension $K \subset L$ is denoted by $\text{trdeg}_K L$, and it is defined as the cardinal of the maximal algebraically independent subset $S \subset L$ such that $K(S) \subset L$ is an algebraic field extension.
Therefore, the dimension of $V(P)$ defined as above is such that

$$\dim(V(P)) = \text{trdeg}_{\mathbb{R}}\mathbb{R}(x, y, z).$$

Now we focus in a particular case that will be very important in the development of the first part of this thesis.
Suppose that $X \subset \mathbb{C}^3$ is an affine variety cut by a prime ideal $P \subset \mathbb{R}[x, y, z]$ and such that $\dim(V(P)) = 2$, that is to say, $\dim(\mathbb{R}[x, y, z]/P) = 2$.
This implies that $P \subset \mathbb{R}[x, y, z]$ is a prime ideal of height 1 and hence, $P = (h)$ where $h(x, y, z) \in \mathbb{R}[x, y, z]$ is a real irreducible polynomial. Therefore $X = V(h)$.

Definition 1. With the about notation, we define the *singular locus* of $X = V(h)$ as the complex

affine variety cut by the ideal $I_S = (h, \partial h/\partial x, \partial h/\partial y, \partial h/\partial z) \subset \mathbb{R}[x, y, z]$. The singular locus of X is denoted by Sing$X$.

Remark 1. The dimension of Sing$X$ is smaller than the dimension of X.

Proof. Notice that $\partial h/\partial x \notin (h)$, since the degree in the variable x of $\partial h/\partial x$ is less than the degree in the variable x of h. Therefore, $(h) \subsetneq I_S$ what implies that $\dim(\mathbb{R}[x, y, z]/I_S) < \dim(\mathbb{R}[x, y, z]/(h))$. Hence, $\dim(\text{Sing}X) < \dim(X)$. □

2.2 Discriminant variety

The existence of $\lim_{(x,y,z)\to(a,b,c)} f(x, y, z)/g(x, y, z)$ is obviously independent of the particular choice of local coordinates. Hence, by a translation, there is no loss of generality in assuming that (a, b, c) is the origin. Our objective is to compute

$$\lim_{(x,y,z)\to(0,0,0)} \frac{f(x, y, z)}{g(x, y, z)} \tag{2.1}$$

where $f(x, y, z)$ and $g(x, y, z)$ are rational polynomial functions, and g has an isolated zero at $(0, 0, 0)$. If $q(x, y, z) = f(x, y, z)/g(x, y, z)$, we define the *discriminant variety* $X(q)$ associated to q as the variety cut by the 2×2 minors of the matrix

$$A = \begin{bmatrix} x & y & z \\ \partial q/\partial x & \partial q/\partial y & \partial q/\partial z \end{bmatrix}. \tag{2.2}$$

Notice that the 2×2 minors of A has the form $x_i\partial q/\partial x_j - x_j\partial q/\partial x_i$ which are not polynomial functions, however, as $q = f/g$ then

$$x_i\partial q/\partial x_j - x_j\partial q/\partial x_i = \frac{x_i(g\partial f/\partial x_j - f\partial g/\partial x_j)}{g^2} - \frac{x_j(g\partial f/\partial x_i - f\partial g/\partial x_i)}{g^2}$$

and therefore if we define $f_{x_i,x_j} = x_i(g\partial f/\partial x_j - f\partial g/\partial x_j) - x_j(g\partial f/\partial x_i - f\partial g/\partial x_i)$ then $X(q)$ means the affine variety cut by the polynomial ideal

$$J = (f_{x,y}, f_{x,z}, f_{y,z}).$$

The following proposition states that in order to determine the existence of the limit (2.1), it suffices to analyze the behaviour of the function $q(x, y, z)$ along the discriminant variety $X(q)$.

Proposition 1. *The limit* $\lim_{(x,y,z)\to 0} q(x, y, z)$ *exists and equals* $L \in \mathbb{R}$*, if and only if for every* $\epsilon > 0$ *there is* $\delta > 0$ *such that for every* $(x, y, z) \in X(q)$ *with* $0 < |(x, y, z)| < \delta$ *the inequality* $|q(x, y, z) - L| < \epsilon$ *holds.*

Proof. The method of Lagrange multipliers applied to the function $q(x,y,z)$ with the constraint $x^2+y^2+z^2=r^2$ where $r>0$, guarantees that if $C_r(0)=\{(x,y,z)\in\mathbb{R}^3 \ : \ x^2+y^2+z^2=r^2\}$ then the extreme values of $q(x,y,z)$ on $C_r(0)$ are achieved among those points $p=(a,b,c)\in C_r(0)$ for which $(\partial q/\partial x(p),\partial q/\partial y(p),\partial q/\partial z(p))=\lambda(a,b,c)$, and therefore among points of $X(q)$.
Suppose that given $\epsilon>0$ there is $\delta>0$ such that for every $(x,y,z)\in X(q)\cap D^*_\delta$ the inequality $|q(x,y,z)-L|<\epsilon$ holds, where $D^*_\delta=\{(x,y,z)\in\mathbb{R}^3 \ : \ 0<\sqrt{x^2+y^2+z^2}<\delta\}$. Let $(x,y,z)\in D^*_\delta$ and $r=\sqrt{x^2+y^2+z^2}$. If $t(r),s(r)\in C_r(0)$ are the maximum and minimum values of $q(x,y,z)$ subject to $C_r(0)$ respectively, then

$$q(s(r))-L\leq q(x,y,z)-L\leq q(t(r))-L.$$

As $t(r),s(r)\in X(q)\cap C_r(0)\subset X(q)\cap D^*_\delta$, then $-\epsilon<q(s(r))-L$ and $q(t(r))-L<\epsilon$ and therefore $|q(x,y,z)-L|<\epsilon$.
The reciprocal is clear. □

2.3 Algebraic plane curves

In this section we present some results that allow us to prove that every irreducible algebraic curve is birationally equivalent to an irreducible plane curve, a result that plays a very important role in this chapter since it is the main argument in the reduction to the case of bivariate functions.
In this section by an irreducible algebraic curve we mean a complex affine variety $X\subset\mathbb{C}^n$ cut by a prime ideal $P\subset\mathbb{R}[x_1,\ldots,x_n]$ and such that $\dim(X)=1$, where remain that $\dim(X)=\dim(\mathbb{R}[x_1,\ldots,x_n]/P)$.

Proposition 2 (Existence of primitive elements)**.** *Let K be a field of characteristic zero, L a finite algebraic extension of K. Then there is $z\in L$ such that $L=K(z)$.*

Proof. As L is a finite extension of K then $L=K(x_1,\ldots,x_n)$ for some $x_1,\ldots,x_n\in L$.
We argue by induction on n.
The case $n=1$ is trivial. Now we discuss the case $n=2$.
Suppose that $L=K(x,y)$ where $x,y\in L\backslash K$. As x and y are algebraic over K, there are monic polynomials $F(t),G(t)\in K[t]$ such that $F(x)=0$ and $G(y)=0$. We factor $F(t)$ and $G(t)$ in some extension $L'\supset K$, say $F(t)=\prod_{i=1}^k(t-x_i)$ and $G(t)=\prod_{j=1}^s(t-y_j)$ with $x_i,y_j\in L'$. Suppose that $x=x_1\in L'$ and $y=y_1\in L'$. As $x,y\in L'$ then $L\subset L'$.
As K is an infinite field there is some $\lambda\in K$ such that $x_i+\lambda y_j\neq x_t+\lambda y_l$ for all $i\neq t$ and $j\neq l$. Note that it is possible to choose such λ since it is enough to take $\lambda\neq\frac{x_t-x_i}{y_j-y_l}$ for

all $t \neq i$ and $j \neq l$.
We claim that $L = K(z)$, where $z = x + \lambda y$.
In fact, consider $H(t) = F(z - \lambda t) \in K(z)[t]$. Note that $H(y) = 0$ since $H(y) = F(x) = 0$ and $H(y_j) \neq 0$ for $j \neq 1$ since $H(y_j) = F(z - \lambda y_j)$ and $z - \lambda y_j = x + \lambda y - \lambda y_j \neq x_i$ for all $i \neq 1$ since $x + \lambda y \neq x_i + \lambda y_j$ for all $i, j \neq 1$. Therefore the maximum common divisor $(H(t), G(t)) = t - y \in K(z)[t]$, thus $y \in K(z)$ and hence $L = K(z)$. Now suppose that $L = K(x_1, \ldots, x_n) = K(x_1, \ldots, x_{n-1})(x_n)$. By the induction hypothesis $K(x_1, \ldots, x_{n-1}) = K(\lambda_1 x_1 + \cdots + \lambda_{n-1} x_{n-1})$ for some $\lambda_i \in K$ and by the argument used for the case of two variables we have that $L = K(\lambda_1 x_1 + \cdots + \lambda_{n-1} x_{n-1})(x_n) = k(\lambda_1 x_1 + \cdots + \lambda_{n-1} x_{n-1} + \lambda_n x_n)$ for some $\lambda_n \in K$. □

Remark 2. From the proof of the above proposition, we can deduce that given K a field of characteristic zero and $L = K(y, z)$ a finite algebraic extension, it is always possible to find $\lambda \in K$ such that $L = K(y + \lambda z)$. Furthermore, the set $\{\lambda \in K : K(y + \lambda z) \neq K(y, z)\}$ is finite.

Corollary 1. *Let $X \subset \mathbb{C}^n$ be an irreducible algebraic curve and let $\mathbb{R}(x, y, z)$ be the quotient field of the integer domain $\mathbb{R}[X, Y, Z]/P$. Then for any $u \in \mathbb{R}(x, y, z) \setminus \mathbb{R}$ which is not algebraic over $\mathbb{R}$, $\mathbb{R}(x, y, z)$ is algebraic over $\mathbb{R}(u)$ and there is an element $v \in \mathbb{R}(x, y, z)$ such that $\mathbb{R}(x, y, z) = \mathbb{R}(u, v)$.*

Proof. As X is an irreducible algebraic curve then $\dim(X) = \mathrm{trdeg}_{\mathbb{R}}\mathbb{R}(x, y, z) = 1$, therefore there is $w \in \mathbb{R}(x, y, z)$ such that $\mathbb{R}(x, y, z)$ is algebraic over $\mathbb{R}(w)$. Take $u \in \mathbb{R}(x, y, z) \setminus \mathbb{R}$ such that u is not algebraic over $\mathbb{R}$. Since u is algebraic over $\mathbb{R}(w)$ there is a polynomial $F(t) \in \mathbb{R}(w)[t]$ such that $F(u) = 0$. Cleaning denominators we have a polynomial $F(s, t) \in \mathbb{R}[s, t]$ such that $F(w, u) = 0$. As u is not algebraic over $\mathbb{R}$ the variable s has to appear in $F(s, t)$, hence w is algebraic over $\mathbb{R}(u)$. Now as $\mathbb{R}(x, y, z)$ is algebraic over $\mathbb{R}(w)$ then $\mathbb{R}(x, y, z)$ is algebraic over $\mathbb{R}(w, u)$. $(\mathbb{R}(w) \subset \mathbb{R}(w, u) \subset \mathbb{R}(x, y, z))$, thus we have $\mathbb{R}(x, y, z)$ algebraic over $\mathbb{R}(w, u)$ and $\mathbb{R}(w, u) = \mathbb{R}(u)(w)$ algebraic over $\mathbb{R}(u)$, which implies $\mathbb{R}(x, y, z)$ algebraic over $\mathbb{R}(u)$.
On the other hand, as $\mathbb{R}$ is a field of characteristic zero then $\mathbb{R}(u)$ has also characteristic zero. Now, as $\mathbb{R}(x, y, z)$ is algebraic over $\mathbb{R}(u)$ and finitely generated over $\mathbb{R}(u)$, by Proposition (2) there is $v \in \mathbb{R}(x, y, z)$ such that $\mathbb{R}(x, y, z) = \mathbb{R}(u, v)$. □

The following theorem states that every irreducible algebraic curve is birationally equivalent to an irreducible plane curve. It is a well known fact. Notwithstanding, we include a constructive proof, since we shall need it in the next section.

Theorem 1. *Let X be an irreducible algebraic curve X in $\mathbb{C}^3$ passing through the origin. Then, there exists an irreducible algebraic plane curve $Y \subset \mathbb{C}^2$ crossing the origin, and a morphism of varieties $\mu : X \to Y$ such that:*

1. *The map μ is a birrational isomorphism that can be explicitly constructed.*
2. *There are open neighborhoods of the origin, in the Zariski topology, $X_0 \subset X$ and $Y_0 \subset Y$ such that the restriction $\mu|_{X_0} : X_0 \to Y_0$ is an isomorphism sending $O \in X_0$ into $O \in Y_0$.*

Proof. Suppose that $X = V(P)$ where $P \subset \mathbb{R}[X, Y, Z]$ is a prime ideal. Since X is an irreducible algebraic curve, then by definition $\dim(X) = \dim(\mathbb{R}[X, Y, Z]/P) = 1$. Denote by $\mathbb{R}(x, y, z)$ to the fraction field of $\mathbb{R}[X, Y, Z]/P$. Recall that $\dim(X) = \mathrm{trdeg}_{\mathbb{R}}\mathbb{R}(x, y, z)$.
It is clear for dimensional reasons that some of the variables x, y, z has to be transcendental over $\mathbb{R}$. Suppose without loss of generality that x is transcendental over $\mathbb{R}$. By Corollary 1, $\mathbb{R}(x) \subset \mathbb{R}(x, y, z)$ is an algebraic extension and by Proposition 2, we can always find $u = y + \lambda z$, for some $\lambda \in \mathbb{R}(x)$, such that $\mathbb{R}(x, y, z) = \mathbb{R}(x, u)$. Moreover, since this is true for almost all λ, this element can be taken to be any real constant, except for finitely many choices. Define $\varphi : \mathbb{R}[S, T] \to \mathbb{R}[x, u] \subset \mathbb{R}(x, y, z)$ as the $\mathbb{R}$-algebra homomorphism that sends $S \to x$ and $T \to u$. Clearly φ is surjective and therefore, if $J = \ker(\varphi)$, there is an isomorphism of $\mathbb{R}$-algebras $\varphi : \mathbb{R}[S, T]/J \xrightarrow{\sim} \mathbb{R}[x, u]$, and consequently $J \in \mathbb{R}[S, T]$ is a prime ideal. Denote $Y = V(J)$. The last isomorphism induces a field isomorphism $\mathbb{R}(Y) \cong \mathbb{R}(x, u) = \mathbb{R}(x, y, z)$, and therefore $\dim(Y) = \dim(X) = 1$. Hence $Y = V(J)$ is an irreducible algebraic plane curve which is birationally equivalent to X.

We also denote by φ its extension to the fraction field $\mathbb{R}(Y) = \mathbb{R}(s, t)$:

$$\varphi : \mathbb{R}(s, t) \to \mathbb{R}(x, y, z),$$

which sends $s \mapsto x$ and $t \mapsto u = y + \lambda z$. This morphism induces a morphism of varieties $\mu : X \to Y$ defined as $\mu(a, b, c) = (x(a, b, c), u(a, b, c)) = (a, b + \lambda c)$.
On the other hand, since $y, z \in \mathbb{R}(x, u)$ then we can write $y = f_1(x, u)/g_1(x, u)$ and $z = f_2(x, u)/g_2(x, u)$, for some polynomials $f_1, f_2, g_1, g_2 \in \mathbb{R}[X, U]$.
We claim that we can express y as $y = f_1(x, u)/g_1(x)$, with $g_1(x) \neq 0$, for suitable choices of $f_1(X, U) \in \mathbb{R}[X, U]$, and $g_1(X) \in \mathbb{R}[X]$, and such that $g_1(0) \neq 0$, where $u = y + \lambda z$. In fact, since x is transcendental over $\mathbb{R}$, by Corollary 1, the extension $\mathbb{R}(x) \subset \mathbb{R}(x)(u)$ is algebraic. Therefore, since $y \in \mathbb{R}(x, u)$ we can write y as:

$$y = \frac{a_0(x)}{b_0(x)} + \frac{a_1(x)}{b_1(x)}u + \cdots + \frac{a_r(x)}{b_r(x)}u^r,$$

where r is smaller than the degree of the field extension $[\mathbb{R}(x)(u) : \mathbb{R}(x)]$. Taking $b(x) = b_0(x) \cdots b_r(x)$ we can rewrite the last equation as

$$b(x)y = c_0(x) + c_1(x)u + \cdots + c_r(x)u^r, \tag{2.3}$$

for certain $c_i(x)$. Let us write $b(x) = x^l b'(x)$ and $c_i(x) = x^{l_i} c_i'(x)$, with $l, l_i \geq 0$, and with $b'(0) \neq 0$, $c_i'(0) \neq 0$. If $l > m = \min\{l_i : i = 0, \ldots, r\}$, we could divide both sides of 2.3 by x^m, and then, by letting $x = 0$ we would obtain a nonzero polynomial equation for u over $\mathbb{R}$, a contradiction. Thus, $l \leq l_i$, for all $i = 0, \ldots, r$, and we could divide both sides of 2.3 by x^l to obtain:

$$b'(x)y = d_0(x) + d_1(x)u + \cdots + d_r(x)u^r,$$

where $d_i(x) = x^{l_i - l} c_i'(x)$. Since $b'(0) \neq 0$, we may take

$$f_1(x, u) = d_0(x) + d_1(x)u + \cdots + d_r(x)u^r$$

and $g_1(x) = b'(x)$.

A similar argument shows that $z = f_2(x, u)/g_2(x)$ with $g_2(0) \neq 0$.
Summarizing, we have

$$y = \frac{f_1(x, u)}{g_1(x)} \quad \text{and} \quad z = \frac{f_2(x, u)}{g_2(x)}, \quad \text{where} \quad g_1(0) \neq 0, g_2(0) \neq 0.$$

These expressions induce a morphism $\tau : Y_0 \subset Y \to X$, defined as $\tau(d, e) = (d, \frac{f_1(d,e)}{g_1(d)}, \frac{f_2(d,e)}{g_2(d)})$, where $Y_0 \subset Y$ is the Zariski open set

$$D(g_1 g_2) = \{(d, e) \in \mathbb{R}^2 : g_1(d) \neq 0 \text{ and } g_2(d) \neq 0\}.$$

Notice that $(0, 0) \in Y_0$. Denote $\tau(Y_0)$ by X_0. The last morphism induces an $\mathbb{R}$-algebra homomorphism $\psi : \mathbb{R}(X) \to O_Y(Y_0)$ given by $\psi(x) = s$, $\psi(y) = f_1(s, t)/g_1(s)$, and $\psi(z) = f_2(s, t)/g_2(s)$. Clearly,

$$\varphi \circ \psi(x) = x, \quad \varphi \circ \psi(y) = \frac{f_1(x, u)}{g_1(x)} = y, \quad \varphi \circ \psi(z) = \frac{f_2(x, u)}{g_2(x)} = z. \tag{2.4}$$

Therefore, $\varphi \circ \psi = Id_{\mathbb{R}(X)}$, and thus $\varphi \circ \psi|_{X_0} : O_X|_{X_0} \to O_Y|_{Y_0}$ is the identity. On the other hand, $\psi \circ \varphi(s) = \psi(x) = s$ and $\psi \circ \varphi(t) = \psi(u)$. By (2.4) we have $\varphi \circ \psi(u) = u$ and $\varphi(t) = u$ which implies that $t = \psi(u)$, since φ is injective. Hence, $\psi \circ \varphi(t) = t$ and we conclude that $\psi \circ \varphi|_{Y_0} : O_Y|_{Y_0} \to O_X|_{X_0}$ is the identity. Therefore, $\psi : O_X|_{X_0} \to O_Y|_{Y_0}$ is the inverse of the morphism $\varphi : O_Y|_{Y_0} \to O_X|_{X_0}$, and thus the homomorphism $\rho : Y_0 \to X_0$ induced by ψ is the inverse of the restriction of $\mu : X_0 \to Y_0$.

Finally, it is clear that the morphism $\mu : X_0 \to Y_0$ sends the real part of X_0 into the real part of Y_0, and since $\mu^{-1} : Y_0 \to X_0$ is determined by the polynomials f_1, f_2, g_1 and g_2, which are all real polynomials, then μ^{-1} also sends the real part of Y_0 into the real part of X_0. □

2.4 Groebner bases

In this section we present some basic notions about Groebner bases and also some important results above Elimination theory that we will need in order to develop an algorithm to compute limits of quotients of polynomial functions of three varibles.

Let R denotes the polynomial ring in n-variables with coefficients in a field K, $R = K[x_1, \ldots, x_n]$, and denote the set of monomials of R by M, where recall that a monomial of R is a term of the form $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$.

Definition 2. A monomial order in R is a total order on M satisfying that given monomials $m_1 > m_2$, $nm_1 > nm_2 > m_2$ for every monomial $n \neq 1$.

One important property of monomial orders is that every monomial order is Artinian, in other words, every subset of M has a least element.

For a fixed monomial order $>$ in R, we define the initial term of an element $p \in R$, as the greatest term of p relative to $>$, and we denote it by $\text{in}(p)$. In other words, if $p \in R$ then $\text{in}(p) = \alpha x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, $\alpha \in K$, a term of p with the property that $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \geq m$ for every monomial m of p.
Given an ideal $I \subset R$ we define $\text{in}(I)$ as the ideal generated by the set $\{\text{in}(p) : p \in I\}$.

Definition 3. Let $I \subset R$ be an ideal and fix a monomial order in R. We say that a set of elements of I $\{f_1, \ldots, f_k\}$ is a *Groebner basis* for I if $\text{in}(I) = (\text{in}(f_1), \ldots, \text{in}(f_k))$.

We list some interesting facts about Groebner bases.

Remark 3.

1. The word *basis* in the name Groebner basis come from the fact that the set of monomials not in the ideal $\text{in}(I)$ forms a basis for the K-vector space R/I.

2. There always exists a Grobner basis for an ideal $I \subset R$. As R is a Noetherian ring then I is finitely generated, say, $I = (f_1, \ldots, f_k)$. Consider the ideal $J = (\text{in}(f_1), \ldots, \text{in}(f_k))$. If $J = \text{in}(I)$ then $\{f_1, \ldots, f_k\}$ is a Groebner basis for I. Otherwise, we can find $g_1 \in \text{in}(I)$ such that $g_1 \notin J$. As $g_1 \in \text{in}(I)$ then $\text{in}(g_1) = \text{in}(p_1)$ for some $p_1 \in I$, and we can consider now the set $\{f_1, \ldots, f_k, p_1\}$ and $J = (\text{in}(f_1), \ldots, \text{in}(f_k), \text{in}(p_1))$. We repeat this process until obtaining

$p_1, \dots p_s \in I$ such that $\text{in}(I) = (\text{in}(f_1), \dots, \text{in}(f_k), \text{in}(p_1), \dots, \text{in}(p_s))$. Notice that s is finite since R is Noetherian.

3. If $\{f_1, \dots, f_k\}$ is a Groebner basis for I then $I = (f_1, \dots, f_k)$. Suppose that there is $p \in I$ such that $p \notin (f_1, \dots, f_k)$. We can take the element p with $\text{in}(p)$ minimal. As $\text{in}(I) = (\text{in}(f_1), \dots, \text{in}(f_k))$ and $\text{in}(p) \in \text{in}(I)$ then $\text{in}(f_j)|\text{in}(p)$ for some $1 \leq j \leq k$, hence $\text{in}(p) = m\text{in}(f_j)$ for some monomial m. Notice that the polynomial $p - mf_j \notin (f_1, \dots, f_k)$ and $p - mf_j \in I$. However, $\text{in}(p - mf_j) < \text{in}(p)$ which is a contradiction.

4. There is a criterion that allows to compute algorithmically a Groebner basis for an ideal $I \subset R$. This criterion is known as the Buchberger's criterion (See [3], page 332).

5. Let I, J be ideals of R such that $I \subset J$. If $\text{in}(I) = \text{in}(J)$ then $I = J$.

An example of a monomial order is the pure lexicography order which is defined in the following way. Fix an order between the variables, for example $x_1 > x_2 > \cdots > x_n$, and define $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} > x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ if for the first j with $a_j \neq b_j$ we have that $a_j > b_j$. This is the main monomial order that we will use in this section.

Now we present an important result that will be needed later.

Consider the inclusion homomorphism $K[x_1, \dots, x_n] \hookrightarrow K[x_1, \dots x_n, y_1, \dots, y_s]$ and consider an ideal $I \subset K[x_1, \dots x_n, y_1, \dots, y_s]$. Given a Groebner basis for I we want to compute a Groebner basis for $I \cap K[x_1, \dots, x_n]$. For this we have to introduce the notion of an *elimination order*

Definition 4. A monomial order in $K[x_1, \dots x_n, y_1, \dots, y_s]$ is called an elimination order if the following condition holds: $f \in K[x_1, \dots x_n, y_1, \dots, y_s]$ with $\text{in}(f) \in K[x_1, \dots, x_n]$ implies $f \in K[x_1, \dots, x_n]$.

Lemma 1. *Let $I \subset K[x_1, \dots x_n, y_1, \dots, y_s]$ be an ideal and let $\mathcal{B} = \{f_1, \dots, f_k\}$ be a Groebner basis for I with respect to an elimination order. Assume that $f_1, \dots, f_t$ with $t \leq k$ are all elements of $\mathcal{B}$ such that $f_1, \dots, f_t \in K[x_1, \dots, x_n]$. Then $\{f_1, \dots, f_t\}$ is a Groebner basis for $I \cap K[x_1, \dots, x_n]$.*

See [3], page 380 for a proof.

Remark 4. Suppose that we have a ring homomorphism $\varphi : K[x_1, \dots, x_n] \to K[y_1, \dots, y_s]/J$ defined as $\varphi(x_i) = f_i$. Consider $F_i \in K[y_1, \dots, y_s]$ such that $\overline{F_i} = f_i$ in $K[y_1, \dots, y_s]/J$ and

define the ideal $I = JT + (F_1 - x_1, \ldots, F_n - x_n) \subset T$, where $T = K[x_1, \ldots, x_n, y_1, \ldots, y_s]$. Then $\ker \varphi = I \cap K[x_1, \ldots, x_n]$ (See [3], page 358). Therefore the above lemma implies that $\ker \varphi$ can be computed algorithmically.

3. REDUCTION TO THE CASE OF BIVARIATE FUNCTIONS

In order to compute $\lim_{(x,y,z)\to(0,0,0)} q(x,y,z)$, where $q(x,y,z) = f(x,y,z)/g(x,y,z)$, we introduced the *discriminant variety* $X(q) \subset \mathbb{C}^3$ associated to q, as the variety cut by the 2×2 minors of the matrix A (2.2). As a variety, $X(q)$ may be decomposed into its irreducible components:

$$X(q) = X_1 \cup X_2 \cup \cdots \cup X_n.$$

We are only interested in those components that contain the origin $O = (0,0,0)$. Suppose these are $X_1, X_2, \ldots, X_k$. We consider three possible cases:

1. dim $X_i = 0$: in this case, if $X_i = V(P_i)$ then $\mathbb{R}[X,Y,Z]/P_i$ is a field and therefore $X_i = \{O\}$. Hence, X_i does not contribute to any trajectory in $\mathbb{R}^3$ that approach O.

2. dim $X_i = 1$: in this case X_i is an irreducible algebraic curve.

3. dim $X_i = 2$: in this case X_i is an hypersurface, i.e., $X_i = V(P_i)$, where P_i is a principal ideal.

We only have to study cases 2 and 3.

Let us first deal with case 2. Suppose that we have q defined on an irreducible affine variety $X = V(P)$ of dimension 1, i.e., X is an irreducible space curve. By Theorem 1 the irreducible algebraic curve X is birationally equivalent to a plane curve Y, and furthermore, there exist a neighborhood X_0 of the origin in X and a neighborhood Y_0 of the origin in Y, and a homeomorphism $\mu : X_0 \to Y_0$ sending the origin to the origin and such that μ and μ^{-1} send real tuples in real tuples. Thus, the existence of the limit of q as $(x,y,z) \to O$ along the space curve X is equivalent to the existence of the limit of $q \circ \mu^{-1}(u,v)$ as $(u,v) \to (0,0)$ along the plane curve Y. Moreover,

$$\lim_{\substack{(x,y,z)\to O \\ (x,y,z)\in X}} q(x,y,z) \;=\; \lim_{\substack{(u,v)\to 0 \\ (u,v)\in Y}} q\circ\mu^{-1}(u,v).$$

Therefore, the problem of computing the last limit can be solved using the methods developed in [1].

Given X_i an irreducible component of $X(q)$ going through the origin O and of dimension 1, we denote by Y_i to the corresponding irreducible plane curve which is birationally equivalent to X_i and by $\mu_{X_i} : X_i \to Y_i$ to the corresponding local isomorphism (as in Theorem 1).
We have then proved the following:

Proposition 3. *Let X_i be an irreducible component of $X(q)$ of dimension 1. Then the existence as well as the value of the limit of $q(x, y, z)$ as $(x, y, z) \to O$ along X_i is determined by the limit of $q \circ \mu_{X_i}^{-1}(x, y)$ as $(x, y) \to (0, 0)$ along the irreducible plane curve Y_i.*

Now let us consider case 3. We want to see that this case may be reduced to case 2. Suppose that we have a rational function $q(x, y, z)$ defined on an irreducible hypersurface $X = V(h)$ where h is a real polynomial function of three variables and q has an isolated zero at 0. Let $\mathcal{S} = \mathrm{Sing}(X)$ be the singular locus of X. By Remark 1, $\mathcal{S}$ must be a variety of dimension strictly less than two. Hence, if $\mathcal{S}$ contains the origin, the limit of q as $(x, y, z) \to O$ along $\mathcal{S}$ can be computed as in case 2.
Now, we restrict our analysis to the nonsingular locus of X, that we will denote by $\mathcal{N} = X \setminus \mathcal{S}$. Without loss of generality we may assume that $\mathcal{N}$ approaches the origin, otherwise there is nothing to analyze.
Define a family of real ellipsoids $E_r = \{(x, y, z) \in \mathbb{R}^3 \ : \ Ax^2 + By^2 + Cz^2 - r^2 = 0\}$, $A, B, C > 0$, $r \neq 0$, where we denote $p_r(x, y, z) = Ax^2 + By^2 + Cz^2 - r^2$.

Definition 5. Let $X = V(h) \subset \mathbb{C}^3$ and $E_r = \{(x, y, z) \in \mathbb{R}^3 \ : \ Ax^2 + By^2 + Cz^2 - r^2 = 0\}$, $r \neq 0$ as above. The critical set $C_r(q)$ will be the set of all real points in $E_r \cap X$ where $q(x, y, z)$ attains its maxima and minima. The union $\cup_{r>0} C_r(q)$ of all critical sets will be denote by $\mathrm{Crit}_X(q)$.

Since each $E_r \cap X$ is a compact set, and by hypothesis O is an isolated zero of q, then $\mathrm{Crit}_X(q)$ is a well defined subset of X.

We have an analogous of Proposition 1.

Proposition 4. *The limit $\lim_{(x,y,z)\to O} q(x, y, z)$ along X exists and equals L if and only if for every $\epsilon > 0$ there is $\delta > 0$ such that for every $0 < r < \delta$ the inequality $|q(x, y, z) - L| < \epsilon$ holds for all $(x, y, z) \in C_r(q) \cap X$.*

Proof. Each point in the critical set must lie in some E_r, since $p = (a, b, c)$ is obviously contained in E_r, with $r = \sqrt{Aa^2 + Bb^2 + Cc^2}$. The rest of the proof is elementary, and follows identical lines as in Proposition 1. □

Our objective is to determine $\mathrm{Crit}_X(q)$. We may decompose this set as $\mathrm{Crit}_{\mathcal{N}}(q) = \mathrm{Crit}_X(q) \cap \mathcal{N}$ and $\mathrm{Crit}_X(q) \cap \mathcal{S}$. Since $\mathrm{Crit}_X(q) \cap \mathcal{S} \subset \mathcal{S}$ and the limit along $\mathcal{S}$ can be determined as in case 2, then we focus on $\mathrm{Crit}_{\mathcal{N}}(q)$.

First, we want to determine the nonsingular part of $\mathrm{Crit}_{\mathcal{N}}(q)$ by using Lagrange multipliers, as in [1]. For this we define $\mathfrak{X} = V(\mathfrak{J}) \subset X$, the zero set of the ideal $\mathfrak{J}$ generated by h and the determinant

$$d(x,y,z) = \begin{vmatrix} \partial p_r/\partial x & \partial p_r/\partial y & \partial p_r/\partial z \\ \partial h/\partial x & \partial h/\partial y & \partial h/\partial z \\ \partial q/\partial x & \partial q/\partial y & \partial q/\partial z \end{vmatrix}.$$

As the points of X already satisfy $\nabla q(x,y,z) = \lambda(x,y,z)$, (where ∇q denotes the gradient of q), and since $\nabla p_r(x,y,z) = (2Ax, 2By, 2Cz)$, the affine variety $\mathfrak{X}$ is then cut by the ideal generated by h and by the following determinant

$$D(x,y,z) = \begin{vmatrix} Ax & By & Cz \\ x & y & z \\ \partial h/\partial x & \partial h/\partial y & \partial h/\partial z \end{vmatrix}.$$

That is, $\mathfrak{X} = V(D,h)$. This variety is precisely the set of regular points of X that are critical points of q.

Proposition 5. *(Notations as above) Let us assume $O \in \mathcal{N}$. Then it is possible to choose (in a generic way) suitable positive constants A, B and C such that the height of the ideal $\mathfrak{J} = (D,h)$ in the polynomial ring $\mathbb{R}[x,y,z]$ is grater than one, and consequently* $\dim \mathfrak{X} < 2$.

Proof. It suffices to show that for a suitable choice of positive constants A, B, C there is at least one point $p \neq O$ in $\mathcal{N}$ such that $D(p) \neq 0$.

First, let us see that there is at least one point $p \in \mathcal{N}$ different from the origin such that the gradient of h does not point in the direction of p, i.e, such that $\nabla h(p) \neq \lambda p$, for all $\lambda \in \mathbb{R}$. Indeed, suppose on the contrary that for every $p \in \mathcal{N}$ there exists $\lambda(p) \neq 0$ such that $\nabla h(p) = \lambda(p)p$. Since each p is a regular point of X, $\nabla h(p) \neq 0$. Hence, after making an appropriated change of coordinates that fixes O (a rotation, and then a homothety) we may assume without loss of generality that $\partial h/\partial z(0,0,1) \neq 0$, and that $p = (0,0,1)$. Hence, by the implicit function theorem there would exist $U_0 \subset \mathbb{R}^2$, a neighborhood of $(0,0)$, and a smooth function $u(x,y)$ in U_0 such that $u(0,0) = 1$, and $h(x,y,u(x,y)) = 0$, for all $(x,y) \in U_0$. Since $\nabla h(p) = \lambda(p)p$, we must have $\partial h/\partial x(0,0,1) = \partial h/\partial y(0,0,1) = 0$, and consequently $\partial u/\partial x(0,0) = 0 = \partial u/\partial y(0,0)$.

Let W_p be the graph $W_p = \{(x, y, u(x, y)) \ : \ (x, y) \in U_0\}$. For any $\mathfrak{t} \in W_p$ the normal vector at $\mathfrak{t}$ is given by

$$n(\mathfrak{t}) = \frac{(-u_x, -u_y, 1)}{\sqrt{u_x^2 + u_y^2 + 1}}.$$

Henceforth, if $\mu(\mathfrak{t}) = \lambda(\mathfrak{t})/\|\nabla h(\mathfrak{t})\|$ we have that $\nabla h(\mathfrak{t}) = \mu(\mathfrak{t})\|\nabla h(\mathfrak{t})\|\mathfrak{t}$, and consequently $n(\mathfrak{t})$ can be written as

$$n(\mathfrak{t}) = \frac{(x, y, u(x, y))}{\sqrt{x^2 + y^2 + u^2(x, y)}}.$$

From this, we deduce:

$$\begin{aligned} \frac{1}{\sqrt{u_x^2 + u_y^2 + 1}} &= \frac{u(x, y)}{\sqrt{x^2 + y^2 + u^2(x, y)}}, \\ \frac{-u_x}{\sqrt{u_x^2 + u_y^2 + 1}} &= \frac{x}{\sqrt{x^2 + y^2 + u^2(x, y)}}, \end{aligned}$$

and

$$\frac{-u_y}{\sqrt{u_x^2 + u_y^2 + 1}} = \frac{y}{\sqrt{x^2 + y^2 + u^2(x, y)}}.$$

This implies $u_x = -x/u(x, y)$, and $u_y = -y/u(x, y)$. Hence, $u(x, y) = \sqrt{1 - x^2 - y^2}$, since $u(0, 0) = 1$. *We conclude that W_p would be a neighborhood of p in $\mathcal{N}$ which is part of a sphere centered at the origin.* But on the other hand, a theorem of Whitney asserts that $\mathcal{N}$ can only have finitely many connected components (see [4]). This would then imply that $\mathcal{N}$ could not pass through the origin, a contradiction.

Therefore, we may assume there exists a point $p \neq O$ in $\mathcal{N}$ such that $\nabla h(p) \neq \lambda p$, for all $\lambda \neq 0$. After applying a rotation, if necessary, we may also assume that a, b, c are all nonzero.

With this preliminaries, it is clear how to choose positive constants A, B and C such that the determinant

$$\begin{vmatrix} Aa & Bb & Cc \\ a & b & c \\ \partial h/\partial x(a, b, c) & \partial h/\partial y(a, b, c) & \partial h/\partial z(a, b, c) \end{vmatrix}$$

does not vanish: The vectors $\nabla h(p)$ and $p = (a, b, c)$ generate a plane H, since they are not parallel. Therefore, it suffices to choose any point (α, β, γ) outside H and such that $A = \alpha/a$, $B = \beta/b$, and $C = c/\gamma$ are positive. □

As before, for the limit $\lim_{(x,y,z)\to O} q(x, y, z)$ to exist along X it is necessary that it exists along any real curve that crosses O. In particular, they should exist along any component of $\mathfrak{X}$, and they

all must be equal. By the previous proposition $\dim(\mathfrak{X}) < 2$, hence, this last problem reduces to the cases 1 and 2.

Let $\mathfrak{Z}$ be the affine variety defined by the ideal generated by h and by the minors 2×2 of the matrix

$$\begin{bmatrix} Ax & By & Cz \\ \partial h/\partial x & \partial h/\partial y & \partial h/\partial z \end{bmatrix}.$$

The set $\mathfrak{Z} \cap E_r \cap \mathcal{N}$ defines the locus of those real points where E_r and $\mathcal{N}$ do not intersect transversely. Outside this set, $E_r \cap \mathcal{N}$ is a 1-dimensional manifold (See [42], page 30) that we shall denote by Σ. Clearly, the vanishing of these two by two minors forces the vanishing of the determinant $D(x, y, z)$. Henceforth, $\mathfrak{Z} \subset \mathfrak{X}$, and consequently $\dim(\mathfrak{Z}) < 2$, by Proposition 5.

Again, for the existence of the limit $\lim_{(x,y,z)\to O} q(x, y, z)$ it is required, in particular, its existence along any component of $\mathfrak{Z}$ that crosses O, and the problem reduces again to the cases 1 and 2. This take care of the subset of $\mathrm{Crit}_{\mathcal{N}}(q)$ inside $\mathfrak{Z}$.

As for those points in $\mathrm{Crit}_{\mathcal{N}}(q)$ that lie outside $\mathfrak{Z}$, we notice that they are contained in the 1-dimensional manifold Σ, then by Lagrange multipliers, they are part of $\mathfrak{X}$, since this variety is precisely those regular points where q attains an extreme value. Thus, the points in $\mathrm{Crit}_{\mathcal{N}}(q)$ that lie outside $\mathfrak{Z}$ must be contained in $\mathfrak{X}$, and thus the problem reduces again to the cases 1 and 2.

We summarize the discussion above in the following proposition:

Proposition 6. *Let X be an irreducible component of dimension 2 of the discriminant variety $X(q)$ passes through the origin O. Consider $\mathcal{S}$, $\mathfrak{X}$, and $\mathfrak{Z}$ defined as above. Then, the limit of $q(x, y, z)$ as $(x, y, z) \to O$ along X exists, and equals L, if and only if, the limit of $q(x, y, z)$ as $(x, y, z) \to O$ exists and equals L along each one of the components of the curves $\mathcal{S}$, $\mathfrak{X}$, and $\mathfrak{Z}$.*

We are ready to state our main result.

Theorem 2. *Let $q(x, y, z) = f(x, y, z)/g(x, y, z)$, where f and g are rational polynomial functions. Let $X(q)$ be the discriminant variety associated to q, and let us denote by $\{X_1, \ldots, X_k\}$ the irreducible components of dimension one of $X(q)$ that cross the origin, and by $\{X_{k+1}, \ldots, X_n\}$ the irreducible components of dimension two of $X(q)$ that pass through the origin. Then, the limit of q as $(x, y, z) \to O$ exists, and equals L, if and only if the limit of $q(x, y, z)$ as $(x, y, z) \to O$ along X_i exists, and equals L, for all $i = 1, 2, \ldots, n$. Moreover:*

1. *For the components X_i, $i = 1, 2, \ldots, k$, the limit of $q(x, y, z)$ as $(x, y, z) \to (0, 0, 0)$ along X_i is determined as in Proposition 3.*

2. *For the components* X_j, $j = k+1, \ldots, n$, *the limit of* $q(x, y, z)$ *as* $(x, y, z) \to (0, 0, 0)$ *along* X_j *is determined as in Proposition 6.*

4. A HIGH LEVEL ALGORITHM

In this chapter, using some ideas from Groebner bases, we develop an algorithm to compute the limit of a quotient of rational polynomial functions of three variables.

Using the ideas showed in the preliminaries in the section of Groebnes bases, we will show that given $X = V(P) \subset \mathbb{C}^3$ an irreducible space curve, if $\mathbb{R}(x, y, z)$ denotes the fraction field of $\mathbb{R}[X, Y, Z]/P$ and if x is transcendental over $\mathbb{R}$, we can check algorithmically if given $\lambda \in \mathbb{R}$, $\mathbb{R}(x, u) = \mathbb{R}(x, y, z)$ where $u = y + \lambda z$. Furthermore, we will see that if the last equality holds, it is algorithmically possible to compute the irreducible plane curve Y which is birrationally equivalent to X and also to compute the local isomorphism $\mu : X \to Y$, induced by the equality $\mathbb{R}(x, u) = \mathbb{R}(x, y, z)$.

Suppose that we have $X = V(P) \subset \mathbb{C}^3$ an irreducible algebraic curve, and denote the fraction field of $\mathbb{R}[X, Y, Z]/P$ by $\mathbb{R}(x, y, z)$. By Proposition 2 and Corollary 1, we know that if x is transcendental over $\mathbb{R}$ there exists $\lambda \in \mathbb{R}(x)$ such that $\mathbb{R}(x, y, z) = \mathbb{R}(x, u)$ where $u = y + \lambda z$. Also, by Theorem 1, if we consider $\varphi : \mathbb{R}[X, U] \to \mathbb{R}[X, Y, Z]/P$ defined by $\varphi(X) = x$, $\varphi(U) = y + \lambda z$, then $\ker \varphi$ defines the irreducible plane curve Y that is birrationally equivalent to X. Now, as we saw in the preliminaries in the section of Groebner bases, $\ker \varphi = (PT + (U - (Y + \lambda Z))) \cap \mathbb{R}[X, U]$ where $T = \mathbb{R}[X, U, Y, Z]$ is algorithmically computable. On the other hand, the ring homomorphism $\mathbb{R}[X, U]/\ker \varphi \to \mathbb{R}[X, Y, Z]/P$ induces a morphism of varieties $\mu : X \to Y$. As we saw in the proof of Theorem 1, since $y, z \in \mathbb{R}(x, u)$ then $y = f_1(x, u)/g_1(x)$ and $z = f_2(x, u)/g_2(x)$ for some f_1, f_2, g_1 and g_2 with real coefficients. Also in that proof, we saw that the local isomorphism $\mu : X \to Y$ is determined by those polynomials.

Remark 5. We can always assume that x, y and z are transcendental over $\mathbb{R}$, since otherwise the algebraic curve is actually a plane curve.

Remark 6. Let $X = V(P) \subset \mathbb{R}^3$ be an irreducible algebraic curve and denotes the fraction field of $\mathbb{R}[X, Y, Z]/P$ by $\mathbb{R}(x, y, z)$. Let $T = \mathbb{R}[X, U, Y, Z]$ and consider the lexicography order with

$Z > Y > U > X$. Let $I = \{h_1, \ldots, h_t\}$ be a Groebner basis for the ideal $I = PT + (U - (Y + \lambda Z))$ where $\lambda \in \mathbb{R}$. Then there exist $i, j \in \{1, 2, \ldots, t\}$ such that $h_i \in \mathbb{R}[X, U, Y]$ and $h_j \in \mathbb{R}[X, U, Z]$ involve the variable Y and Z respectively.

Proof. Notice that if $h_j \in \mathbb{R}[X, U]$ for all $j = 1, 2, \ldots, t$, then $\text{in}(h_j) = \alpha_j U^{a_j} X^{b_j}$ and as $U - (Y + \lambda Z) \in I$ then $U^{a_j} X^{b_j}$ divides Z for some $j = 1, 2, \ldots, t$ which is a contradiction. Hence, some h_j involves the variable Z or Y. Assume that $h_1, \ldots, h_k \in \mathbb{R}[X, U]$ and that $h_{k+1}, \ldots, h_t \notin \mathbb{R}[X, U]$. Thus $\text{in}(h_i) = \alpha U^{a_i} X^{b_i}$ with $a_i \neq 0$ for $i = 1, 2, \ldots, k$ and $\text{in}(h_j) = \alpha_j Z^{a_j} Y^{b_j} U^{c_j} X^{d_j}$ with $a_j \neq 0$ or $b_j \neq 0$ for $j = k + 1, \ldots, t$. As y and z are algebraic over $\mathbb{R}(x)$ there are non-null polynomials $p(X, Y) \in P \cap \mathbb{R}[X, Y] \subset I \cap \mathbb{R}[X, Y]$ and $q(X, Z) \in P \cap \mathbb{R}[X, Z] \subset I \cap \mathbb{R}[X, Z]$, thus $\text{in}(p) = \alpha Y^a X^b \in (\text{in}(h_1), \ldots, \text{in}(h_t))$ and $\text{in}(q) = \beta Z^c X^d \in (\text{in}(h_1), \ldots, \text{in}(h_t))$ where $a, c \neq 0$. Therefore $\text{in}(h_i) | Y^a X^b$ and $\text{in}(h_j) | Z^c X^d$ for some $i, j = 1, 2, \ldots, t$. Notice that $\text{in}(h_j)$ divides neither $Y^a X^b$ nor $Z^c X^d$ for $j = 1, 2, \ldots, k$, therefore $Z^{a_j} Y^{b_j} U^{c_j} X^{d_j} | Y^a X^b$ for some $j = k+1, \ldots, t$ which implies that $a_j = 0$ and thus $b_j \neq 0$ and $\text{in}(h_j) = \alpha_j Y^{b_j} U^{c_j} X^{d_j}$ with $b_j \neq 0$, hence $h_j \in \mathbb{R}[X, Y, U]$ and h_j involves the variable Y. In the same way, $Z^{a_i} Y^{b_i} U^{c_i} X^{d_i} | Z^c X^d$ for some $i = k + 1, \ldots, t$ which implies that $b_i = 0$ and thus $a_i \neq 0$ and $\text{in}(h_i) = \alpha_i Z^{a_i} U^{c_i} X^{d_i}$ with $a_i \neq 0$, hence $h_i \in \mathbb{R}[X, U, Z]$ and h_i involves the variable Z. □

The following lemma shows that given $\lambda \in \mathbb{R}$, it is possible to verify algorithmically if the equality $\mathbb{R}(x, y + \lambda z) = \mathbb{R}(x, y, z)$ holds.

Lemma 2. *Let $X = V(P) \subset \mathbb{C}^3$ be an irreducible algebraic curve and denotes the fraction field of $\mathbb{R}[X, Y, Z]/P$ by $\mathbb{R}(x, y, z)$. Let $T = \mathbb{R}[X, U, Y, Z]$ and consider the lexicography order with $Z > Y > U > X$. Let $\mathcal{B} = \{h_1, \ldots, h_t\}$ be a Groebner basis for the ideal $I = PT + (U - (Y + \lambda Z))$ where $\lambda \in \mathbb{R}$. Then $\mathbb{R}(x, u) = \mathbb{R}(x, y, z)$ where $u = y + \lambda z$ if and only if there are $i, j \in \{1, 2, \ldots, t\}$ such that $h_i \in \mathbb{R}[X, U, Y]$, $h_j \in \mathbb{R}[X, U, Z]$ have degree 1 in the variable Y and Z when they are viewed as polynomials in the variable Y and Z respectively. Furthermore, if $\mathbb{R}(x, u) = \mathbb{R}(x, y, z)$, then the values $f_1(x, u), f_2(x, u), g_1(x), g_2(x)$ described in Theorem 1 are given precisely by the elements $h_i, h_j \in \mathcal{B}$ satisfying that $h_i \in \mathbb{R}[X, U, Y]$ and $h_j \in \mathbb{R}[X, U, Z]$ have degree 1 in the variable Y and Z respectively.*

Proof. Suppose that $\mathbb{R}(x, u) = \mathbb{R}(x, y, z)$ where $u = y + \lambda z$. We saw in the proof of Theorem 1, that $y = f(x, u)/g(x)$ for some $f(X, U) \in \mathbb{R}[X, U]$, $g(X) \in \mathbb{R}[X]$, where $g(x, u) \neq 0$, and $g(0) \neq 0$. Thus $g(x)y - f(x, u) = 0$ in $\mathbb{R}(x, u)$, then $g(x)y - f(x, y + \lambda z) = 0$ in $\mathbb{R}(x, y, z)$. Therefore $g(X)Y - f(X, Y + \lambda Z) \in P \subset I$. Thus, $g(X)Y - f(X, (Y + \lambda Z - U) + U) \in I$ and as $Y + \lambda Z - U \in I$

then we get that $g(X)Y - f'(X,U) \in I$. If $p = g(X)Y - f'(X,U)$ then since $p \in I$, $\text{in}(h_j)$ divides $\text{in}(p)$ for some $j = 1, 2, \ldots, t$. Suppose that $\text{in}(p) = X^aY$, then the initial term of h_j need to have the form $\text{in}(h_j) = X^cY$. Hence, the other monomials of h_j involving the variable Y have the form X^kY. Thus, $h_j = r(X)Y + t(X,U)$, and clearly $r(X) \notin I$ since x is not algebraic over $\mathbb{R}$.
The reciprocal is clear. □

4.1 Description of the Algorithm

Let $q(X,Y,Z) = f(X,Y,Z)/g(X,Y,Z)$ where f and g are rational polynomial functions of three variables. Consider $X(q)$ the discriminant variety associated to q described in (2.2). We decompose $X(q)$ into its irreducible components and we choose only the irreducible components $\{X_1, \ldots, X_n\}$ going through the origin.
For the irreducible components of dimension 1 the algorithm do the following:
Suppose $\dim X = 1$ where $X = V(P)$. Denote the fraction field of $\mathbb{R}[X,Y,Z]/P$ by $\mathbb{R}(x,y,z)$. For random values $\lambda \in \mathbb{R}$, the algorithm verifies using the method described in Lemma 2, if $\mathbb{R}(x,u) = \mathbb{R}(x,y,z)$, where $u = y + \lambda z$. Notice that by Remark 2 discussed in the preliminaries, there are only finitely many values $\lambda \in \mathbb{R}$ such that $\mathbb{R}(x,u) \neq \mathbb{R}(x,y,z)$. If $\mathbb{R}(x,u) = \mathbb{R}(x,y,z)$, the algorithm compute the kernel of the map $\varphi : \mathbb{R}[X,U] \to \mathbb{R}[X,Y,Z]/P$ given by $\varphi(X) = x$ and $\varphi(U) = u = y + \lambda z$. As we saw before, this kernel is precisely the ideal $(PT + (U - (Y + \lambda Z))) \cap \mathbb{R}[X,U]$ where $T = \mathbb{R}[X,U,Y,Z]$, which is computable using Groebner bases. The plane curve which is birrationally equivalent to X is the variety Y cut by the ideal $\ker \varphi$.
Finally, the algorithm find the local isomorphism $\mu : X \to Y$ induced by the equality $\mathbb{R}(x,u) = \mathbb{R}(x,y,z)$. Again by Lemma 2 this morphism is computable. The existence of the limit

$$\lim_{(X,Y,Z)\to(0,0,0)} q(X,Y,Z)$$

along the irreducible space curve X is determined by the existence of the limit

$$\lim_{(X,U)\to(0,0)} q \circ \mu^{-1}(X,U)$$

along the irreducible plane curve Y and when the limits exist they are equal. The last limit is computed using the algorithm developed in [1].
For the irreducible components of dimension 2 the algorithm do the following:
Suppose that $\dim X = 2$. Then X is an affine variety cut by a principal ideal $P = (h)$. For random

positive values A, B and C the algorithm compute the height of the ideal $\mathfrak{J} = (h, D)$ where

$$D = \begin{vmatrix} Ax & By & Cz \\ x & y & z \\ \partial h/\partial x & \partial h/\partial y & \partial h/\partial z \end{vmatrix}.$$

As we saw in the reduction to plane curves, there always exist positive constants A, B and C such that $\mathrm{ht}(\mathfrak{J}) \geq 2$. Since $\dim(\mathfrak{X}) \leq 1$, $\mathfrak{X} = V(\mathfrak{J})$, then we compute the limit of $q(x, y, z)$ as $(x, y, z) \to O$ along $\mathfrak{X}$ using the above description for algebraic curves.

Since $\mathcal{S} = \mathrm{Sing}X$, the affine variety defined by the ideal $(h, \frac{\partial h}{\partial x}, \frac{\partial h}{\partial y}, \frac{\partial h}{\partial z})$ has dimension smaller than the dimension of X, then $\mathcal{S}$ is also an algebraic curve, and again we can compute the limit of $q(x, y, z)$ as $(x, y, z) \to O$ along $\mathcal{S}$ using the description of the algorithm for algebraic curves. (Recall that it is possible to have $X = \mathcal{S}$)

Now, the affine variety $\mathfrak{Z}$ defined by the ideal generated by the minors 2×2 of the matrix

$$\begin{bmatrix} Ax & By & Cz \\ \frac{\partial h}{\partial x} & \frac{\partial h}{\partial y} & \frac{\partial h}{\partial z} \end{bmatrix}$$

and the polynomial h, has also dimension less than 2. Hence, the limit of $q(x, y, z)$ as $(x, y, z) \to O$ along $\mathfrak{Z}$ is computed using the description of the algorithm for algebraic curves.

Finally, if the limit of $q(x, y, z)$ as $(x, y, z) \to O$ along each irreducible component of $X(q)$ of dimension one and two containing the origin exists and equals L, then we say that the limit of $q(x, y, z)$ as $(x, y, z) \to O$ is L. Otherwise, we say that this limit does not exists.

5. EXAMPLE

In this chapter we present an example of how the algorithm computes limits of quotients of rational polynomial functions of three varibales.

Suppose that we want to compute the following limit

$$\lim_{(X,Y,Z)\to(0,0,0)} \frac{YX - ZY + ZX}{X^2 + Y^2 + Z^2}.$$

If $q(X,Y,Z) = YX - ZY + XZ/X^2 + Y^2 + Z^2$, then in *maple* using the command **PrimeDecomposition(X(q))** we get the irreducible components of $X(q)$:

$V((Y-X+Z))$, $V((X^2+Y^2+Z^2))$, $V((X+Y, Z-2X))$, $V((X+Y, Z+X))$ and $V((X+Y, Z^2+2X^2))$.

Using in *Maple* the command **HilbertDimension(Q)** we see that for example the irreducible component $V(X+Y, Z+X)$ has dimension 1. Let us see that for $\lambda = 1$, $\mathbb{R}(x,u) = \mathbb{R}(x,y,z)$ where $u = y + z$. Here $\mathbb{R}(x,y,z)$ denotes the fraction field of the coordinate ring of $V(X+Y, Z+X)$. Consider the ideal $I = (X+Y, Z+X)T + (U-(Y+Z))$ where $T = \mathbb{R}[X,Y,Z,U]$. In *Maple* the command **EliminationIdeal(I,{U,X})** produces the ideal $J = (2X+U)$. On the other hand, the command **Basis(I,plex(Z,Y,U))** gives us a Groebner basis for I respect to the lexicography monomial order with $Z > Y > U$. In this particular case we obtain the following basis $\{2X + U, Y + X, Z + X\}$. From this basis we can deduce that $y = -x$ and $z = -x$ as elements of $\mathbb{R}(x,u)$. Therefore $\mathbb{R}(x,u) = \mathbb{R}(x,y,z)$ and the ideal $J = (2X+U)$ defines the irreducible plane curve which is birrationally equivalent to $V(X+Y, Z+X)$. Also, $y = -x$ and $z = -x$ determine the isomorphism $\mu^{-1} : V(2X+U) \to V(X+Y, Z+X)$. Therefore, the limit of $q(X,Y,Z)$ as $(X,Y,Z) \to (0,0,0)$ along $V(X+Y, Z+X)$ is equivalent to the limit of $q \circ \rho(X,U)$ as $(X,U) \to (0,0)$ along $V(2X+U)$. The last limit can be computed using the algorithm developed in [1], however in this case it is easy to see that the value of this limit is -1 since $q \circ \mu^{-1}(X,U) = q(X,-X,-X) = -1$. Therefore, the limit of $q(X,Y,Z)$ as $(X,Y,Z) \to (0,0,0)$ along $V(X+Y, Z+X)$ is -1.

Now, for the irreducible component of dimension 2, $V(Y-X+Z)$, if $h(X,Y,Z)=Y-X+Z$ then with the positive constants $A=1$, $B=2$ and $C=1$, using the command **HilbertDimension(P)** with $P=(h,D)$, where $D=\begin{vmatrix} X & 2Y & Z \\ X & Y & Z \\ \frac{\partial h}{\partial X} & \frac{\partial h}{\partial Y} & \frac{\partial h}{\partial Z} \end{vmatrix}$, we obtain that the variety cut by the ideal $P=(h,D)$ has dimension 1. In this case $V(P)=V(-XY-YZ,Y-X+Z)$. Using again the command **PrimeDecomposition(P)** we obtain the irreducible components of the variety $V(P)$, $V(P)=V(Y,-X+Z)\cup V(2X-Y,Y+2Z)$ where each of these components has dimension 1. Therefore we can apply the algorithm for irreducible algebraic curves, and it is not difficult to see following the same procedure as for the variety $V(Y+X,Z+X)$ that the limit of $q(X,Y,Z)$ as $(X,Y,Z)\to(0,0,0)$ along the variety $V(Y,-X+Z)$ is $1/2$.

Hence, we conclude that

$$\lim_{(X,Y,Z)\to(0,0,0)} \frac{YX-ZY+ZX}{X^2+Y^2+Z^2}$$

does not exist.

6. COMPUTATIONS OVER REAL EXTENSIONS OF $\mathbb{Q}$

In this section we show how to extend the methods thus developed to compute the limit of quotients of polynomials, when their coefficients lie in a *real extension* of the rationals. This is a standard procedure that is independent of the number of variables involved, and it was already discussed in great detail in [1]. Hence, we will just limit ourselves to recall how this could be achieved. We refer the reader to [1] for a thorough discussion.

Let $\mathbb{Q} \subset E$ be any finite field extension of the rationals. E will be called a *real extension* if there is an embedding of fields $\lambda : E \to \mathbb{R}$. Let $g(z)$ be an irreducible polynomial in $E[z]$. The class of z in the quotient $F[z]/(g(z))$ will be called a *symbolic root* of g. Symbolic roots will be denoted by lower case letters, so that, for instance, $E(b)$ will denote the extension field $E(b) \simeq E[z]/(g(z))$. If E is a real extension, we speak of b as a *real symbolic root over* E if any given embedding $\lambda : E \to \mathbb{R}$ can be extended to an embedding $\lambda' : E(b) \to \mathbb{R}$.

Let $\lambda : E \to \mathbb{R}$ be an embedding of a finite field extension of the rationals, and let b be a symbolic root over E. Since any extension of the rationals is principal, there exists b' such that $E(b) = \mathbb{Q}(b')$, an element that can be computed as a linear combination with rational coefficients of a finite set of generators of $E(b)$. From this, its minimal polynomial over $\mathbb{Q}$ can also be effectively determined. Sturm's Theorem [7] can then be used to *effectively* determine if the minimal polynomial of b' over the rationals has a real root, and consequently to determine if b is a real symbolic root over E.

Suppose now that $q(X, Y, Z) = f(X, Y, Z)/g(X, Y, Z)$ is a quotient of polynomial functions with coefficients that lie in possibly different real extensions of $\mathbb{Q}$. Without lost of generality, we may assume that they are all contained in a larger real extension E. We want to compute the limit of $q(X, Y, Z)$, as $(X, Y, Z) \to (0, 0, 0)$. For this, we notice that the discriminant variety $X(q)$ associated to q is defined by an ideal also generated by polynomials with coefficients that turn out to be in E. Thus, when we decompose $X(q)$ into its irreducible components, the varieties obtained also have all their coefficients in E. Once the problem has been reduced to the case of two variables, the necessary computations are all carried out within E, as shown in [1].

Part II

CLASSIFICATION OF G-GRADED TWISTED ALGEBRAS

7. INTRODUCTION

G-graded twisted algebras were introduced in [17], and independently in [19], as distinguished mathematical structures which arise naturally in theoretical physics [20], [21], [22], [23], [24] and [18]. A G-graded twisted algebra W is an algebra over a commutative ring R with a G-grading, i.e., $W = \oplus_{g \in G} W_g$, with $W_a W_b \subset W_{ab}$. Each W_g is assumed to be a free R-module of rank one, and we demand that W is free of zero monomial divisors, i.e., $w_a \cdot w_b \neq 0$ for every non-zero elements $w_a \in W_a$, $w_b \in W_b$. We also demand that W has an identity element $1 \in W_e$, where W_e denotes the graded component corresponding to the identity element $e \in G$.

We deal with the classification problem for non-associative G-graded twisted algebras that satisfy a particular type of symmetry condition. In Theorem 10 we provide an exact formula to count (up to graded isomorphisms) all symmetric algebras that are graded over an abelian group. This generalizes the main result obtained in [26] for cyclic groups.

8. PRELIMINARIES

8.1 Group Cohomology

We start recalling the standard definition of the group cohomology.

Let G be a group and A a G-module.

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

We write $H^*(G, A)$ for right derived functors $R^*(\_^G)$ and call them the cohomology groups of G with coefficients in A.

It is not difficult to see that if we consider $\mathbb{Z}$ as a trivial G-module then we have that $A^G \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ and therefore $H^*(G, A) \cong \mathrm{Ext}^*_{\mathbb{Z}[G]}(\mathbb{Z}, A)$.

We will show a particular projective resolution of $\mathbb{Z}[G]$-modules for $\mathbb{Z}$ as a trivial G-module and with this resolution we will compute $\mathrm{Ext}^*_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ and hence the cohomology groups of G with coefficients in A.

8.1.1 A particular free resolution for $\mathbb{Z}$

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

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

An straightforward computation shows that $\partial_{n-1} \circ \partial_n = 0$, thus we have the following complex of free $\mathbb{Z}$-modules

$$\cdots \longrightarrow F_n \xrightarrow{\partial_n} F_{n-1} \xrightarrow{\partial_{n-1}} F_{n-2} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\partial_1} F_0 \longrightarrow 0 \tag{8.1}$$

Note that $F_0 = \mathbb{Z}[G]$. If we consider the augmentation of the complex (8.1), that is to say, define $\mathcal{E} : F_0 = \mathbb{Z}[G] \to \mathbb{Z}$ as the $\mathbb{Z}$-homomorphism that sends every $g \in G$ to $1 \in \mathbb{Z}$ and

consider the following new complex

$$\cdots \longrightarrow F_n \xrightarrow{\partial_n} F_{n-1} \xrightarrow{\partial_{n-1}} F_{n-2} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\mathcal{E}} \mathbb{Z} \longrightarrow 0 \tag{8.2}$$

We claim that (8.2) is a resolution of free $\mathbb{Z}$-modules for $\mathbb{Z}$.

Indeed, if $F_\bullet$ denotes the complex (8.2), let us see that the morphisms of complexes $id : F_\bullet \to F_\bullet$ and $0 : F_\bullet \to F_\bullet$ are homotopic.

Define $h_{-1} : \mathbb{Z} \to F_0$ as $h_{-1}(1) = e \in G$ and for $n = 0, 1, 2, \ldots$ define $h_n : F_n \to F_{n+1}$ as $h_n(g_0, \ldots, g_n) = (e, g_0, \ldots, g_n)$.

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

It is an easy exercise to verify that $id - 0 = id = \partial_{n+1} \circ h_n + h_{n-1} \circ \partial_n$ for $n = 0, 1, 2, \ldots$ where $\partial_0 = \mathcal{E}$.

Therefore the induced maps in the homologies are the same, i.e., $id : \frac{\ker(\partial_n)}{\mathrm{im}(\partial_{n+1})} \to \frac{\ker(\partial_n)}{\mathrm{im}(\partial_{n+1})}$ and $0 : \frac{\ker(\partial_n)}{\mathrm{im}(\partial_{n+1})} \to \frac{\ker(\partial_n)}{\mathrm{im}(\partial_{n+1})}$ are the same maps and hence $\frac{\ker(\partial_n)}{\mathrm{im}(\partial_{n+1})} = 0$.

Thus we have that the complex (8.2) is actually 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 $g \cdot (g_0, \ldots, g_n) = (gg_0, \ldots, gg_n)$ and $\mathbb{Z}$ is a G-module with the trivial action.

Let us see that each F_n is a free $\mathbb{Z}[G]$-module.

We have an action of G over G^{n+1}. Note that every $(g_0, g_1, \ldots, g_n) = g_0 \cdot (e, g_0^{-1}g_1, \ldots g_0^{-1}g_n)$, and $(e, g_1, \ldots, g_n) \neq g \cdot (e, g_1', \ldots, g_n')$ for all $g \neq e$.

Therefore the orbits given by this action are $\mathcal{O}_{(e,g_1,\ldots,g_n)}$ with $g_i \in G$ for $i = 1, 2, \ldots, n$ and thus

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

Hence

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

but $\mathcal{O}_{(e,g_1,\ldots,g_n)} \cong G/G_{(e,g_1,\ldots,g_n)}$ where $G_{(e,g_1,\ldots,g_n)} = \{g \in G : g \cdot (e, g_1, \ldots, g_n) = (e, g_1, \ldots, g_n)\} = \{e\}$. Thus $\mathcal{O}_{(e,g_1,\ldots,g_n)} \cong G$.

We conclude 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 they are linear independent.
Finally what we have is that the resolution of free $\mathbb{Z}$-modules for $\mathbb{Z}$ given in (8.2) is actually a resolution of free $\mathbb{Z}[G]$-modules for $\mathbb{Z}$ viewed as a G-module with the trivial action.

8.1.2 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 basis that we call the bar basis for F_n.
Define $[g_1|g_2|\cdots|g_n] := (e, g_1, g_1g_2, \dots, g_1g_2\cdots g_n)$.
We claim that the set $\{[g_1|g_2|\cdots|g_n] : (g_1, \dots, g_n) \in G^n\}$ is also a basis for F_n. In fact, this set is clearly linear independent and note that 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 $\{[g_1|g_2|\cdots|g_n] : (g_1, \dots, g_n) \in G^n\}$, since $(e, g_1, g_2, \dots, g_n) = (e, g_1', g_1'g_2', \dots, g_1'g_2'\cdots g_n') = [g_1'|g_2'|\cdots|g_n']$ where $g_i' = g_{i-1}^{-1}g_i$ for $i = 1, 2, \dots, n$.
Therefore $\{[g_1|g_2|\cdots|g_n] : (g_1, \dots, g_n) \in G^n\}$ is a basis for F_n as a $\mathbb{Z}[G]$-module and we say it is the bar basis for F_n.
Now, if we compute the boundary homomorphisms $\partial_n : F_n \to F_{n-1}$ given in (8.2) in the bar basis, we get the following equation:

$$\begin{aligned}
\partial_n([g_1|g_2|\cdots|g_n]) &= \partial_n(e, g_1, g_1g_2, \dots, g_1g_2\cdots g_n) = (g_1, g_1g_2, \dots, g_1g_2\cdots g_n) \ + \\
&+ \ \sum_{i=1}^{n-1}(-1)^i(e, g_1, \dots, g_1g_2\cdots g_{i-1}, g_1\widehat{g_2\cdots}g_i, g_1g_2\cdots g_{i+1}, \dots, g_1g_2\cdots g_n) \\
&+ (-1)^n(e, g_1, g_1g_2, \dots, g_1g_2\cdots g_{n-1}) \\
&= g_1[g_2|\cdots|g_n] + \sum_{i=1}^{n-1}(-1)^i[g_1|\cdots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\cdots|g_n] \ + \\
&+ \ (-1)^n[g_1|\cdots|g_{n-1}].
\end{aligned}$$

Thus we have that $\partial_n : F_n \to F_{n-1}$ in the bar basis is given by

$$\partial_n([g_1|\cdots|g_n]) = g_1[g_2|\cdots|g_n] + \sum_{i=1}^{n-1}(-1)^i[g_1|\cdots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\cdots|g_n] \ + \ (-1)^n[g_1|\cdots|g_{n-1}]. \tag{8.3}$$

The resolution given in (8.2)

$$\cdots \longrightarrow F_n \xrightarrow{\partial_n} F_{n-1} \xrightarrow{\partial_{n-1}} F_{n-2} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \tag{8.4}$$

in the bar basis is what we call the bar resolution for $\mathbb{Z}$.
(Note that $\{[e] = (e)\}$ is the bar basis for F_0).

8.1.3 Another way to compute the cohomology of groups

From now on, we consider F_n with the bar basis.
For $n = 0, 1, 2, \ldots$ define $C^n(G, A) = \{\varphi : G^n \to A\}$ the set of functions from G^n to A. $(G^0 = \{e\})$.
$C^n(G, A)$ 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 $\mathrm{Hom}_{\mathbb{Z}[G]}(F_n, A)$ as G-modules.
Indeed, define

$$\begin{array}{rccc} \mu: & C^n(G,A) & \to & \mathrm{Hom}_{\mathbb{Z}[G]}(F_n, A) \\ & \varphi & \mapsto & \mu(\varphi) \end{array}$$

where $\mu(\varphi)([g_1|\cdots|g_n]) = \varphi(g_1, \ldots, g_n)$.
It is a $\mathbb{Z}[G]$-homomorphism with inverse

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

where $\mu^{-1}(\psi)(g_1, \ldots, g_n) = \psi([g_1|\cdots|g_n])$.
Therefore we have the following commutative diagram:

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

where $\partial^*_{n+1}(\psi) = \psi \circ \partial_{n+1}$, μ is an isomorphism and $\partial^n = \mu \circ \partial^*_{n+1} \circ \mu^{-1}$.
If we compute explicitly the morphism ∂^n we have:

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

and by (8.3)

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

hence

$$\begin{aligned}
&\partial^n(\varphi)(g_1,\ldots,g_{n+1}) = \mu\circ\varphi(\partial_{n+1}([g_1|\cdots|g_{n+1}]))\\
&= \mu\circ\varphi(\partial_n([g_1|\cdots|g_{n+1}]) = g_1[g_2|\cdots|g_{n+1}] + \sum_{i=1}^{n}(-1)^i[g_1|\cdots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\cdots|g_{n+1}] \ + \ (-1)^{n+1}[g_1|\cdots|g_n])\\
&= \mu(g_1\varphi([g_2|\cdots|g_{n+1}]) + \sum_{i=1}^{n}(-1)^i\varphi([g_1|\cdots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\cdots|g_{n+1}]) + (-1)^{n+1}\varphi([g_1|\cdots|g_n]))\\
&= g_1\varphi(g_2,\ldots,g_{n+1}) + \sum_{i=1}^{n}(-1)^i\varphi(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_{n+1}) + (-1)^{n+1}\varphi(g_1,\ldots,g_n).
\end{aligned} \tag{8.5}$$

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

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

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

where the squares commutes.

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

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

and

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

8.2 G-graded twisted algebras

Definition 6. Let G denote a group. A G-graded twisted algebra W is an algebra over a commutative ring R with a G-grading, i.e., $W = \oplus_{g\in G}W_g$, with $W_aW_b \subset W_{ab}$. Each W_g is assumed to be a free

R-module of rank one, and we demand that W is free of zero monomial divisors, i.e., $w_a \cdot w_b \neq 0$ for every non-zero elements $w_a \in W_a$, $w_b \in W_b$. We also demand that W has an identity element $1 \in W_e$, where W_e denotes the graded component corresponding to the identity element $e \in G$.

As each graded component W_g is a vector space of dimension one, each choice of a non zero element $w_g \in W_g$, for each $g \in G$, produces a graded basis $\mathcal{B} = \{w_g : g \in G\}$ for W. For each such basis there is a structure constant associated to it, $C_{\mathcal{B}} : G \times G \to A$, defined by the identity: $w_a \cdot w_b = C_{\mathcal{B}}(a,b)w_{ab}$. Here $A \subset K^*$ must be a subgroup of the multiplicative group of all nonzero elements of K, since W has no zero divisor monomials. From now on we will omit the subscript $\mathcal{B}$ if a particular basis is clear in the context.

Given a structure constant $C : G \times G \to A$, we define two important functions $q : G \times G \to A$ and $r : G \times G \times G \to A$ as:

$$\begin{aligned} q(a,b) &= C(a,b)C(b,a)^{-1} \\ r(a,b,c) &= C(b,c)C(ab,c)^{-1}C(a,bc)C(a,b)^{-1}. \end{aligned} \tag{8.6}$$

The associativity of elements of W can be described in terms of the function $r : G \times G \times G \to A$ as follows: $w_a \cdot (w_b \cdot w_c) = r(a,b,c)(w_a \cdot w_b) \cdot w_c$. When G is an abelian group, the commutativity of elements of W is given in terms of the function $q : G \times G \to A$ as $w_a \cdot w_b = q(a,b)w_b \cdot w_a$.

Definition 7. A morphism between two G-graded twisted K-algebras $W = \oplus_{g\in G} W_g$ and $V = \oplus_{g\in G} V_g$ is an unitarian homomorphism of K-algebras $\varphi : W \to V$. If the homomorphism preserves the grading, i.e., $\varphi(W_g) \subset V_g$, we say the morphism is *graded*.

The following theorem relates the associative G-graded twisted algebras with elements of the second group of cohomology $H^2(G,A)$. This is fundamental in the classification of all associative G-graded twisted algebras.

Theorem 3. *Let $V = \oplus_{g\in G} V_g$ and $W = \oplus_{g\in G} W_g$ be two G-graded twisted K-algebras. Let us fix bases $\mathcal{B}_1$ and $\mathcal{B}_2$ for V and W, respectively, and let $C_1, C_2 : G \times G \to K^*$ be the respective structure constants. Then V is graded-isomorphic to W if and only if the function $C_1C_2^{-1}$ belongs to the kernel of $\partial^2 : C^2(G,K^*) \to C^3(G,K^*)$ and the equivalence class $[C_1C_2^{-1}]$ is trivial in $H^2(G,K^*)$, where K^* is viewed as a G-module with the trivial action.*

Proof. Suppose that V and W are graded-isomorphic as K-algebras, this means that there is a grading preserving isomorphism $\psi : V \to W$. This isomorphism induces a function $\varphi : G \to K^*$ defined as $\varphi(g) \in K^*$ is the unique element satisfying $\psi(v_g) = \varphi(g)w_g$. As ψ is a homomorphism then $\psi(v_a)\psi(v_b) = \psi(v_a \cdot v_b)$ which implies $\varphi(a)\varphi(b)w_a \cdot w_b = C_1(a,b)\varphi(ab)w_{ab}$, and thus

$\varphi(a)\varphi(b)C_2(a,b) = C_1(a,b)\varphi(ab)$. Therefore, $C_1(a,b)C_2(a,b)^{-1} = \varphi(a)\varphi(ab)^{-1}\varphi(b)$. Now, notice that $\partial^1(\varphi)(a,b) = \varphi(a)\varphi(ab)^{-1}\varphi(b)$, hence $C_1C_2^{-1} \in C^2(G,K^*)$ is such that $C_1C_2^{-1} = \partial^1(\varphi)$, thus $C_1C_2^{-1} \in \mathrm{im}(\partial^1)$ which implies that $C_1C_2^{-1} \in \ker\partial^2$, and $[C_1C_2^{-1}] = 1$ in $H^2(G,K^*)$.
Reciprocally, if $\partial^2(C_1C_2^{-1}) = 1$ and $[C_1C_2^{-1}] = 1$ in $H^2(G,K^*)$, then $C_1C_2^{-1} \in \mathrm{im}(\partial^1)$ and therefore there exists $\varphi \in C^1(G,K^*)$ such that $\partial^1(\varphi) = C_1C_2^{-1}$, then $C_1(a,b)C_2(a,b)^{-1} = \varphi(a)\varphi(ab)^{-1}\varphi(b)$. This last equation implies that the homomorphism of K-vector spaces $\psi : V \to W$ defined as $\psi(v_g) = \varphi(g)w_g$ is a homomorphism of K-algebras. As $\varphi(g) \neq 0$ for every $g \in G$ it follows that ψ is injective, and as V and W are K-vector spaces of the same dimension we conclude that ψ is an isomorphism. □

Remark 7. If $W = \oplus_{g\in G}W_g$ is a G-graded twisted K-algebra with a fixed basis $\mathcal{B} = \{w_g : g \in G\}$ and structure constant $C : G \times G \to A$, the function $r : G \times G \times G \to A$ defined in (8.6) is precisely $\partial^2(C)$.

As a consequence of the last theorem we have the following corollaries:

Corollary 2. *Let $W = \oplus_{g\in G}W_g$ be a G-graded twisted K-algebra, and let $\mathcal{B}$ and $\mathcal{B}'$ be bases for W, with associated structure constants C and C' respectively. Then the corresponding associative functions r and r' defined as in (8.6), are the same. In other words, the associative function of W does not depend on any chosen basis.*

Proof. Consider the identity homomorphism $i : W \to W$ which is clearly graded. By Theorem 3, $C'C^{-1} \in \ker\partial^2$ and $[C'C^{-1}] = 1$ in $H^2(G,K^*)$. Hence, $\partial^2(C'C^{-1}) = 1$ which implies that $\partial^2(C) = \partial^2(C')$. Thus, $r = r'$. □

Corollary 3. *Let $V = \oplus_{g\in G}V_g$ and $W = \oplus_{g\in G}W_g$ two associative G-graded twisted K-algebras, and let $\mathcal{B}$ and $\mathcal{B}'$ be bases for V and W, respectively, and let C_1 and C_2 the respective associated structure constants. Then V is graded-isomorphic to W if and only if $[C_1] = [C_2]$ in $H^2(G,K^*)$, where K^* is viewed as a G-module with the trivial action.*

Proof. As V and W are associative algebras, then the associative functions r and r' for V and W, are 1. Therefore, $\partial^2(C_1) = 1$ and $\partial^2(C_2) = 1$, i.e., $C_1, C_2 \in \ker\partial^2$. Hence, $[C_1C_2^{-1}] = 1$ in $H^2(G,K^*)$ is equivalent to $[C_1] = [C_2]$ in $H^2(G,K^*)$, and the result follows from Theorem 3. □

9. CLASSIFICATION OF $(1,2)$-SYMMETRIC G-GRADED TWISTED $\mathbb{C}$-ALGEBRAS.

In [26], it was proved that for $G \cong \mathbb{Z}_n$, a cyclic group, the number of non-(graded) isomorphic $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebras with structure constants taking values in a finite subgroup $A \subset \mathbb{C}^*$ is given by $|R_n|^{|G|-2} = |R_n|^{n-2}$, where R_n denotes the set of n-th roots of unity in A. In this chapter, we provide a generalization of the arguments used in [26] that will allow us to state an equivalent result for the case of any finite abelian group. For the sake of clarity we first focus on groups that are the product of only two cyclic groups. At the end of this chapter we deal with finite abelian groups in general.

Definition 8. Let W be a G-graded twisted K-algebra. We say that W is $(1,2)$-symmetric if $r(a,b,c) = r(b,a,c)$ for every $a,b,c \in G$.

9.1 Classification of $(1,2)$-symmetric $\mathbb{Z}_m \times \mathbb{Z}_n$- graded twisted $\mathbb{C}$-algebras.

Suppose G is presented as a product $\mathbb{Z}_m \times \mathbb{Z}_n$, and consider $W = \bigoplus_{a,b\in G} W_{a,b}$ a $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebra, with a fixed basis $\{x_{a,b} \ : \ x_{a,b} \in W_{a,b}\}$ and structure constant $\widetilde{C} : G \times G \to A \subset \mathbb{C}^*$, A a subgroup of $\mathbb{C}^*$. When $G = \mathbb{Z}_n$ is a cyclic group with generator $g \in G$, a basis for W was called *standard* in [26] if it had the form $\{1, w_g^{(1)}, w_g^{(2)}, \ldots, w_g^{(n-1)}\}$ where $w_g^{(i)} = w_g \cdot w_g^{(i-1)}$ and $w_g \cdot w_g^{(n-1)} = 1$ [26]. We generalize this construction as follows. We may

think of the graduation of W as an array of the following form:

$$\begin{array}{ccccc} W_{0,0} & W_{0,1} & W_{0,2} & \cdots & W_{0,n-1} \\ W_{1,0} & W_{1,1} & W_{1,2} & \cdots & W_{1,n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ W_{m-1,0} & W_{m-1,1} & W_{m-1,2} & \cdots & W_{m-1,n-1} \end{array}.$$

As in the cyclic case, we choose standard bases for the first row and first column. These two bases will be denoted by $\{1, w_{0,1}, w_{0,2}, \ldots, w_{0,n-1}\}$ and $\{1, w_{1,0}, w_{2,0}, \ldots, w_{m-1,0}\}$, respectively. Now for the i-th row define $w_{i,j} = w_{0,1} \cdot w_{i,j-1}$ for $j = 1, \ldots, n-1$. We notice that $w_{0,1} \cdot w_{i,n-1} \in W_{i,0}$. Hence, $w_{0,1} \cdot w_{i,n-1} = \alpha_i \cdot w_{i,0}$, for some $\alpha_i \in A$. We call $\mathcal{B} = \{w_{i,j} \ : \ i = 0, \ldots, m-1, \ j = 0, \ldots, n-1\}$ a *standard basis* for W.

Define $T_{i,j} : W \to W$ to be the linear transformation given by $T_{i,j}(x) = w_{i,j} \cdot x$. For $T_{0,1}$, its rational form consists of m-blocks where each one looks like

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & \alpha_i \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix},$$

where $\alpha_0 = 1, \alpha_1, \ldots, \alpha_{m-1}$ are elements in A such that $T_{0,1}(w_{i,n-1}) = \alpha_i \cdot w_{i,0}$. Let us denote by $\{e_{i,j}\}_{j=0,\ldots,n-1}$ the n-th roots of α_i, for $i = 0, \ldots, m-1$. we claim that $e_{i,j}$ is an eigenvalue of $T_{0,1}$ with eigenvector

$$z_{i,j} = \sum_{k=0}^{n-1} e_{i,j}^{-k} \cdot w_{i,k}. \tag{9.1}$$

In fact,

$$\begin{aligned} T_{0,1}(z_{i,j}) &= \sum_{k=0}^{n-1} e_{i,j}^{-k} T_{0,1}(w_{i,k}) \\ &= \sum_{k=0}^{n-2} e_{i,j}^{-k} w_{i,k+1} + e_{i,j}^{-(n-1)} \alpha_i w_{i,0} \\ &= \sum_{k=1}^{n-1} e_{i,j}^{-k+1} w_{i,k} + e_{i,j} w_{i,0} \\ &= e_{i,j} \sum_{k=0}^{n-1} e_{i,j}^{-k} w_{i,k} = e_{i,j} z_{i,j}. \end{aligned} \tag{9.2}$$

From now on, the elements of the group G will be denoted by products of the form $a^r b^s$, with $0 \leq r \leq m-1$, $0 \leq s \leq n-1$. Also we will write $w_{r,s} \cdot w_{i,j} = C(a^r b^s, a^i b^j) \cdot w_{r+i,s+j}$.
We claim that $T_{r,s} \circ T_{i,j}(x) = q(a^r b^s, a^i b^j) \cdot T_{i,j} \circ T_{r,s}(x)$ for every $x \in W$. It is enough to prove it for the basis elements. Indeed,

$$\begin{aligned} T_{r,s} \circ T_{i,j}(w_g) &= w_{r,s} \cdot (w_{i,j} \cdot w_g) = r(a^r b^s, a^i b^j, g)(w_{r,s} \cdot w_{i,j}) \cdot w_g \\ &= r(a^r b^s, a^i b^j, g) q(a^r b^s, a^i b^j)(w_{i,j} \cdot w_{r,s}) \cdot w_g \\ &= r(a^r b^s, a^i b^j, g) q(a^r b^s, a^i b^j) r(a^i b^j, a^r b^s, g)^{-1} w_{i,j} \cdot (w_{r,s} \cdot w_g) \\ &= q(a^r b^s, a^i b^j) T_{i,j} \circ T_{r,s}(w_g), \end{aligned} \tag{9.3}$$

since $r(a^r b^s, a^i b^j, g) = r(a^i b^j, a^r b^s, g)$.
In particular,

$$\begin{aligned} T_{0,1}(T_{r,s}(z_{i,j})) &= q(b, a^r b^s) T_{r,s}(T_{0,1}(z_{i,j})) = q(b, a^r b^s) T_{r,s}(e_{i,j} z_{i,j}) \\ &= q(b, a^r b^s) e_{i,j} T_{r,s}(z_{i,j}). \end{aligned}$$

Hence, $T_{r,s}(z_{i,j})$ is an eigenvector of $T_{0,1}$ associated to the eigenvalue $q(b, a^r b^s) e_{i,j}$. Since

$$T_{r,s}(z_{i,j}) = w_{r,s} \cdot \sum_{k=0}^{n-1} e_{i,j}^{-k} w_{i,k} = \sum_{k=0}^{n-1} e_{i,j}^{-k} C(a^r b^s, a^i b^k)) w_{[r+i],[s+k]}, \tag{9.4}$$

where $[\ ]$ denotes the equivalence class in $\mathbb{Z}_n$ or $\mathbb{Z}_m$, we deduce that

$$T_{r,s}(z_{i,j}) = \eta_{r,s}^{i,j} \cdot z_{[r+i],l}, \tag{9.5}$$

for some $l = 0, 1, \ldots, n-1$ and some $\eta_{r,s}^{i,j} \in K^*$. Also, since $q(b, a^r b^s) e_{i,j}$ is an eigenvalue associated to $T_{r,s}(z_{i,j})$ we see that

$$q(b, a^r b^s) e_{i,j} = e_{[r+i],l}. \tag{9.6}$$

By definition $e^n_{i,j} = \alpha_i$. Therefore,

$$q(b, a^r b^s)^n \alpha_i = \alpha_{[r+i]}. \tag{9.7}$$

It follows from the definition of a standard basis that $C(b, a^r b^s) = 1$, if $s \neq n-1$, and that $C(b, a^r b^{n-1}) = \alpha_r$. Therefore, from equation (9.7) we obtain $\alpha_r = C(a^r b^s, b)^{-n}$, $r = 1, 2, \ldots, m$, when $s \neq n-1$, and $\alpha_r^{n-1} = C(a^r b^{n-1}, b)^n$, $r = 1, 2, \ldots, m$. Hence, as $q(b, a^r b^s) = C(a^r b^s, b)^{-1}$, when $s \neq n-1$, by replacing $q(b, a^r b^s)$ in equation (9.7), we get $\alpha_r \alpha_i = \alpha_{[r+i]}$. From this we see that $\alpha_i = \alpha_1^i$. Finally, notice that $\alpha_i = C(a, b)^{-in}$. Since $\alpha_1^m = 1$, then $C(a, b)^{mn} = 1$.
We summarize below what we have obtained so far:

$$\begin{aligned}
\alpha_i &= \alpha_1^i, \\
\alpha_i &= C(a, b)^{-in}, \\
C(a^r b^s, b)^{-n} &= \alpha_r = (C(a, b)^{-r})^n, \quad \text{for } s \neq n-1, \\
C(a^r b^{n-1}, b)^n &= \alpha_r^{n-1} = (C(a, b)^{-r(n-1)})^n, \\
C(b^s, b)^n &= 1, \quad \text{(cyclic case)} \\
C(a^r, a)^m &= 1, \quad \text{(cyclic case)} \\
C(a, b)^{mn} &= 1.
\end{aligned} \tag{9.8}$$

On the other hand, by equation (9.6) it follows that

$$\eta^{i,j}_{r,s} \cdot Z_{[r+i],l} = \sum_{k=0}^{n-1} \eta^{i,j}_{r,s} \cdot e^{-k}_{[r+i],l} \cdot w_{[r+i],k} = \sum_{k=0}^{n-1} \eta^{i,j}_{r,s} \cdot q(b, a^r b^s)^{-k} \cdot e^{-k}_{i,j} \cdot w_{[r+i],k}.$$

Equations (9.4) and (9.5) imply the following identity:

$$\sum_{k=0}^{n-1} e^{-k}_{i,j} C(a^r b^s, a^i b^k) w_{[r+i],[s+k]} = \sum_{k=0}^{n-1} \eta^{i,j}_{r,s} \cdot q(b, a^r b^s)^{-k} \cdot e^{-k}_{i,j} \cdot w_{[r+i],k}.$$

But the last equation is equivalent to the following two equations:

$$\sum_{k=s}^{n-1} e^{-(k-s)}_{i,j} C(a^r b^s, a^i b^{k-s}) w_{[r+i],k} = \sum_{k=s}^{n-1} \eta^{i,j}_{r,s} \cdot q(b, a^r b^s)^{-k} \cdot e^{-k}_{i,j} \cdot w_{[r+i],k},$$

and

$$\sum_{k=0}^{s-1} e^{-(n+k-s)}_{i,j} C(a^r b^s, a^i b^{n+k-s}) w_{[r+i],k} = \sum_{k=0}^{s-1} \eta^{i,j}_{r,s} \cdot q(b, a^r b^s)^{-k} \cdot e^{-k}_{i,j} \cdot w_{[r+i],k} \quad \text{for} \quad s \neq 0.$$

Therefore, the equations

$$e^{-(k-s)}_{i,j} \cdot C(a^r b^s, a^i b^{k-s}) = \eta^{i,j}_{r,s} \cdot q(b, a^r b^s)^{-k} \cdot e^{-k}_{i,j} \text{ for } k = s, s+1, \ldots, n-1, \tag{9.9}$$

and

$$e_{i,j}^{-(n+k-s)} \cdot C(a^r b^s, a^i b^{n+k-s}) = \eta_{r,s}^{i,j} \cdot q(b, a^r b^s)^{-k} \cdot e_{i,j}^{-k} \text{ for } k = 0, 1, \ldots, s-1, \quad \text{for } s \neq 0 \quad (9.10)$$

hold.

From (9.9) if we let $k = s$, we deduce that $\eta_{r,s}^{i,j} = C(a^r b^s, a^i) \cdot q(b, a^r b^s)^s \cdot e_{i,j}^s$. Replacing the last equation in (9.9) and in (9.10) we get that:

$$C(a^r b^s, a^i b^l) = C(a^r b^s, a^i) \cdot C(b, a^r b^s)^{-l} \cdot C(a^r b^s, b)^l, \quad \text{if } \ 0 \leq l < n - s, \quad (9.11)$$

and

$$C(a^r b^s, a^i b^l) = C(a^r b^s, a^i) \cdot C(b, a^r b^s)^{n-l} \cdot C(a^r b^s, b)^{l-n} \cdot \alpha_i, \quad \text{if } \ n - s \leq l \leq n - 1; \quad s \neq 0. \quad (9.12)$$

Now we take in account the symmetry condition of r: $r(a, b, c) = r(b, a, c)$ for every $a, b, c \in G$. For any three general elements $a^r b^s, a^i b^k, a^j b^l \in G$ the symmetry condition looks like:

$$C(a^i b^k, a^j b^l) C(a^r b^s, a^{i+j} b^{k+l}) C(a^r b^s, a^i b^k)^{-1} = C(a^r b^s, a^j b^l) C(a^i b^k, a^{r+j} b^{s+l}) C(a^i b^k, a^r b^s)^{-1}. \quad (9.13)$$

Taking $k = 0$ and $l = 0$ in the above equation, and using the equation (9.11) and the fact that $C(a^i, a^j) = C(a^i, a)^j$ (cyclic case, see [26]) we obtain: $C(a^r b^s, a^{i+j}) = C(a^r b^s, a^i) C(a^r b^s, a^j)$. Then, recursively, we get $C(a^r b^s, a^j) = C(a^r b^s, a)^j$, and therefore $C(a^r b^s, a)^m = 1$. Also, notice that since $C(a^r b^s, b)^{-n} = \alpha_r$ when $s \neq n-1$ and $C(a^r b^{n-1}, b)^{-n} = \alpha_r^{1-n}$, we can rewrite equations (9.11) and (9.12) in the following manner:

$$\begin{aligned}
C(a^r b^s, a^i b^l) &= C(a^r b^s, a)^i C(a^r b^s, b)^l, \quad \text{for } \ 0 \leq l \leq n - s - 1, \\
C(a^r b^s, a^i b^l) &= C(a^r b^s, a)^i C(a^r b^s, b)^l \alpha_r \alpha_i, \quad \text{for } \ n - s \leq l \leq n - 1 \ \text{ and } \ s \neq n - 1, \\
C(a^r b^{n-1}, a^i b^l) &= C(a^r b^s, a)^i C(a^r b^s, b)^l \alpha_r^{1-l} \alpha_i.
\end{aligned}$$

We conclude that for a $(1,2)$-symmetric $\mathbb{Z}_m \times \mathbb{Z}_n$-graded twisted $\mathbb{C}$-algebra the structure constant

$C : G \times G \to A$ referred to a standard basis $\mathcal{B}$ must satisfy the following equations:

$$\begin{aligned}
C(a^r b^s, a^i b^l) &= C(a^r b^s, a)^i C(a^r b^s, b)^l, \quad \text{for } \ 0 \leq l \leq n-s-1, \\
C(a^r b^s, a^i b^l) &= C(a^r b^s, a)^i C(a^r b^s, b)^l \alpha_r \alpha_i, \quad \text{for } \ n-s \leq l \leq n-1 \ \text{ and } \ s \neq n-1, \ s \neq 0, \\
C(a^r b^{n-1}, a^i b^l) &= C(a^r b^{n-1}, a)^i C(a^r b^{n-1}, b)^l \alpha_r^{1-l} \alpha_i \ \text{ if } \ 1 \leq l \leq n-1, \\
C(a^r b^s, a)^m &= 1, \\
\alpha_i &= \alpha_1^i, \\
\alpha_i &= C(a,b)^{-in}, \\
C(a^r b^s, b)^{-n} &= \alpha_r = (C(a,b)^{-r})^n, \quad \text{for } s \neq n-1, \\
C(a^r b^{n-1}, b)^n &= \alpha_r^{n-1} = (C(a,b)^{-r(n-1)})^n, \\
C(b^s, b)^n &= 1, \quad \text{(cyclic case)} \\
C(a^r, a)^m &= 1, \quad \text{(cyclic case)} \\
C(a,b)^{mn} &= 1.
\end{aligned} \tag{9.14}$$

Now we prove that two $(1,2)$-symmetric G-graded twisted algebras W_1 and W_2 are graded-isomorphic if and only if their structure constants referred to standard bases are the same.

Theorem 4. *Let W_1 and W_2 be $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebras with standard bases $\mathcal{B}_1$ and $\mathcal{B}_2$, respectively, and associated structure constants $C_1, C_2 : G \times G \to A$. Then, W_1 is graded-isomorphic to W_2 if and only if $C_1 = C_2$.*

Proof. Suppose that W_1 is graded-isomorphic to W_2. By Corollary 3, $r_1 = r_2$ and $[C_1] = [C_2]$ in $H^2(G, A)$. If $[C_1] = [C_2]$, then there exists $\rho : G \to A$ such that $C_1 = \partial^1(\rho) C_2$. That is:

$$C_1(a^r b^s, a^i b^k) = \rho(a^i b^k) \rho(a^{r+i} b^{s+k})^{-1} \rho(a^r b^s) C_2(a^r b^s, a^i b^k). \tag{9.15}$$

Since the structure constants C_1, C_2 are referred to standard bases, the following equalities hold for $j = 1, 2$:

$$\begin{aligned}
C_j(1, a^i b^k) &= C_j(a^i b^k, 1) = 1, \text{ for all } i, k. \\
C_j(a, a^i) &= 1, \quad \text{for } \ i = 0, 1, \ldots, m-1. \\
C_j(b, a^i b^k) &= 1, \quad \text{for } \ i = 0, 1, \ldots, m-1, \quad k = 0, 1, \ldots, n-2. \\
C_j(b, a^i b^{n-1}) &= \alpha_{i,(j)}.
\end{aligned}$$

These identities together with equation (9.15) yield: $\rho(a^i) = \rho(a)^i$ for all $i = 0, 1, 2, \ldots, n-1$. In

particular, $\rho(1)=1$ and $\rho(a)^m=1$, and

$$\rho(a^ib^k)=\rho(a)^i\rho(b)^k \quad \text{for} \quad k\neq n.$$

Moreover, $\rho(b^i)=\rho(b)^i$ for $i=0,1,\ldots,n$, since

$$\begin{aligned} 1 &= C_1(b,b^i)=\rho(b^i)\rho(b^{i+1})^{-1}\rho(b)C_2(b,b^i) \\ &= \rho(b^i)\rho(b^{i+1})^{-1}\rho(b). \end{aligned}$$

Therefore, $\rho(b)^n=\rho(b^n)=1$. All this can be summarize by saying that $\rho: G\to A$ is a group homomorphism. It immediately follows $\partial^1(\rho)\equiv 1$ what implies that $C_1=C_2$.
The reciprocal is clear. □

Finally, we want to see that if $C: G\times G\to A$ is a function satisfying the identities stated in (9.14) then the vector space $\mathbb{C}^m\times\mathbb{C}^n$, endowed with the structure of a G-graded twisted algebra defined by the functions C (referred to the canonical basis of $\mathbb{C}^m\times\mathbb{C}^n$) is a $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebra.

Theorem 5. *Let $G=\mathbb{Z}_m\times\mathbb{Z}_n$ and let $A\subset\mathbb{C}^*$ be a finite subgroup. Suppose that we choose values in A for $C(a^rb^s,a)$ and $C(a^rb^s,b)$ satisfying the identities in (9.14). Then $W=\mathbb{C}^m\times\mathbb{C}^n$ with the multiplication given by C (referred to the canonical basis of $\mathbb{C}^m\times\mathbb{C}^n$) is a $(1,2)$-symmetric G-graded twisted $\mathbb{C}$- algebra.*

Proof. For $0\leq r,i\leq m-1$ and $0\leq s,l\leq n-1$ define

$$f(r,s,i,l)=\begin{cases} 1 & \text{if } 0\leq l\leq n-s-1 \\ \alpha_r\alpha_i & \text{if } n-s\leq l\leq n-1, \text{ and } s\neq n-1 \\ \alpha_r^{1-l}\alpha_i & \text{if } s=n-1,\ 1\leq l\leq n-1 \end{cases}$$

Therefore, by equation (9.14) we have

$$C(a^rb^s,a^ib^l)=C(a^rb^s,a)^iC(a^rb^s,b)^lf(r,s,i,l).$$

We know that $r(a^rb^s,a^ib^k,a^jb^l)=r(a^ib^k,a^rb^s,a^jb^l)$ if and only if

$$C(a^ib^k,a^jb^l)C(a^rb^s,a^{i+j}b^{k+l})C(a^rb^s,a^ib^k)^{-1}=C(a^rb^s,a^jb^l)C(a^ib^k,a^{r+j}b^{s+l})C(a^ib^k,a^rb^s)^{-1}$$

and therefore if and only if

$$\begin{aligned} &f(i,k,j,l)f(r,s,i+j,[k+l])f(r,s,i,k)^{-1}C(a^rb^s,b)^{[k+l]-(k+l)}= \\ &=f(r,s,j,l)f(i,k,r+j,[s+l])f(i,k,r,s)^{-1}C(a^ib^k,b)^{[s+l]-(s+l)}, \end{aligned} \tag{9.16}$$

where $[\ ]$ denotes the class module n.

In order to check the above equation, we have to consider several cases:

1) $[k+l]+s<n$ and $[s+l]+k<n$:

In this case we can rewrite (9.16) as:

$$f(i,k,j,l)f(r,s,i,k)^{-1}C(a^rb^s,b)^{[k+l]-(k+l)}=f(r,s,j,l)f(i,k,r,s)^{-1}C(a^ib^k,b)^{[s+l]-(s+l)}. \tag{9.17}$$

i) $k\neq n-1$ and $s\neq n-1$:

Notice that in this case we have $f(r,s,i,k)=f(i,k,r,s)$, hence (9.17) is equivalent to

$$f(i,k,j,l)C(a^rb^s,b)^{[k+l]-(k+l)}=f(r,s,j,l)C(a^ib^k,b)^{[s+l]-(s+l)}. \tag{9.18}$$

Now, suppose $k+l\geq n$. If $s+l<n$ then as $[s+l]+k<n$ and $[s+l]=s+l$, we have $s+l+k<n$ and therefore $k+l<n-s\leq n$. But also note that $s\neq 0$ since $s=0$ implies $[s+l]+k=l+k<n$, which is a contradiction. Hence, $k+l\geq n$ implies $s+l\geq n$.

In the same way, $s+l\geq n$ implies $k+l\geq n$.

Thus, we only have to check the cases $k+l\geq n$, $s+l\geq n$ and $k+l<n$, $s+l<n$.

In these two cases, the equation (9.18) is equivalent to $\alpha_i\alpha_j\alpha_r=\alpha_r\alpha_j\alpha_i$ and $1=1$ respectively.

ii) $k=n-1$:

If $s+l\geq n$ then $s\neq 0$ and $l\neq 0$; and as $[k+l]+s=[l-1]+s=l-1+s<n$ then $s+l<n+1$. Hence $s+l=n$.

As we saw above, $s+l\geq n$ implies $k+l\geq n$. Also, as $s\neq 0$ then $k+s=n-1+s\geq n$. Thus, the equation (9.17) is equivalent to

$$\alpha_i^{1-l}\alpha_j\alpha_r^{-1}\alpha_i^{-1}\alpha_r=\alpha_r\alpha_j\alpha_i^{s-1}\alpha_r^{-1}\alpha_i^{1-n}\quad\Leftrightarrow\quad\alpha_i^0=1$$

when $s\neq n-1$ and equivalent to

$$\alpha_i^{1-l}\alpha_j\alpha_r^{k-1}\alpha_i^{-1}\alpha_r^{1-n}=\alpha_r^{1-l}\alpha_j\alpha_i^{s-1}\alpha_r^{-1}\alpha_i^{1-n}\quad\Leftrightarrow\quad\alpha_r^0=\alpha_i^0$$

when $s=n-1$, since $s=n-1$ implies $l=1$.

If $s+l<n$ then as $[s+l]+k<n$ we have $s+l+n-1<n$ and therefore $s+l<1$. Hence $s=0$ and $l=0$. Hence equation (9.17) is equivalent to:

$$1=1.$$

iii) $s = n-1$:

This case is symmetric with the last case.

2) $[k+l]+s < n$ and $[s+l]+k \geq n$:

Notice that in this case, the cases $k+l<n,\ s+l<n,\ k+l\geq n,\ s+l\geq n$ and $s+l\geq n,\ k+l<n$ are not possible.

Therefore we only have to check the case $k+l\geq n,\ s+l<n$.

Notice that as $k+l\geq n$ then $l\geq 1$, and as $s+l<n$ then $s\neq n-1$.

i) $k\neq n-1$:

In this case $f(r,s,i,k)=f(i,k,r,s)$ and therefore the equation (9.16) is equivalent to

$$\alpha_i\alpha_j\alpha_r=\alpha_i\alpha_{r+j} \quad \Leftrightarrow \quad 1=1.$$

ii) $k=n-1$:

If $s\neq 0$ then $k+s=n-1+s\geq n$. Therefore equation (9.16) is equivalent to:

$$\alpha_i^{1-l}\alpha_j\alpha_r^{-1}\alpha_i^{-1}\alpha_r=\alpha_i^{1-[s+l]}\alpha_{r+j}\alpha_i^{s-1}\alpha_r^{-1} \quad \Leftrightarrow 1=1.$$

If $s=0$, then equation (9.16) is equivalent to:

$$\alpha_i^{1-l}\alpha_j\alpha_r=\alpha_i^{1-l}\alpha_{r+j} \quad \Leftrightarrow \quad 1=1.$$

3) $[k+l]+s\geq n$ and $[s+l]+k<n$:

This case is symmetric with the last case.

4) $[k+l]+s\geq n$ and $[s+l]+k\geq n$:

Notice that the cases $k+l\geq n,\ s+l<n$ and $k+l<n,\ s+l\geq n$ are not possible, since if for example $k+l\geq n$ and $s+l<n$, then as $[k+l]+s\geq n$ we have $k+l+s\geq 2n$, but $s+l<n$ implies $k+l+s<n+k\leq 2n-1$, which is a contradiction; and if $k+l<n$ and $s+l\geq n$, then as $[s+l]+k\geq n$ we have $k+l+s\geq 2n$, but $k+l<n$ implies $k+l+s<n+s\leq 2n-1$, which is a contradiction.

i) $k\neq n-1$ and $s\neq n-1$:

As $f(r,s,i,k)=f(i,k,r,s)$, equation (9.16) is equivalent to

$$f(i,k,j,l)f(r,s,i+j,[k+l])C(a^rb^s,b)^{[k+l]-(k+l)}=f(r,s,j,l)f(i,k,r+j,[s+l])C(a^ib^k,b)^{[s+l]-(s+l)} \tag{9.19}$$

If $k+l \geq n,\ s+l \geq n,$ then equation (9.19) is equivalent to

$$\alpha_i\alpha_j\alpha_r\alpha_{i+j}\alpha_r = \alpha_r\alpha_j\alpha_i\alpha_{r+j}\alpha_i \quad \Leftrightarrow \quad 1=1.$$

If $k+l < n,\ s+l < n$ then equation (9.19) is equivalent to

$$\alpha_r\alpha_{i+j} = \alpha_i\alpha_{r+j} \quad \Leftrightarrow \quad 1=1.$$

ii) $k = n-1$:

If $k+l \geq n,\ s+l \geq n$:

If $s = n-1$:

In this case the equation (9.16) is equivalent to

$$\alpha_i^{1-l}\alpha_j\alpha_r^{1-[k+l]}\alpha_{i+j}\alpha_r^{k-1}\alpha_i^{-1}\alpha_r^{1-n} = \alpha_r^{1-l}\alpha_j\alpha_i^{1-[s+l]}\alpha_{r+j}\alpha_i^{s-1}\alpha_r^{-1}\alpha_i^{1-n} \quad \Leftrightarrow \quad 1=1.$$

If $s \neq n-1$:

In this case the equation (9.16) is equivalent to

$$\alpha_i^{1-l}\alpha_j\alpha_r\alpha_{i+j}\alpha_r^{-1}\alpha_i^{-1}\alpha_r = \alpha_r\alpha_j\alpha_i^{1-[s+l]}\alpha_{r+j}\alpha_i^{s-1}\alpha_r^{-1}\alpha_i^{1-n} \quad \Leftrightarrow \quad 1=1.$$

If $k+l < n$ then as $k = n-1$ we have $l = 0$, and therefore $s+l = s < n$.

If $s \neq n-1,$ equation (9.16) is equivalent to

$$\alpha_r\alpha_{i+j}\alpha_r^{-1}\alpha_i^{-1} = \alpha_i^{1-s}\alpha_{r+j}\alpha_i^{s-1}\alpha_r^{-1} \quad \Leftrightarrow \quad 1=1.$$

If $s = n-1,$ then we have that equation (9.16) is equivalent to

$$\alpha_r^{1-k}\alpha_{i+j}\alpha_r^{k-1}\alpha_i^{-1} = \alpha_i^{1-s}\alpha_{r+j}\alpha_i^{s-1}\alpha_r^{-1} \quad \Leftrightarrow \quad 1=1.$$

We conclude that $W = \mathbb{C}^m \times \mathbb{C}^n$ with the multiplication given by C (referred to the canonical basis of $\mathbb{C}^m \times \mathbb{C}^n$) is a $(1,2)$-symmetric G-graded twisted $\mathbb{C}$- algebra. □

We are ready to state the main theorem of this section.

Theorem 6. *The number of (graded) isomorphism classes of $(1,2)$-symmetric $\mathbb{Z}_m \times \mathbb{Z}_n$-graded twisted $\mathbb{C}$-algebras with structure constants taking values in a finite subgroup $A \subset \mathbb{C}^*$ is given by:*

$$|R_m|^{mn-3}|R_n|^{mn-3}|R_{mn}|,$$

where R_k denotes the set of k-th roots of unity: $\{\omega \in A \ : \ \omega^k = 1\}$.

Proof. From the discussion above, a $(1,2)$-symmetric $\mathbb{Z}_m \times \mathbb{Z}_n$-graded twisted $\mathbb{C}$-algebra is determined, up to graded isomorphisms, by the structure constant that is defined with respect to a standard basis. In turn, this function is completely determined by all possible choices of $C(a^r b^s, a)$ and $C(a^r b^s, b)$, satisfying the identities in (9.14). As $C(a^r b^s, a)^m = 1$ for all $0 \leq r \leq m-1,\ 0 \leq s \leq n-1$, and

$$1 = C(1,a) = C(a,a) = C(b,a),$$

then we see that there are $|R_m|^{mn-3}$ possible choices for $C(a^r b^s, a)$. Similarly, as $C(b^s, b)^n = 1$ for $0 \leq s \leq n-1$, and $C(1,b) = 1 = C(b,b)$, then $C(b^s, b)$ may be chosen in $|R_n|^{n-2}$ possible ways. Since $C(a,b)^{mn} = 1$, there are $|R_{mn}|$ possible values for $C(a,b)$. In the case where $s \neq n-1$ and $r \neq 0$, the identities in (9.14) tell us that

$$C(a^r b^s, b)^n = C(a,b)^{rn} = (C(a,b)^r)^n.$$

Therefore, $C(a^r b^s, b) = \omega C(a,b)^r$, where ω is some fixed n-th root of unity. Thus, there are $|R_n|^{(n-1)(m-1)-1}$ possible choices for $C(a^r b^s, b)$, if $s \neq n-1$ and $r \neq 0$.

Finally, again by using (9.14) we obtain: $C(a^r b^{n-1}, b)^n = (C(a,b)^{-r(n-1)})^n$, and therefore $C(a^r b^{n-1}, b) = \omega C(a,b)^{-r(n-1)}$, where $\omega^n = 1$. Hence, if $r \geq 1$, the value of $C(a^r b^{n-1}, b)$ can be chosen in $|R_n|^{m-1}$ possible manners. In conclusion, the number of algebras satisfying the hypothesis of the theorem is given by

$$|R_m|^{mn-3}|R_n|^{n-2+(n-1)(m-1)-1+m-1}|R_{mn}| = |R_m|^{mn-3}|R_n|^{mn-3}|R_{mn}|.$$

□

Remark 8. If m and n are relatively prime, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$, and since $|R_{mn}| = |R_m||R_n|$, the above number is equal to $|R_{mn}|^{mn-2}$ which gives the correct number of non-isomorphic algebras in the cyclic case, as provided in [26].

Now, we discuss the general case of any finite abelian group, presented as $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

9.2 Classification of $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebra, for G any finite abelian group

First, we start by defining a generalized standard basis for a G-graded twisted algebra W. We proceed by induction on the number of factors. Suppose $G = G_1 \times \mathbb{Z}_{n_k}$, where $G_1 = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{k-1}}$. Fix $a_i \in \mathbb{Z}_{n_i}$ a generator. We define a standard basis for W as a basis of the form $\{w_{g,j}\}$, where

$w_{e,j} = w_{a_k}^{(j)}$ (e denotes the identity element of G_1), as it was defined in the cyclic case, and where $\{w_{g,0} = w_g \ : \ g \in G_1\}$ is a standard basis for W restricted to G_1, and $w_{g,j} = w_{a_k}^{(1)} \cdot w_{g,j-1}$, for $g \neq e$ and $j \neq 0$. So for each $g \in G_1$ there is $\alpha_g \in A$ such that $w_{a_k}^{(1)} \cdot w_{g,n_k-1} = \alpha_g \cdot w_g$.

Remark 9. Notice that since $\mathcal{B}$ was defined recursively, its restriction to $H = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$ with $1 \leq t \leq k$, is a standard basis for $W|_H$.

Let W be a $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebra, with standard basis $\mathcal{B}$ and structure constant $C : G \times G \to A$. Consider as before $T_{a_k} : W \to W$ the linear transformation given by $T_{a_k}(x) = w_{a_k} \cdot x$. For each $g \in G_1$, let $\{e_{g,j}\}$ denotes the set of n_k-th roots of α_g. Notice that $\alpha_e = 1$ and therefore $\{e_{e,j}\}$ is the set of n_k-roots of unity. Define

$$z_{g,j} = \sum_{\mu=0}^{n_k-1} e_{g,j}^{-\mu} w_{g,\mu}. \tag{9.20}$$

Similarly as in (9.2), we can see that $z_{g,j}$ is an eigenvector of T_{a_k} associated to the eigenvalue $e_{g,j}$. Also, since W is $(1,2)$-symmetric, following the same argument described in (9.3) we see that

$$T_{a_k}(T_{g',s}(z_{g,j})) = q(a_k, g' \cdot a_k^s) \cdot e_{g,j} \cdot T_{g',s}(z_{g,j}).$$

Therefore $T_{g',s}(z_{g,j})$ is an eigenvector of T_{a_k} associated to the eigenvalue $q(a_k, g' \cdot a_k^s) \cdot e_{g,j}$. Here, $T_{g',s}$ denotes the linear transformation given by $T_{g',s}(x) = w_{g',s} \cdot x$. Since

$$T_{g',s}(z_{g,j}) = \sum_{\mu=0}^{n_k-1} e_{g,j}^{-\mu} \cdot C(g' \cdot a_k^s, g \cdot a_k^\mu) \cdot w_{g'g,[s+\mu]} \tag{9.21}$$

where $[\ ]$ denotes residue classes in $\mathbb{Z}_{n_k}$, then it holds that

$$T_{g',s}(z_{g,j}) = \eta_{g',s}^{g,j} \cdot z_{g'g,l}, \quad \text{for some} \ \ 0 \leq l \leq n_k - 1. \tag{9.22}$$

Hence,

$$q(a_k, g' \cdot a_k^s) \cdot e_{g,j} = e_{g'g,l}. \tag{9.23}$$

This last equation is the generalization of equation (9.6). As in that case, we may derive the following identities: If $g = a_1^{r_1} a_2^{r_2} \ldots a_{k-1}^{r_{k-1}}$, then

$$\begin{aligned}
\alpha_g &= C(a_1, a_k)^{-r_1 n_k} \cdots C(a_{k-1}, a_k)^{-r_{k-1} n_k} \\
\alpha_{a_i} &= C(a_i, a_k)^{-n_k} \\
C(a_k, g \cdot a_k^{n_k-1}) &= \alpha_g = C(g, a_k)^{-n_k} \\
C(g \cdot a_k^s, a_k) &= \omega_{g,s} \cdot C(a_1, a_k)^{r_1} \cdots C(a_{k-1}, a_k)^{r_{k-1}}, \quad \text{for} \ \ s \neq n_k - 1, \quad \text{where} \ \ \omega_{g,s}^{n_k} = 1 \\
C(g \cdot a_k^{n_k-1}, a_k) &= \omega_g \cdot C(a_1, a_k)^{-r_1(n_k-1)} \cdots C(a_{k-1}, a_k)^{-r_{k-1}(n_k-1)} \quad \text{where} \ \ \omega_g^{n_k} = 1 \\
C(a_i, a_k)^{n_i n_k} &= 1.
\end{aligned} \tag{9.24}$$

Now, equations (9.21), (9.22) and (9.23) imply:

$$\begin{aligned}\sum_{\mu=0}^{n_k-1} e_{g,j}^{-\mu}\cdot C(g'\cdot a_k^s, g\cdot a_k^\mu)\cdot w_{g'g,[s+\mu]} &= \eta_{g',s}^{g,j}\cdot z_{g'g,l}\\ &= \sum_{\mu=0}^{n_k-1}\eta_{g',s}^{g,j}\cdot e_{g'g,l}^{-\mu}\cdot w_{g'g,\mu}\\ &= \sum_{\mu=0}^{n_k-1}\eta_{g',s}^{g,j}\cdot q(a_k, g'\cdot a_k^s)^{-\mu}\cdot e_{g,j}^{-\mu}\cdot w_{g'g,\mu}\end{aligned}$$

Similarly, as in the case of a product of two cyclic groups, the last equation implies that for every $g, g'\in G_1$,

$$\begin{aligned}C(g'\cdot a_k^s, g\cdot a_k^l) &= C(g'\cdot a_k^s, g)\cdot C(g'\cdot a_k^s, a_k)^l, \quad \text{if } \ 0\le l<n_k-s.\\ C(g'\cdot a_k^s, g\cdot a_k^l) &= C(g'\cdot a_k^s, g)\cdot C(g'\cdot a_k^s, a_k)^{l-n_k}\cdot\alpha_g, \quad \text{if } \ n_k-s\le l\le n_k-1; \quad s\neq 0, \quad s\neq n_k-1.\\ C(g'\cdot a_k^{n_k-1}, g\cdot a_k^l) &= C(g'\cdot a_k^{n_k-1}, g)\cdot C(g'\cdot a_k^{n_k-1}, a_k)^{l-n_k}\cdot\alpha_{g'}^{n_k-l}\cdot\alpha_g.\end{aligned} \tag{9.25}$$

That proves the following theorem:

Theorem 7. *Suppose that $G=\mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2}\times\cdots\times\mathbb{Z}_{n_k}$, and fix generators $a_1,a_2,\ldots,a_k$, $a_i\in\mathbb{Z}_{n_i}$. Suppose that W is a $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebra. If $\mathcal{B}$ is a standard basis for W with structure constant $C: G\times G\to\mathbb{C}^*$, then:*

If $\ 0\le l<n_k-s$:

$C(g'\cdot a_k^s, g\cdot a_k^l) = C(g'\cdot a_k^s, g)\cdot C(g'\cdot a_k^s, a_k)^l,$

If $\ n_k-s\le l\le n_k-1, \quad s\neq 0, \quad s\neq n_k-1$:

$C(g'\cdot a_k^s, g\cdot a_k^l) = C(g'\cdot a_k^s, g)\cdot C(g'\cdot a_k^s, a_k)^{l-n_k}\cdot\alpha_g.$

For $s=n_k-1$:

$C(g'\cdot a_k^{n_k-1}, g\cdot a_k^l) = C(g'\cdot a_k^{n_k-1}, g)\cdot C(g'\cdot a_k^{n_k-1}, a_k)^{l-n_k}\cdot\alpha_{g'}^{n_k-l}\cdot\alpha_g.$

If the element g is written as $g=a_1^{r_1}a_2^{r_2}\ldots a_{k-1}^{r_{k-1}}$ then:

$\alpha_g = C(a_1, a_k)^{-r_1 n_k} \cdots C(a_{k-1}, a_k)^{-r_{k-1} n_k}$
$\alpha_{a_i} = C(a_i, a_k)^{-n_k}$,
$C(a_k, g \cdot a_k^{n_k - 1}) = \alpha_g = C(g, a_k)^{-n_k}$.

For $s \neq n_k - 1$, *where* $\omega_{g,s}^{n_k} = 1$:

$C(g \cdot a_k^s, a_k) = \omega_{g,s} \cdot C(a_1, a_k)^{r_1} \cdots C(a_{k-1}, a_k)^{r_{k-1}}$,
$C(g \cdot a_k^{n_k - 1}, a_k) = \omega_g \cdot C(a_1, a_k)^{-r_1(n_k-1)} \cdots C(a_{k-1}, a_k)^{-r_{k-1}(n_k-1)}$
$C(a_i, a_k)^{n_i n_k} = 1$.

As in the case of a product of two factors, the $(1,2)$-symmetry provides some extra information about the structure constant C that we summarize in the following two lemmas.

Lemma 3. *Suppose that* $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$, *and fix generators* $a_1, a_2, \ldots, a_k$, $a_i \in \mathbb{Z}_{n_i}$. *Suppose that* W *is a* $(1,2)$*-symmetric* G*-graded twisted* $\mathbb{C}$*-algebra. Then if* $\mathcal{B}$ *is a standard basis for* W *with structure constant* $C : G \times G \to \mathbb{C}$, *then:*

$$C(g_1 \cdot a_k^s, g_2 g_3) = C(g_1 \cdot a_k^s, g_2) \cdot C(g_1 \cdot a_k^s, g_3) \cdot C(g_2, g_3)^{-1} \cdot C(g_2, g_1 g_3) \cdot C(g_2, g_1)^{-1}$$

for every $g_1, g_2, g_3 \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_{k-1}}$.
Furthermore, if $g = a_1^{r_1} \cdots a_i^{r_i} \cdots a_{k-1}^{r_{k-1}}$ *and we denote* $\widetilde{g} = a_1^{r_1} \cdots a_{i-1}^{r_{i-1}}$, *then*

$$C(g \cdot a_k^s, a_i^j) = C(g \cdot a_k^s, a_i)^j \cdot C(a_i, \widetilde{g} \cdot a_i^{r_i})^{-(j-1)} \cdot C(a_i, \widetilde{g} \cdot a_i^{r_i+1}) \cdots C(a_i, \widetilde{g} \cdot a_i^{r_i+j-1}).$$

Hence,

$$C(g \cdot a_k^s, a_i^j) = C(g \cdot a_k^s, a_i)^j \cdot C(\widetilde{g}, a_i)^{(j-1)n_i} \quad \text{if } r_i = n_i - 1,$$

and if $r_i \neq n_i - 1$, *then*

$$C(g \cdot a_k^s, a_i^j) = C(g \cdot a_k^s, a_i)^j \cdot C(\widetilde{g}, a_i)^{-n_i} \quad \text{or } C(g \cdot a_k^s, a_i^j) = C(g \cdot a_k^s, a_i)^j.$$

In particular,

$$C(g \cdot a_k^s, a_i)^{n_i} = C(a_i, \widetilde{g} \cdot a_i^{r_i})^{n_i - 1} \cdot C(a_i, \widetilde{g} \cdot a_i^{r_i+1})^{-1} \cdots C(a_i, \widetilde{g} \cdot a_i^{r_i+n_i-1})^{-1}.$$

Therefore,

$$C(g \cdot a_k^s, a_i)^{n_i} = (C(\widetilde{g}, a_i)^{-(n_i-1)})^{n_i} \quad \text{if } r_i = n_i - 1,$$
$$C(g \cdot a_k^s, a_i)^{n_i} = C(\widetilde{g}, a_i)^{n_i} \quad \text{if } r_i \neq n_i - 1.$$

Proof. Remember that $r(g_1 \cdot a_k^s, g_2 \cdot a_k^j, g_3 \cdot a_k^v) = r(g_2 \cdot a_k^j, g_1 \cdot a_k^s, g_3 \cdot a_k^v)$ is equivalent to:

$$C(g_2{\cdot}a_k^j, g_3{\cdot}a_k^v)C(g_1{\cdot}a_k^s, g_2g_3{\cdot}a_k^{j+v})C(g_1{\cdot}a_k^s, g_2{\cdot}a_k^j)^{-1} = C(g_1{\cdot}a_k^s, g_3{\cdot}a_k^v)C(g_2{\cdot}a_k^j, g_1g_3{\cdot}a_k^{s+v})C(g_2{\cdot}a_k^j, g_1{\cdot}a_k^s)^{-1}.$$

Now, with $j = 0 = v$ in the last equation we obtain:

$$C(g_2, g_3)C(g_1 \cdot a_k^s, g_2g_3)C(g_1 \cdot a_k^s, g_2)^{-1} = C(g_1 \cdot a_k^s, g_3)C(g_2, g_1g_3 \cdot a_k^s)C(g_2, g_1 \cdot a_k^s)^{-1},$$

and therefore

$$C(g_1 \cdot a_k^s, g_2g_3) = C(g_1 \cdot a_k^s, g_2) \cdot C(g_1 \cdot a_k^s, g_3) \cdot C(g_2, g_3)^{-1} \cdot C(g_2, g_1g_3 \cdot a_k^s) \cdot C(g_2, g_1 \cdot a_k^s)^{-1}.$$

By the first equation in (9.25) we have that $C(g_2, g_1g_3{\cdot}a_k^s) = C(g_2, g_1g_3){\cdot}C(g_2, a_k)^s$, and $C(g_2, g_1{\cdot}a_k^s) = C(g_2, g_1) \cdot C(g_2, a_k)^s$, thus we have:

$$C(g_1 \cdot a_k^s, g_2g_3) = C(g_1 \cdot a_k^s, g_2) \cdot C(g_1 \cdot a_k^s, g_3) \cdot C(g_2, g_3)^{-1} \cdot C(g_2, g_1g_3) \cdot C(g_2, g_1)^{-1}.$$

This proves the first part of the lemma.

In order to prove the second part, notice that if we take $g_2 = a_i = g_3$, for $i = 1, 2, \ldots, k-1$, then we obtain:

$$C(g \cdot a_k^s, a_i^2) = C(g \cdot a_k^s, a_i)^2 \cdot C(a_i, g \cdot a_i) \cdot C(a_i, g)^{-1},$$

since $C(a_i, a_i) = 1$.

Therefore, recursively and using the fact that $C(a_i, a_i^j) = 1$, we get:

$$C(g \cdot a_k^s, a_i^j) = C(g \cdot a_k^s, a_i)^j \cdot C(a_i, g)^{-(j-1)} \cdot C(a_i, g \cdot a_i) \cdot C(a_i, g \cdot a_i^2) \cdots C(a_i, g \cdot a_i^{j-1}). \quad (9.26)$$

Thus, if $g = a_1^{r_1} \cdots a_i^{r_i} \cdots a_{k-1}^{r_{k-1}}$ and $\widetilde{g} = a_1^{r_1} \cdots a_{i-1}^{r_{i-1}}$, then using the first equation in Theorem 7, we have

$$\begin{aligned}
C(a_i, g \cdot a_i^l) &= C(a_i, a_1^{r_1} \cdots a_i^{r_i+l} \cdots a_{k-1}^{r_{k-1}}) \\
&= C(a_i, a_1^{r_1} \cdots a_i^{r_i+l} \cdots a_{k-2}^{r_{k-2}}) \cdot C(a_i, a_{k-1})^{r_{k-1}} \\
&= C(a_i, a_1^{r_1} \cdots a_{i-1}^{r_{i-1}} a_i^{r_i+l}) \cdot C(a_i, a_{i+1})^{r_{i+1}} \cdot C(a_i, a_{i+2})^{r_{i+2}} \cdots C(a_i, a_{k-1})^{r_{k-1}} \\
&= C(a_i, \widetilde{g} \cdot a_i^{r_i+l}) \cdot C(a_i, a_{i+1})^{r_{i+1}} \cdot C(a_i, a_{i+2})^{r_{i+2}} \cdots C(a_i, a_{k-1})^{r_{k-1}} \\
&= C(a_i, \widetilde{g} \cdot a_i^{r_i+l}) \cdot M
\end{aligned}$$

where $M = C(a_i, a_{i+1}) \cdot C(a_i, a_{i+2})^{r_{i+2}} \cdots C(a_i, a_{k-1})^{r_{k-1}}$.

Therefore, replacing in (9.26) we get:

$$\begin{aligned}
C(g \cdot a_k^s, a_i^j) &= C(g \cdot a_k^s, a_i)^j \cdot C(a_i, \widetilde{g} \cdot a_i^{r_i})^{-(j-1)} \cdot M^{-(j-1)} \cdot C(a_i, \widetilde{g} \cdot a_i^{r_i+1}) \cdot M \cdots C(a_i, \widetilde{g} \cdot a_i^{r_i+j-1}) \cdot M \\
&= C(g \cdot a_k^s, a_i)^j \cdot C(a_i, \widetilde{g} \cdot a_i^{r_i})^{-(j-1)} \cdot C(a_i, \widetilde{g} \cdot a_i^{r_i+1}) \cdots C(a_i, \widetilde{g} \cdot a_i^{r_i+j-1}) \cdot M^{-(j-1)} \cdot M^{j-1} \\
&= C(g \cdot a_k^s, a_i)^j \cdot C(a_i, \widetilde{g} \cdot a_i^{r_i})^{-(j-1)} \cdot C(a_i, \widetilde{g} \cdot a_i^{r_i+1}) \cdots C(a_i, \widetilde{g} \cdot a_i^{r_i+j-1})
\end{aligned}$$

Now, if $r_i = n_i - 1$ then $r_i + j \neq n_i - 1$ in $\mathbb{Z}_{n_i}$ for $j = 1, 2, \ldots, n_i - 1$. Therefore $C(a_i, \widetilde{g} \cdot a_i^l) = 1$ for every $l = 1, 2, \ldots, n_i - 1$. But from Theorem 7, $C(a_i, \widetilde{g} \cdot a_i^{n_i - 1}) = C(\widetilde{g}, a_i)^{-n_i}$, hence,

$$C(g \cdot a_k^s, a_i^j) = C(g \cdot a_k^s, a_i)^j \cdot C(\widetilde{g}, a_i)^{(j-1)n_i}, \quad \text{if } r_i = n_i - 1.$$

If $r_i \neq n_i - 1$, two things can occur:

1. There is a unique $l \in \{1, 2, \ldots, j-1\}$ such that $r_i + l = n_i - 1$ in $\mathbb{Z}_{n_i}$:
   In this case $C(a_i, \widetilde{g} \cdot a_i^{r_i + t}) = 1$ for every $t \neq l$, and $C(a_i, \widetilde{g} \cdot a_i^{r_i + l}) = C(\widetilde{g}, a_i)^{-n_i}$. Therefore,

$$C(g \cdot a_k^s, a_i^j) = C(g \cdot a_k^s, a_i)^j \cdot C(\widetilde{g}, a_i)^{-n_i}.$$

2. $r_i + l \neq n_i - 1$ in $\mathbb{Z}_{n_i}$ for every $l = 0, 1, 2, \ldots, j-1$:
   In this case $C(a_i, \widetilde{g} \cdot a_i^{r_i + l}) = 1$ for $l = 0, 1, 2, \ldots, j-1$. Therefore,

$$C(g \cdot a_k^s, a_i^j) = C(g \cdot a_k^s, a_i)^j.$$

Finally, with $j = n_i$, it is not difficult to see that:

$$C(g \cdot a_k^s, a_i)^{n_i} = (C(\widetilde{g}, a_i)^{-(n_i - 1)})^{n_i}, \quad \text{if } r_i = n_i - 1,$$

and

$$C(g \cdot a_k^s, a_i)^{n_i} = C(\widetilde{g}, a_i)^{n_i}, \quad \text{if } r_i \neq n_i - 1.$$

□

Lemma 4. *Suppose that $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, and fix generators $a_1, a_2, \ldots, a_k$, $a_i \in \mathbb{Z}_{n_i}$. Suppose that W is a $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebra. Then the constants $C(g \cdot a_k^s, g')$ always can be expressed in terms of the constants $C(g \cdot a_k^s, a_i)$, $1 \leq i \leq k-1$ and $C(a_j, a_t)$, $1 \leq j, t \leq k-1$, for every $g, g' \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_{k-1}}$.*

Proof. Suppose that $g' = a_1^{r_1} a_2^{r_2} \cdots a_{k-1}^{r_{k-1}}$.
We argue by induction on $n = r_1 + r_2 + \cdots + r_{k-1}$.
If $n = 1$, then $g' = a_i$ for some $i = 1, 2, \ldots, k-1$, and in this case the lemma is trivial.
Suppose that the result is true for n, and let us see that it is true when $r_1 + \cdots + r_{k-1} = n + 1$.
Indeed, $C(g \cdot a_k^s, g') = C(g \cdot a_k^s, a_1^{r_1} \cdots a_{k-1}^{r_{k-1}})$. Now, assume that $r_i \geq 1$, and $r_j = 0$ for $j < i$, thus we can write

$$C(g \cdot a_k^s, g') = C(g \cdot a_k^s, a_i \cdot (a_i^{r_i - 1} \cdots a_{k-1}^{r_{k-1}})).$$

By Lemma 3, we have that

$$C(g\cdot a_k^s, a_i\cdot(a_i^{r_i-1}\cdots a_{k-1}^{r_{k-1}})) =$$
$$C(g\cdot a_k^s, a_i)\cdot C(g\cdot a_k^s, a_i^{r_i-1}\cdots a_{k-1}^{r_{k-1}})\cdot C(a_i, a_i^{r_1-1}\cdots a_{k-1}^{r_{k-1}})^{-1}\cdot C(a_i, g\cdot a_i^{r_i-1}\cdots a_{k-1}^{r_{k-1}})\cdot C(a_i,g)^{-1}.$$

Now, the Theorem 7, allows us to compute:

$$C(a_i, a_1^{t_1}a_2^{t_2}\cdots a_{k-1}^{t_{k-1}}) = C(a_i, a_1^{t_1}\cdots a_i^{t_i})\cdot C(a_i,a_{i+1})^{t_{i+1}}\cdots C(a_i,a_{k-1})^{t_{k-1}},$$

and again by Theorem 7,

$$C(a_i, a_1^{t_1}\cdots a_{i-1}^{t_{i-1}}a_i^{t_i}) = \begin{cases} 1 & \text{if } t_i \neq n_i-1 \\ C(a_1,a_i)^{-t_1n_i}\cdots C(a_{i-1},a_i)^{-t_{i-1}n_i} & \text{if } t_i = n_i-1 \end{cases}$$

Hence, $C(a_i, a_i^{r_1-1}\cdots a_{k-1}^{r_{k-1}})$, $C(a_i, g\cdot a_i^{r_i-1}\cdots a_{k-1}^{r_{k-1}})$, $C(a_i,g)^{-1}$ can be written as a combination of terms of the form $C(a_t,a_j)$ with $1\leq t,j\leq k-1$; and by the inductive hypothesis, $C(g\cdot a_k^s, a_i^{r_i-1}\cdots a_{k-1}^{r_{k-1}})$ is a combination of terms of the form $C(g\cdot a_k^s, a_l)$ with $1\leq l\leq k-1$, and $C(a_t,a_j)$ with $1\leq t,j\leq k-1$, what completes the proof. □

The following theorem summarizes the above discussion:

Theorem 8. *Let G be presented as $\mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2}\times\cdots\times\mathbb{Z}_{n_k}$, and fix generators $a_1,a_2,\ldots,a_k$, $a_i\in\mathbb{Z}_{n_i}$. Suppose that W is a $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebra. If $\mathcal{B}$ is a standard basis for W with structure constant $C: G\times G\to\mathbb{C}^*$, then the values of $C(g\cdot a_k^s, a_i), C(g\cdot a_k^s, a_k)$ and $C(a_t,a_j)$, with $1\leq i,t,j\leq k-1$, $g\in G_1=\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_{k-1}}$ completely determine the structure constant C. Furthermore, the following identities generalize the ones obtained in (9.14):*

If $0\leq l<n_k-s$, then

$$C(g\cdot a_k^s, g'\cdot a_k^l) = C(g\cdot a_k^s, g')\cdot C(g\cdot a_k^s, a_k)^l.$$

If $n_k-s\leq l\leq n_k-1$, $s\neq 0$, $s\neq n_k-1$, then

$$C(g\cdot a_k^s, g'\cdot a_k^l) = C(g\cdot a_k^s, g')\cdot C(g\cdot a_k^s, a_k)^{l-n_k}\cdot\alpha_{g'}.$$

If $s=n_k-1$ then

$C(g \cdot a_k^{n_k-1}, g' \cdot a_k^l) = C(g \cdot a_k^{n_k-1}, g') \cdot C(g \cdot a_k^{n_k-1}, a_k)^{l-n_k} \cdot \alpha_g^{n_k-l} \cdot \alpha_{g'}$.

If g is written as $g = a_1^{r_1} a_2^{r_2} \dots a_{k-1}^{r_{k-1}}$ then

$\alpha_g = C(a_1, a_k)^{-r_1 n_k} \cdots C(a_{k-1}, a_k)^{-r_{k-1} n_k}$
$\alpha_{a_i} = C(a_i, a_k)^{-n_k}$
$C(a_i, a_k)^{n_i n_k} = 1.$
$C(a_k, g \cdot a_k^{n_k-1}) = \alpha_g = C(g, a_k)^{-n_k}$
$C(g \cdot a_k^{n_k-1}, a_k) = \omega_g \cdot C(a_1, a_k)^{-r_1(n_k-1)} \cdots C(a_{k-1}, a_k)^{-r_{k-1}(n_k-1)}$, *where* $\omega_g^{n_k} = 1$.

For the case where $s \neq 0$ *and* $g \neq a_j$, *for* $j = 1, 2, \dots, k$:

$C(g \cdot a_k^s, a_k) = \omega_{g,s} \cdot C(a_1, a_k)^{r_1} \cdots C(a_{k-1}, a_k)^{r_{k-1}}$, *for* $s \neq n_k - 1$, *where* $\omega_{g,s}^{n_k} = 1$.

For the case $s \neq 0$ *and* $g \neq a_j$ *for* $j = 1, 2, \dots, k-1$, *and* $i = 1, 2, \dots, k-1$ *we have*:

$C(g \cdot a_k^s, a_i) = \omega_{g,s} C(a_1, a_i)^{r_1} \cdots C(a_{i-1}, a_i)^{r_{i-1}}$ *if* $r_i \neq n_i - 1$, *where* $\omega_{g,s}^{n_i} = 1$.
$C(g \cdot a_k^s, a_i) = \omega_{g,s} \cdot (C(a_1, a_i)^{r_1} \cdots C(a_{i-1}, a_i)^{r_{i-1}})^{-(n_i-1)}$, *if* $r_i = n_i - 1$, *where* $\omega_{g,s}^{n_i} = 1$.

Before starting our next theorem we notice that as in Theorem 4, two $(1,2)$-symmetric $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$-graded twisted algebras are graded-isomorphic if and only if they have the same structure constants in their respective standard bases.

Lemma 5. *Let* $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ *and suppose that we have two* $(1,2)$*-symmetric* G*-graded twisted* $\mathbb{C}$*-algebras* W_1 *and* W_2 *with fixed standard bases and structure constants* $C_1, C_2 : G \times G \to A$, $A \subset \mathbb{C}^*$ *finite subgroup. Then,* W_1 *is isomorphic to* W_2 *as graded algebras, if and only if* $C_1 = C_2$.

Proof. Clearly, if $C_1 = C_2$ then W_1 is isomorphic to W_2 as graded algebras.
Now let us see that if $W_1 \cong W_2$ as graded algebras, then $C_1 = C_2$.
We argue by induction on $n = k$.
If $k = 1$, $G = \mathbb{Z}_{n_1}$ is a cyclic group, and the result follows from [26].
Assume that the result holds for $n < k$.
Now, if W_1 is isomorphic to W_2 as graded algebras, then $r_1 = r_2$ and $[C_1 \cdot C_2^{-1}] =$

[1] in $H^2(G,A)$.

Therefore, there exists $\rho : G \to A$ such that $C_1 \cdot C_2^{-1} = \partial^1(\rho)$. Remember that $\partial^1\rho(g\cdot a_k^s, g'\cdot a_k^l) = \rho(g'\cdot a_k^l)\rho(gg'\cdot a_k^{s+l})^{-1}\rho(g\cdot a_k^s)$, where $g, g' \in G_1 = \mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_{k-1}}$, and a_i is a generator of $\mathbb{Z}_{n_i}$. Furthermore, the function ρ is given by the isomorphism φ.

Hence

$$C_1(g\cdot a_k^s, g'\cdot a_k^l) = \rho(g'\cdot a_k^l)\rho(gg'\cdot a_k^{s+l})^{-1}\rho(g\cdot a_k^s)C_2(g\cdot a_k^s, g'\cdot a_k^l). \tag{9.27}$$

By the inductive hypothesis, as $W_1|_{G_1}$ is isomorphic to $W_2|_{G_1}$ as graded algebras, then $C_1|_{G_1\times G_1} = C_2|_{G_1\times G_1}$, and hence, $\rho|_{G_1}$ is a group homomorphism, thus

$$\rho(gg') = \rho(g)\rho(g').$$

On the other hand, from the way we define the standard bases, we can deduce the following properties in terms of the structure constants C_1 and C_2: for $j = 1, 2$

$$C_j(1, g\cdot a_k^s) = 1 = C_j(g\cdot a_k^s, 1)$$

$$C_j(a_i, a_i^j) = 1, \quad \text{for } i = 1, 2, \ldots, k$$

$$C_j(a_k, g\cdot a_k^s) = 1, \quad \text{for } s \neq n_k - 1.$$

Thus, as $C_j(a_k, g\cdot a_k^s) = 1$ for $s \neq n-k-1$, then using equation (9.27) we have

$$\rho(g\cdot a_k^s) = \rho(a_k)\cdot\rho(g\cdot a_k^{s-1}) \text{ for } s \neq n_k,$$

and recursively we get:

$$\rho(g\cdot a_k^s) = \rho(a_k)^s\cdot\rho(g), \quad \text{for } s \neq n_k.$$

Now, using that $C_j(a_k, a_k^j) = 1$ and equation (9.27) we have

$$\rho(a_k^j) = \rho(a_k)^j.$$

In particular, $\rho(a_k)^{n_k} = 1$.

Hence,

$$\rho(g\cdot a_k^s) = \rho(a_k)^s\cdot\rho(g), \quad \text{for every } s.$$

Finally, notice that the above implies that ρ is a group homomorphism, since

$$\begin{aligned}\rho(g\cdot a_k^s, g'\cdot a_k^l) &= \rho(gg'\cdot a_k^{s+l}) = \rho(a_k)^{s+l}\cdot\rho(gg')\\ &= \rho(a_k)^s\cdot\rho(g)\cdot\rho(a_k)^l\cdot\rho(g')\\ &= \rho(g\cdot a_k^s)\cdot\rho(g'\cdot a_k^l).\end{aligned}$$

As $\rho : G \to A$ is a group homomorphism, then by equation (9.27) we conclude that $C_1 = C_2$. □

The following theorem generalizes Theorem 5 when G is a product of an arbitrary number of cyclic groups. Its proof follows the same lines as the proof of Theorem 5 and will be omitted.

Theorem 9. *Let $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ and let $A \subset \mathbb{C}^*$ be a finite subgroup. Suppose that we choose values in A for $C(g \cdot a_k^s, a_k)$, $C(a_i, a_j)$ and $C(g \cdot a_k^s, a_i)$ satisfying the identities in Theorem 8. Then $W = \mathbb{C}^{n_1} \times \cdots \times \mathbb{C}^{n_k}$ with the multiplication given by C (referred to the canonical basis of $\mathbb{C}^{n_1} \times \cdots \times \mathbb{C}^{n_k}$) is a $(1,2)$-symmetric G-graded twisted $\mathbb{C}$- algebra.*

Finally, we may state our main theorem:

Theorem 10. *The number of non-(graded) isomorphic $(1,2)$-symmetric $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$-graded twisted $\mathbb{C}$-algebras with structure constants taking values in a finite subgroup $A \subset \mathbb{C}^*$ is given by the product:*

$$\prod_{i=1}^{k} |R_{n_i}|^{|G|-(k+1)} \prod_{1 \le i < j \le k} |R_{n_i n_j}|,$$

where R_{n_i} denotes the set $\{\omega \in A \ : \ \omega^{n_i} = 1\}$.

Proof. With the same notation, $G_1 = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{k-1}}$ and a_i is a generator of $\mathbb{Z}_{n_i}$.
After all the above discussion, we know that in order to produce this kind of algebras in an standard basis, we only have to give a table with the values $C(g \cdot a_k^s, a_k)$, $C(a_i, a_j)$ with $1 \le i < j \le k$ and $C(g \cdot a_k^s, a_i)$ with $1 \le i \le k-1$, satisfying the equations in Theorem 8.
As $C(a_i, a_j)^{n_i n_j} = 1$ for every $1 \le i < j \le k$, we have

$$\prod_{1 \le i < j \le k} |R_{n_i n_j}|$$

possible values for these constants.
Now, for every $i = 1, 2, \cdots, k-1$, as

$$C(g \cdot a_k^s, a_i) = \omega_{g,s} \cdot M_{g,s},$$

where $M_{g,s}$ is an expression in terms of $C(a_i, a_j)$ with $1 \le i < j \le k-1$, and $\omega_{g,s}^{n_i} = 1$, then we have

$$|R_{n_i}|^{|G_1| n_k - (k+1)} = |R_{n_i}|^{|G|-(k+1)}$$

possibilities for these constants, since when $s = 0$ we have k terms, $C(a_l, a_i)$ for $1 \le l \le k-1$ that we do not have to take in account, and also we do not have to count $C(a_k, a_i) = 1$ and $C(1, a_i)$.
Finally, as

$$C(g \cdot a_k^s, a_k) = \omega_{g,s} \cdot M_{g,s},$$

where $\omega_{g,s}^{n_k} = 1$ and $M_{g,s}$ is an expression in terms of $C(a_i, a_j)$ with $1 \leq i < j \leq k-1$, then we have

$$|R_{n_k}|^{|G_1|n_k-(k+1)} = |R_{n_k}|^{|G|-(k+1)}$$

possibilities for these constants, since we do not have to take in account the constants $C(a_i, a_k)$ for $1 \leq i \leq k$ and $C(1, a_k) = 1$.

Hence, the number of non- (graded) isomorphic $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebras with structure constants taking values in a finite subgroup $A \subset \mathbb{C}^*$ is given by

$$\prod_{i=1}^{k} |R_{n_i}|^{|G|-(k+1)} \prod_{1 \leq i < j \leq k} |R_{n_i n_j}|.$$

□

10. CLASSIFICATION OF $(2,3)$-SYMMETRIC G-GRADED TWISTED $\mathbb{C}$-ALGEBRAS

Here we discuss the classification of $(2,3)$-symmetric G-graded twisted $\mathbb{C}$-algebras, for G any finite abelian group.

Definition 9. A G-graded twisted K-algebras W is called $(2,3)$-symmetric if $r(a,b,c) = r(a,c,b)$ for every $a,b,c \in G$.

Between the Lie algebras, there are two important kind of algebras called *Left Symmetric* algebras and *Right Symmetric* algebras denoted by *LSA* and *RSA*. It is well known that there is a bijective correspondence between these algebras. In the theory of G-graded twisted algebras, the *LSA* are related with the $(1,2)$-symmetric G-graded twisted algebras and the *RSA* are related with the $(2,3)$-symmetric G-graded twisted algebras. Following exactly the same arguments developed in the last chapter, with the only difference that r now satisfies the condition $r(a,b,c) = r(a,c,b)$ for every $a,b,c \in G$, we deduce the following theorem:

Theorem 11. *The number of non-(graded) isomorphic $(2,3)$-symmetric $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$-graded twisted $\mathbb{C}$-algebras with structure constants taking values in a finite subgroup $A \subset \mathbb{C}^*$ is given by the product:*

$$\prod_{i=1}^{k} |R_{n_i}|^{|G|-(k+1)} \prod_{1 \leq i < j \leq k} |R_{n_i n_j}|,$$

where R_{n_i} denotes the set $\{\omega \in A \quad : \quad \omega^{n_i} = 1\}$.

Therefore for the case of G-graded twisted $\mathbb{C}$-algebras, we also have a bijective correspondence between the $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebras and the $(2,3)$-symmetric G-graded twisted $\mathbb{C}$-algebras.

11. LEFT SYMMETRIC ALGEBRAS AND THEIR RELATIONSHIP WITH $(1,2)$-SYMMETRIC G-GRADED TWISTED ALGEBRAS

Definition 10. Given W an algebra, we define the associator (X,Y,Z) as:

$$(X,Y,Z) = (XY)Z - X(YZ), \quad \text{for } X,Y,Z \in W.$$

Definition 11. We say that an algebra W is a *Left Symmetric Algebra* (LSA) if

$$(X,Y,Z) = (Y,X,Z), \text{ for every } X,Y,Z \in W.$$

Suppose that G is any abelian group, and consider W a G-graded twisted algebra with structure constant $C : G \times G \to A$, where $C(a,b) \in A$ is such that $w_a w_b = C(a,b)w_{ab}$. Remember that we have two important functions associated to each G-graded twisted algebra, the functions q and r, where

$$q(a,b) = C(a,b)C(b,a)^{-1},$$

and

$$r(a,b,c) = C(b,c)C(ab,c)^{-1}C(a,bc)C(a,b)^{-1}.$$

Also, remind that W is $(1,2)$-symmetric if

$$r(a,b,c) = r(b,a,c), \quad \text{for every } a,b,c \in W.$$

Theorem 12. *Let W be a $(1,2)$-symmetric G-graded twisted algebra with structure constant $C : G \times G \to A$, where $C(a,b) \in A$ is such that $w_a w_b = C(a,b)w_{ab}$.*
Then, W is a Left Symmetric Algebra if and only if

$$(q(a,b) - 1)(1 - r(a,b,c)) = 0$$

for every $w_a, w_b, w_c \in W$.

Proof. W Left Symmetric Algebra is equivalent to

$$(w_a, w_b, w_c) = (w_b, w_a, w_c), \quad \text{for every } w_a, w_b, w_c \in W,$$

and this is equivalent to

$$(w_a w_b)w_c - w_a(w_b w_c) = (w_b w_a)w_c - w_b(w_a w_c).$$

The last equation is equivalent to

$$C(a,b)C(ab,c) - C(a,bc)C(b,c) = C(b,a)C(ba,c) - C(b,ac)C(a,c).$$

Multiplying both sides by $C(ab,c)^{-1}C(a,b)^{-1}$ we get

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

and as by hypothesis $r(a,b,c) = r(b,a,c)$, then this is equivalent to

$$(q(a,b) - 1)(1 - r(a,b,c)) = 0.$$

□

Now, the following theorem asserts that any $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebra which is Left Symmetric is associative, when G is any finite cyclic group.

Theorem 13. *Let W be a $(1,2)$-symmetric $\mathbb{Z}_n$-graded twisted $\mathbb{C}$-algebra with structure constant $C : \mathbb{Z}_n \times \mathbb{Z}_n \to A$, where $A \subset \mathbb{C}^*$ is a finite subgroup. Suppose that W is also Left Symmetric. Then, W is an associative algebra.*

Proof. By Theorem 18, $(q(a^r, a^s) - 1)(1 - r(a^r, a^s, a^t)) = 0$, for every $a^r, a^s, a^t \in \mathbb{Z}_n$.
By the classification of $(1,2)$-symmetric G-graded twisted algebras for cyclic groups, we know that the structure constant C is totally determined by the values $C(a^r, a)$, since $C(a^r, a^s) = C(a^r, a)^s$ (See [26]).
We claim that $C(a^r, a) = 1$ for $r = 1, 2, \ldots, n-1$, what proves that the associative function $r \equiv 1$, and therefore W is an associative algebra.
Indeed, suppose that $C(a^r, a) \neq 1$ for some $r \in \{1, 2, \ldots, n-1\}$. Therefore,

$$(q(a^r, a) - 1)(1 - r(a^r, a, a)) = 0.$$

Thus, as $C(a, a^r) = 1$ then from the last equation we obtain that $(C(a^r, a) - 1)(1 - C(a^{r+1}, a)^{-1}C(a^r, a)) = 0$. Hence, $C(a^{r+1}, a) = C(a^r, a) \neq 1$. In this way, if we repeat the same for $C(a^{r+1}, a) \neq 1$, we get that $C(a^{r+2}, a) \neq 1$. Going on until $r + i = n$, we obtain $C(1, a) \neq 1$, which is clearly a contradiction. Therefore, we conclude that W is an associative algebra. □

We will prove that the last theorem can be generalized to any product of two finite cyclic groups.

Theorem 14. *Suppose that* $G = \mathbb{Z}_m \times \mathbb{Z}_n$ *and that* W *is a* $(1,2)$*-symmetric* G*-graded twisted* $\mathbb{C}$*-algebra with structure constant* $C : G \times G \to A$*, where* $A \subset \mathbb{C}^*$ *is a finite subgroup. Suppose that* W *is also Left Symmetric. Then,* W *is an associative algebra.*

Proof. Here, we use the properties of the structure constant $C : G \times G \to A$ referred to a standard basis $\mathcal{B}$, described in (9.14). We start proving that $\alpha_i = 1$ for $i = 1, 2, \ldots, m$.
We can assume that $C(a,b) \neq 1$ since if $C(a,b) = 1$ then $\alpha_1 = C(a,b)^{-n} = 1$ and hence $\alpha_i = \alpha_1^i = 1$.
As $C(a,b) \neq 1$ then $C(ab,a) = 1$, since

$$(q(a,b) - 1)(1 - r(a,b,a)) = 0$$

and thus

$$(C(a,b) - 1)(1 - C(ab,a)^{-1}C(a,ab)C(a,b)^{-1}) = 0.$$

But notice that $C(a,ab) = C(a,a)C(a,b) = C(a,b)$, therefore as $C(a,b) \neq 1$ then $C(ab,a) = 1$.
On the other hand, if $i \neq n-1$ then $C(b,ab^i) = 1$, hence as

$$(q(b,ab^i) - 1)(1 - r(b,ab^i,a)) = 0$$

then

$$(C(ab^i,b)^{-1} - 1)(1 - C(ab^i,a)C(ab^{i+1},a)^{-1}C(b,a^2b^i)C(b,ab^i)^{-1}) = 0$$

and thus

$$(C(ab^i,b)^{-1} - 1)(1 - C(ab^i,a)C(ab^{i+1},a)^{-1}) = 0.$$

Notice that $c(ab^i,b) = 1$ implies $\alpha_1 = 1$, since $C(ab^i,b)^{-n} = \alpha_1$. Therefore we can suppose that $C(ab^i,b) \neq 1$ and hence

$$C(ab^{i+1},a) = C(ab^i,a), \text{ for every } i \neq n-1.$$

As we saw above, $C(ab,a) = 1$ and thus recursively we have that

$$C(ab^i,a) = 1 \text{ for every } i.$$

In particular, $C(ab^{n-1},a) = 1$.
Now, we know that

$$(q(b,ab^{n-1}) - 1)(1 - r(b,ab^{n-1},a)) = 0,$$

thus

$$(\alpha_1 C(ab^{n-1},b)^{-1}-1)(1-C(b,a^2b^{n-1})C(b,ab^{n-1})^{-1})=0.$$

If $\alpha_1 = C(ab^{n-1},b)$ then as $C(ab^{n-1},b)^n = \alpha_1^{n-1}$ we have that $\alpha_1^n = \alpha_1^{n-1}$ and therefore $\alpha_1 = 1$. We can assume that $\alpha_1 C(ab^{n-1},b) \neq 1$ and thus we conclude that $C(b,a^2b^{n-1})C(b,ab^{n-1})^{-1} = 1$, and therefore $\alpha_2\alpha_1^{-1} = \alpha_1^2\alpha_1^{-1} = \alpha_1 = 1$.
We have just proved that $\alpha_i = 1$ for every $i = 1,2,\ldots,m$ and therefore

$$C(a^rb^s,a^ib^k) = C(a^rb^s,a)^iC(a^rb^s,b)^k.$$

Also, it is not difficult to see that

$$C(a^rb,a) = 1, \quad \text{for every } r.$$

In fact, if we suppose that $C(a,b) \neq 1$, then as

$$(q(a,b)-1)(1-r(a,b,a)) = 0$$

we have that

$$(C(a,b)-1)(1-C(ab,a)^{-1}) = 0,$$

and thus $C(ab,a) = 1$.
In this way, using the fact that

$$(q(ab,a)-1)(1-r(ab,a,a)) = 0,$$

we get

$$(C(a,b)^{-1}-1)(1-C(a^2b,a)^{-1}) = 0,$$

and thus $C(a^2b,a) = 1$.
Recursively we have that $C(a^rb,a) = 1$ for every r.
Now, if $C(a,b) = 1$ then as

$$(q(a^{m-1}b,a)-1)(1-r(a^{m-1}b,a,a)) = 0$$

we have that

$$(C(a^{m-1}b,a)-1)(1-C(a^{m-1}b,a)) = 0$$

and therefore $C(a^{m-1}b,a) = 1$.
As

$$(q(a^{m-2}b,a)-1)(1-r(a^{m-2}b,a,a)) = 0,$$

then we get that

$$C(a^{m-2}b, a) = 1.$$

In this way, recursively we get that $C(a^r b, a) = 1$ for every r.

Now, we claim that $C(a^r b^s, a) = 1$ for every r, s.

In order to prove this we have to consider two cases:

If $C(a,b)^t = 1$, then as

$$(q(a, b^t) - 1)(1 - r(a, b^t, a)) = 0$$

we have

$$(C(b^t, a)^{-1} - 1)(1 - C(b^t, a)) = 0$$

and therefore $C(b^t, a) = 1$.

Now, as

$$(q(a^{m-1}b^t, a) - 1)(1 - r(a^{m-1}b^t, a, a)) = 0,$$

then

$$(C(a^{m-1}b^t, a) - 1)(1 - C(a^{m-1}b^t, a)) = 0$$

and hence $C(a^{m-1}b^t, a) = 1$.

Now, as

$$(q(a^{m-2}b^t, a) - 1)(1 - r(a^{m-2}b^t, a, a)) = 0,$$

then

$$(C(a^{m-2}b^t, a) - 1)(1 - C(a^{m-2}b^t, a)) = 0$$

and thus $C(a^{m-2}b^t, a) = 1$.

Recursively we conclude that $C(a^r b^t, a) = 1$ for every r.

If $C(a,b)^t \neq 1$, then as

$$(q(ab^t, a) - 1)(1 - r(ab^t, a, a)) = 0$$

we have

$$(C(a,b)^{-t} - 1)(1 - C(a^2b^t, a)^{-1}) = 0,$$

and therefore $C(a^2b^t, a) = 1$.

Now, as

$$(q(a^2b^t, a) - 1)(1 - r(a^2b^t, a, a)) = 0,$$

then

$$(C(a,b)^{-t} - 1)(1 - C(a^3b^t, a)^{-1}) = 0$$

and hence $C(a^3b^t, a) = 1$.
Recursively we get that $C(a^rb^t, a) = 1$ for every r.
We conclude that

$$C(a^rb^s, a) = 1, \quad \text{for every } r, s.$$

Therefore we have

$$C(a^rb^s, a^ib^k) = C(a^rb^s, b)^k.$$

With these simplifications, if we compute the function r we obtain:

$$r(a^rb^s, a^ib^k, a^jb^l) = C(a^ib^k, b)^l C(a^{r+i}b^{s+k}, b)^{-l} C(a^rb^s, b)^l.$$

Therefore, if we are trying to prove that the algebra is associative, then we have to check that $r(a^rb^s, a^ib^k, a^jb^l) = 1$, hence it is enough to prove that

$$C(a^{r+i}b^{s+k}, b) = C(a^rb^s, b)C(a^ib^k, b). \tag{11.1}$$

First of all, let us see that $C(a^rb^s, b) = C(a^r, b)$.
Indeed, if $C(a^r, b) \neq 1$, then as $(q(a^r, b) - 1)(1 - r(a^r, b, b)) = 0$ we get

$$(C(a^r, b) - 1)(1 - C(a^rb, b)^{-1}C(a^r, b)) = 0,$$

and thus $C(a^rb, b) = C(a^r, b)$.
Now, as $C(a^rb, b) \neq 1$ and $(q(a^rb, b)-1)(1-r(a^rb, b, b)) = 0$, then $C(a^rb^2, b) = C(a^rb, b) = C(a^r, b)$.
In this way, recursively we obtain that

$$C(a^rb^s, b) = C(a^r, b) \quad \text{when} \quad C(a^r, b) \neq 1.$$

If $C(a^r, b) = 1$ then $C(a^rb^s, b) = 1$, since if $C(a^rb^s, b) \neq 1$ for some s, the fact that

$$(q(a^rb^s, b) - 1)(1 - r(a^rb^s, b, b)) = 0$$

implies that $C(a^rb^{s+1}, b) = C(a^rb^s, b)$ and therefore, $C(a^rb^{s+1}, b) \neq 1$. But going on in this way, for $s = n - 1$ we obtain that $C(a^r, b) \neq 1$, which is a contradiction.
Therefore, if $C(a^r, b) = 1$ then $C(a^rb^s, b) = 1$. Hence, $C(a^rb^s, b) = C(a^r, b)$.
We conclude that in general,

$$C(a^rb^s, b) = C(a^r, b), \quad \text{for all} \quad s = 1, 2, \ldots, n.$$

Thus, the equation (13.1) is equivalent to

$$C(a^{r+i}, b) = C(a^r, b)C(a^i, b). \tag{11.2}$$

Notice that $C(a,b)=1$ implies $C(a^r,b)=1$ for all r, since if we assume that $C(a^r,b)\neq 1$ for some r, then as $(q(a^r,ab)-1)(1-r(a^r,ab,b))=0$, we obtain that $(C(a^r,b)-1)(1-C(a^{r+1},b)^{-1}C(a^r,b))=0$, and therefore $C(a^{r+1},b)=C(a^r,b)\neq 1$. In this way we get that $C(a^{m-1},b)\neq 1$, and hence $C(a,b)\neq 1$, which is a contradiction.

Therefore when $C(a,b)=1$, equation (11.2) holds trivially.

Now, suppose that $C(a,b)\neq 1$. Let us see that $C(a^r,b)=C(a,b)^r$. In fact, as $C(a,b)\neq 1$, then $(q(ab,a)-1)(1-r(ab,a,b))=0$ implies $C(a,b)C(a^2,b)^{-1}C(a,b)=1$, thus $C(a^2,b)=C(a,b)^2$.

As $(q(a^2b,a)-1)(1-r(a^2b,a,b))=0$, then $C(a,b)C(a^3,b)^{-1}C(a^2,b)=1$, and therefore, $C(a^3,b)=C(a,b)^3$.

Recursively, we obtain that $C(a^r,b)=C(a,b)^r$, and thus the equation (11.2) holds.

This proves that $r(a^rb^s,a^ib^k,a^jb^l)=1$ for all $a^rb^s,a^ib^k,a^jb^l\in G$, and hence, the algebra W is associative. □

Finally, we propose a conjecture above the general case of any finite abelian group $G=\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}$.

Conjecture. *Suppose that $G=\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}$ is any finite abelian group and that W is a $(1,2)$-symmetric G-graded twisted $\mathbb{C}$-algebra with structure constant $C:G\times G\to A$, where $A\subset\mathbb{C}^*$ is a finite subgroup. Suppose that W is also Left Symmetric. Then, W is an associative algebra.*

Part III

COMPUTATION OF THE $\mathcal{F}$-RATIONAL LOCUS

12. INTRODUCTION

In this part we describe an algorithm to compute the $\mathcal{F}$-rational locus of an affine algebra over a field of prime characteristic $p > 0$ by first computing its global test ideal. As a consequence we deduce the Openness of the $\mathcal{F}$-rational locus, a result originally proved in [27].

Let A denote the polynomial ring in n variables over a field of prime characteristic p, and let m be any maximal ideal of A. Let us denote by $R = \widehat{A}_m$ the completion of A_m, the localization of A at the maximal ideal m.

If we start with any ideal $I \subset A$, we will present a constructive procedure to explicitly calculate the parameter test ideal of the ring $T = R/IR$. We will regard T as an $R[\theta]$-module, where $\theta : T \to T$ is the natural Frobenius map on T that sends $t \in T$ to its p-th power. In Section 13.2, we will see how to extend this action to an action on $\mathrm{H}^d_m(T)$, the top local cohomology module of T. As will see in Theorem 19, to compute the tight closure of a parameter ideal $J = (x_1, \ldots, x_d)$ of T amounts to compute $0^*_{\mathrm{H}^d_m(T)}$, the tight closure of the zero submodule 0 in $\mathrm{H}^d_m(T)$. But this submodule can be characterized as *the largest $R[\theta]$-submodule N of H that is annihilated by c^2.*

We show how to calculate *globally* the Matlis dual of $N_J = 0^*_{\mathrm{H}^d_m(T)}$ Theorem 25, by computing appropriated matrices $\mathcal{E}_{s\times l}, U_{s\times s}, Q$, with entries in A, so that if Ω denotes the submodule defined by the image of Q in A^s, then Ω is the smallest submodule of A^s satisfying that $(c^2A^s + \mathrm{im}(\mathcal{E}_{s\times l})) \subset \Omega$ and $U_{s\times s}\Omega \subset \Omega^{[p]}$, where $\Omega^{[p]} = \mathrm{im}(Q^{[p]})$. From this we obtain a way of computing the $\mathcal{F}$-rational locus of A/I, where $A = K[x_1, \ldots, x_n]$ is the polynomial ring over a field K of prime characteristic $p > 0$, and $I \subset A$ a prime ideal.

13. PRELIMINARIES

In this part of this thesis, we will use some basic notions of Commutative Algebra and Homological Algebra, classic notions like localization, completion, derived functors, Koszul cohomology, the injective hull, and so on. The reader may consult [3].

13.1 Local Cohomology

In this section, we present briefly some basic notions related with the Local Cohomology Theory, as well as some important results that will be needed in the next sections. The reader may consult [32], for more details.

13.1.1 The injective hull of the residue field of a local ring

Definition 12. Let R be a ring. A homomorphism of R-modules $\tau : M \to N$ is called an *essential extension* if it is injetive and the following equivalent conditions hold:

(1) Every nonzero submodule of N has nonzero intersection with $\tau(M)$.

(2) Every nonzero element of N has a nonzero multiple in $\tau(M)$.

(3) If $\psi : N \to Q$ is a homomorphism and $\psi \circ \tau$ is injective then ψ is injective.

The following proposition summarizes the main properties of essential extensions.

Proposition 7. *Let M, N, and Q be R-modules.*

(1) If $M \subset N \subset Q$ then $M \subset Q$ is essential if and only if $M \subset N$ and $N \subset Q$ are both essential.

(2) If $M \subset N$ and $\{N_i\}_i$ is a family of submodules of N each containing M such that $N = \bigcup_i N_i$, then $M \subset N$ is essential if and only if $M \subset N_i$ is essential for every i.

(3) The identity map on M is an essential extension.

(4) If $M \subset N$ then there is a maximal submodule N' of N such that $M \subset N'$ is essential

The last item in the above Proposition is an immediate consequence of the Zorn's Lemma, and allows to introduce the notion of a *maximal essential extension*.

Given M an R-module, there exists an injective R-module E such that $M \subset E$. We consider a maximal submodule $E_R(M) \subset E$ such that $M \subset E_R(M)$ is essential. The extension $M \subset E_R(M)$ is absolutely essential, in the sense that there are no essential extensions of $E_R(M)$. The definition of $E_R(M)$ seems to depend on the injective module E, however, it is not difficult to see that if $M \subset E'$ for some injective module E', then $E_R(M) \cong E'_R(M)$, in other words, $E_R(M)$ is unique up to isomorphisms. This motivates the following definition:

Definition 13. Let M be an R-module, we define the *injective hull* of M, denoted by $E_R(M)$ as a maximal essential extension of M

Now, suppose that (R, m) is a local ring, we denote E_R by an injective hull of the residue field R/m, i.e., $E_R = E_R(R/m)$.

13.1.2 Local Cohomology

Suppose that R is a Noetherian ring, $I \subset R$ an ideal, and M an R-module. The decreasing sequence of idelas $\cdots \subset I^{k+1} \subset I^k \subset I^{k-1} \subset \cdots$ induces a family of homomorphisms $\{R/I^k \to R/I^{k-1}\}_k$. Given any R-module N, we have a family of homomorphisms $\{\mathrm{Hom}_R(R/I^{k-1}, N) \to \mathrm{Hom}_R(R/I^k, N)\}_k$. Recall that the module $\mathrm{Ext}^i_R(A, B)$ can be computed taking any projective resolution of A

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

removing A, applying the functor $\mathrm{Hom}_R(\_\_, B)$ and taking the i-th homology.
Therefore, if

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow R/I^t \longrightarrow 0$$

and

$$\cdots \longrightarrow Q_n \longrightarrow Q_{n-1} \longrightarrow \cdots \longrightarrow Q_0 \longrightarrow R/I^{t+1} \longrightarrow 0$$

are projective resolutions, then the homomorphism $\theta_{t+1} : R/I^{t+1} \to R/I^t$ induces a map in the homology $\mathrm{Ext}^i_R(R/I^t, M) \to \mathrm{Ext}^i_R(R/I^{t+1}, M)$. Hence, we have a family of homomorphisms $\{\mathrm{Ext}^i_R(R/I^t, M) \to \mathrm{Ext}^i_R(R/I^{t+1}, M)\}_t$.

Definition 14. Let R be a Noetherian ring and let M be an arbitrary module. For $I \subset R$ an ideal, we define the i-th local cohomology module of M with support in I as the direct limit

$$\mathrm{H}^i_I(M) = \varinjlim_t \mathrm{Ext}^i_R(R/I^t, M).$$

In the following theorem we exhibit some important properties of $\mathrm{H}^i_I(M)$.

Theorem 15. *Let R be a Noetherian ring.*

(1) If I, J are ideals of R with the same radical, then $H^i_I(M) \cong H^i_J(M)$ canonically for all i and for all R-module M.

(2) Let $I \subset R$ an ideal and let M be any R-module. Then every element of $H^i_I(M)$ is killed by a power of I.

(3) Let $R \to S$ be a homomorphism of Noetherian rings, let $I \subset R$ be an ideal and let M be an S-module. Then $H^i_I(M) \cong H^i_{IS}(M)$ as S-modules.

(4) Let S be a flat Noetherian R-algebra, and let I be an ideal of R and M an R-module. Then $S \otimes_R H^i_I(M) \cong H^i_I(S \otimes_R M) \cong H^i_{IS}(S \otimes_R M)$.

Let (R, m) be a local ring. The *Matlis dual* is a contravariant functor denoted by $(\_\_)^\vee$ and defined as

$$M^\vee = \mathrm{Hom}_R(M, E_R),$$

where recall that E_R is an injective hull of the residue field R/m.

The proof of the following two theorems may be consulted in [34], pages 12, 16.

Theorem 16 (**Matlis duality**). *Let (R, m) be a Noetherian complete local ring.*

(1) Any Artinian R-module M is isomorphic to a submodule of E^s_R for some integer s. (For this R does not have to be complete)

(2) If M is a module with ACC then $M^\vee$ has DCC, while if M has DCC then $M^\vee$ has ACC. Moreover, if M has either ACC or DCC then the obvious map $M \to M^{\vee\vee}$ is an isomorphism.

Theorem 17 (**local duality for Gorenstein rings**). *Let (R, m, k, E) be a Gorenstein local ring of dimension n. Let M be a finitely generated R-module. Then*

$$H^{n-i}_m(M) \cong Ext^i_R(M, R)^\vee$$

for $0 \leq i \leq n$.

As a consequence of this last theorem, it follows that for every finitely generated R-module M, $\mathrm{H}^i_m(M)$ has DCC, i.e., every descending chain of submodules stabilizes.

Remark 10. Let (R, m) be a Noetherian local ring of dimension d, and let $x_1, \ldots, x_d$ be a system of parameters. It is well known (See [35] , page 100), that the top local cohomology module with support in m, $\mathrm{H}^d_m(R)$ can be seen as the following direct limit

$$\mathrm{H}^d_m(R) \cong \lim_{\overrightarrow{t}} R/(x_1^t, \ldots, x_d^t),$$

where the map $R/(x_1^t, \ldots, x_d^t) \to R/(x_1^{t+1}, \ldots, x_d^{t+1})$ is given by multiplication by $x_1 x_2 \cdots x_d$.

13.2 The Frobenius Functor

Let R be a commutative ring of prime characteristic $p > 0$. The map $\theta : R \to R$ that sends r into r^p is a homomorphism of rings, called the *Frobenius homomorphism*. This homomorphism endows R of structure of R-module by restriction of scalars: $r \cdot s = \theta(r)s = r^p s$. The ring R endowed with the last multiplication will be denoted by S. Notice that $S = R$, but S is viewed as a R-module with the multiplication given by the Frobenius homomorphism θ.

Definition 15. Let M be an R-module. We define $\mathcal{F}_R(M) = S \otimes_R M$, where $r^p s \otimes m = s \otimes r \cdot m$. Clearly $\mathcal{F}_R(M)$ is an S-module with the multiplication $s' \cdot (s \otimes m) = s's \otimes m$.

In general, for any natural number e, we define $\mathcal{F}^e_R(M) = S \otimes_R M$, where $r^{p^e} \otimes m = s \otimes r \cdot m$, and S is the ring R but with the R-module structure given by $r \cdot s = r^{p^e} s$.

If we remember that $S = R$, then M is obviously an S-module with its original structure, and therefore $\mathcal{F}^e_R(\_)$ defines a covariant right exact functor from the category of S-modules to itself. The functor $\mathcal{F}^e_R(\_) : {}_S\mathfrak{Mod} \to {}_S\mathfrak{Mod}$ is called the *Frobenius* or *Peskine-Szpiro* functor. We will omit the subscript R when R is clear from the context.

Remark 11. (1) $\mathcal{F}^e_R(R^n) \cong R^n$, since $\mathcal{F}^e_R(R^n)$ is by definition $S \otimes_R R^n$ which is clearly isomorphic to R^n.

(2) If $I \subset R$ is a ideal then $F^e_R(R/I) \cong R/I^{[p^e]}$, where $I^{[p^e]}$ denotes the ideal generated by the p^e-th powers of the elements of I. This is clear since $\mathcal{F}^e_R(R/I) = S \otimes_R R/I \cong S/IS$, and as the action of R on S is given by $r \cdot s = r^{p^e} s$ then $S/IS \cong R/I^{[p^e]}$.

Proposition 8. *Let M be the cokernel of a matrix A, that is to say, $M = R^n/im(A)$ where $R^m \xrightarrow{A} R^n$. Then, $\mathcal{F}_R^e(R^n/im(A)) = S^n/im(A^{[p^e]})$, where $A^{[p^e]}$ denotes the matrix obtained from A by raising all entries of A to the p^e-th power.*

Proof. We have an exact sequence $R^m \xrightarrow{A} R^n \longrightarrow M \longrightarrow 0$. Applying the Frobenius functor $\mathcal{F}_R^e(\_)$ we obtain a sequence $S^m \xrightarrow{\varphi} S^n \longrightarrow \mathcal{F}_R^e(M) \longrightarrow 0$. Let us compute the map φ. Consider $e_i = (0, \dots 1, \dots 0) \in S^m$ the vector with 1 in the i-th position and zero elsewhere. Notice that $\varphi(e_i) = 1 \cdot Ae_i = (1 \cdot a_{1i}, \dots, 1 \cdot a_{in}) = (a_{1i}^{p^e}, \dots, a_{in}^{p^e})$, where $(a_{1i}, \dots, a_{in})$ is the i-th column of A. This proves that the homomorphism φ is given by the matrix $A^{[p^e]}$. Therefore we have the following commutative diagram

$$\begin{array}{ccccccc} S^m & \xrightarrow{A^{[p]}} & S^n & \longrightarrow & \mathcal{F}_R^e(M) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ S^m & \xrightarrow{A^{[p]}} & S^n & \longrightarrow & S^n/\mathrm{im}(A^{[p^e]}) & \longrightarrow & 0 \end{array}$$

hence, $\mathcal{F}_R^e(R^n/\mathrm{im}(A)) \cong S^n/\mathrm{im}(A^{[p^e]})$. □

Remark 12. A well known theorem of Kunz (See [36], page 247) guarantees that the Frobenius functor $\mathcal{F}_R^e(\_)$ is an exact functor when R is a regular ring. Moreover, it can be readily seen that $\mathcal{F}_R^e(\_)$ also commutes with direct sums and direct limits.

Now we define what is known as a *Frobenius map*.

Definition 16. Let M be an R-module. A morphism of abelian groups $\phi : M \to M$ such that $\phi(rm) = r^p\phi(m)$, is called a *Frobenius map* on M.

The first example of a Frobenius map that comes to mind is the map θ defined above, $\theta : R \to R$, $\theta(r) = r^p$. This map provides an obvious Frobenius map on R^n defined as $\theta(r_1, \dots, r_n) = (r_1^p, \dots, r_n^p)$.

The following proposition allows us to move back and forth from Frobenius maps to ordinary R-linear maps.

Proposition 9. *Let R be a commutative ring of characteristic $p > 0$. Let M be any R-module, and let $\phi : M \to M$ be a Frobenius map on M. Then, there is an S-linear map $\widetilde{\phi} : \mathcal{F}_R(M) \to M$ given by $\widetilde{\phi}(s \otimes m) = s\phi(m)$. Reciprocally, for any S-linear map $\beta : \mathcal{F}_R(M) \to M$, the map $\phi : M \to M$ defined by $\phi(m) = \beta(1 \otimes m)$ is a Frobenius map on M. Any Frobenius map ϕ arises in this way for an appropriate β.*

Proof. Suppose that $\phi : M \to M$ is a Frobenius map on M. Let us see that $\widetilde{\phi}$ is S-linear. Indeed, if we see M as a R-module with the multiplication $r \cdot m = r^p m$, then the map $\beta : S \times M \to M$ given as $\beta(s, m) = s\phi(m)$ is R-bilinear, since $\beta(r \cdot s, m) = \beta(sr^p, m) = sr^p\phi(m) = s\phi(rm)$, and $r \cdot \beta(s, m) = r^p\beta(s, m) = sr^p\phi(m) = s\phi(rm)$. In the same way, $\beta(s, rm) = s\phi(rm) = sr^p\phi(m) = r \cdot \beta(s, m)$. Therefore this R-bilinear map induces the morphism $\widetilde{\phi} : S \otimes_R M \to M$, and this morphism is clearly S-linear.

On the other hand, suppose that we have $\beta : S \otimes_R M \to M$ an S-homomorphism. Define $\phi : M \to M$ as $\phi(m) = \beta(1 \otimes m)$. Notice that $\phi(rm) = \beta(1 \otimes rm) = \beta(r^p \otimes m) = \beta(r^p(1 \otimes m)) = r^p\phi(m)$. Therefore, ϕ is a Frobenius map on M. □

Remark 13. (1) If $M = R/I$, where $I \subset R$ is an ideal, then the natural Frobenius map $\theta : R \to R$ induces a Frobenius map on R/I, $\theta : R/I \to R/I$ given by $\theta(\overline{r}) = \overline{r}^p$. By the last proposition, this Frobenius map on R/I induces the R-linear map $\widetilde{\theta} : \mathcal{F}(R/I) \to R/I$ defined by $\widetilde{\theta}(s \otimes \overline{r}) = s\overline{r}^p$. As $\mathcal{F}(R/I) \cong R/I^{[p]}$ by the isomorphism given by $s \otimes \overline{r} \mapsto \overline{r^p s}$, then the morphism $\widetilde{\theta}$ is just the R-homomorphism induced by the inclusion of ideals $I^{[p]} \subset I$.

(2) In the same way, if $M = R^n/\mathrm{im}(A)$ then θ induces a Frobenius map on $R^n/\mathrm{im}(A)$. An again, the map $\widetilde{\theta} : R^n/\mathrm{im}(A^{[p]}) \to R^n/\mathrm{im}(A)$ is the natural map induced by the inclusion of submodules $\mathrm{im}(A^{[p]}) \subset \mathrm{im}(A)$.

(3) Let R be any commutative ring of characteristic prime $p > 0$, $I \subset R$ an ideal, and let M be any R/I-module. Given $\phi : M \to M$ a Frobenius map on M, as M is a R-module with the multiplication given by $r \cdot m = \overline{r}m$, then ϕ is also a Frobenius map on M viewed as a R-module. As we saw in Proposition 9, ϕ induces an S-linear map $S \otimes_R M \xrightarrow{\widetilde{\phi}} M$ defined as $\widetilde{\phi}(s \otimes m) = s\phi(m)$. Reciprocally, given any S-linear map $\beta : S \otimes_R M \to M$, $\phi : M \to M$ defined by $\phi(m) = \beta(1 \otimes m)$ is a Frobenius map on the R/I-module M, since $\phi(\overline{r}m) = \beta(1 \otimes rm) = \beta(r^p(1 \otimes m)) = \overline{r}^p\beta(1 \otimes m) = \overline{r}^p\phi(m)$.

(4) Let (T, η) be any complete local ring of dimension d of prime characteristic $p > 0$. Let $x_1, \ldots, x_d$ be a fixed system of parameters for T. By Remark 10, the d-th local cohomology with support on η can be calculated as the direct limit $\mathrm{H}^d_\eta(T) = \lim_t T/(x_1^t, \ldots, x_d^t)$ where the maps are given by multiplication by $x = x_1 \cdots x_d$. If $u = [a + (x_1^t, \ldots, x_d^t)]$ denotes the class in the direct limit of the coset $a + (x_1^t, \ldots, x_d^t)$, the map $\theta(u) = [a^p + (x_1^{pt}, \ldots, x_d^{pt})]$ is well defined, and clearly satisfies the condition $\theta(ru) = r^p\theta(u)$. Hence, it is a Frobenius map on $\mathrm{H}^d_\eta(T)$ that we will call the *natural Frobenius map* on $\mathrm{H}^d_\eta(T)$.

Since T is a complete local ring, by the Cohen Structure Theorem (See [3], page 190), we may write $T = R/I$, where (R, m) is the ring of power series with coefficients on a field of characteristic $p > 0$, for some ideal $I \subset R$. By (3), the Frobenius map θ on $\mathrm{H}^d_\eta(T)$ can be obtained from the R-linear map $S \otimes_R \mathrm{H}^d_\eta(T) \xrightarrow{\widetilde{\theta}} \mathrm{H}^d_\eta(T)$. On the other hand, the local cohomology can also be computed as $\mathrm{H}^d_\eta(T) = \mathrm{H}^d_{mT}(R/I)$. Since R is regular the morphism $R \to S$ is flat (See [36], page 247), and consequently $S \otimes_R \mathrm{H}^d_\eta(T) \cong \mathrm{H}^d_{\eta^{[p]}}(S \otimes_R T) = \mathrm{H}^d_{mT}(R/I^{[p]})$. It can be readily seen that $\widetilde{\theta}$ is the map induced by the R/I-homomorphism $\mathrm{H}^d_{mT}(R/I^{[p]}) \to \mathrm{H}^d_{mT}(R/I)$ obtained by applying the covariant functor $\mathrm{H}^d_{mT}(\_)$ to the canonical morphism $R/I^{[p]} \to R/I$ defined by the inclusion of ideals $I^{[p]} \subset I$.

(5) In general, by applying the covariant functor $\mathrm{H}^i_m(\_)$ to the morphism $R/I^{[p]} \to R/I$ one obtains an R/I-map $S \otimes_R \mathrm{H}^i_\eta(T) \cong \mathrm{H}^i_{\eta^{[p]}}(S \otimes_R T) = \mathrm{H}^i_{mT}(R/I^{[p]}) \to \mathrm{H}^i_{mT}(R/I)$.
The Frobenius map induced by this homomorphism will be called *the natural Frobenius map* on $\mathrm{H}^i_\eta(T)$. We will also denote it by θ.

The next proposition is Lemma 4.1 of [37]. It shows that over a complete local ring the functors $\mathcal{F}_R(\_)$ and dualization with E_R the injective hull of the residue field of R commute. More precisely:

Proposition 10. *Let (R, m) be a complete local ring of prime characteristic. Let E_R be an injective hull of the residue field of R. Let us denote by $\vee$ dualization with E_R, i.e., $\vee = Hom_R(\_, E_R)$. If M is an artinian R-module, then there is a canonical isomorphism $\mathcal{F}_R(M^\vee) \cong \mathcal{F}_R(M)^\vee$.*

Proof. (See Lemma 4.1 of [37]). □

13.3 R[t]-Structures

Let M be an R-module where R is a ring of prime characteristic $p > 0$, let $\phi : M \to M$ be a Frobenius map on M, and let us denote by $R[t]$ the (noncommutative) polynomial ring where the identity $t \cdot a = a^p t$ holds for every $a \in R$. It is clear that any Frobenius map on M induces an $R[t]$-module structure in M, since the action of the variable t on M, given by $t \cdot u = \phi(u)$, is well defined: $t \cdot (ru) = \phi(ru) = r^p \phi(u) = (t \cdot r) \cdot u$. The subring $R[\phi]$ of $\mathrm{Hom}_{\mathbb{Z}}(M, M)$ generated by ϕ together with the homomorphisms given by multiplication by elements of R is clearly a homomorphic copy of $R[t]$, since $\phi r = r^p \phi$. Hence, the $R[t]$-structure of M descends to a natural $R[\phi]$-module structure for M.

As we saw in Remark 13 (4), the top cohomology $\mathrm{H}^d_\eta(T)$ of a complete local ring (T, η) can be given a natural $R[t]$-structure via the natural Frobenius map θ. If T is a regular local ring, this top

cohomology module coincides with the injective hull of the residue field $E_T(T/\eta)$ (See [32], page 40). Hence, $E_T(T/\eta)$ becomes an $R[t]$-module, and so does any direct sum of copies of it, $E_T^{\oplus r}$.

If (R, m) is a complete regular local ring of prime characteristic $p > 0$, then R must be a power series ring $R = k[[x_1, \ldots, x_n]]$ over a field of prime characteristic $p > 0$. In this case, the injective hull of its residue field E_R can be identified with the R-module of all "negative"power series, that is, elements of the form $u = \sum_\alpha c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where $\alpha_i < 0$, with the structure of R-module given by:

$$(x_1^{\alpha_1} \cdots x_n^{\alpha_n})(x_1^{\beta_1} \cdots x_n^{\beta_n}) = \begin{cases} 0 & \text{if } \alpha_i + \beta_i \geq 0 \text{ for some } i \\ x_1^{\alpha_1+\beta_1} \cdots x_n^{\alpha_n+\beta_n} & \text{otherwise} \end{cases}$$

It is not difficult to see that the natural Frobenius map on E_R is obtained raising any negative power series to the power p, i.e., $\theta : E_R \to E_R$ where $\theta(\sum_\alpha c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = \sum_\alpha c_\alpha x_1^{p\alpha_1} \cdots x_n^{p\alpha_n}$, and clearly this Frobenius map induces a Frobenius map on $E_R^{\oplus r}$.
Also, it follows that any other Frobenius map on $E_R^{\oplus r}$, $\phi : E_R^{\oplus r} \to E_R^{\oplus r}$, has the form $\phi = u\theta$, where u is an $r \times r$ matrix with coefficients in R.

Remark 14. Let (T, η) be a complete local ring of prime characteristic $p > 0$, and of dimension d. By the Cohen Structure Theorem, we know that $T = R/I$ for some ideal $I \subset R$, and where R is the power series ring $k[[x_1, \ldots, x_n]]$ with k a field of prime characteristic $p > 0$. Consider θ the natural Frobenius map on $\mathrm{H}^d_\eta(T)$, defined in Remark 13 (4). Then, any other Frobenius map on $\mathrm{H}^d_\eta(T)$, $\phi : \mathrm{H}^d_\eta(T) \to \mathrm{H}^d_\eta(T)$ has the form $\phi = u\theta$, where u is a matrix with coefficients in R.

Proof. As $\mathrm{H}^d_\eta(T)$ is an artinian T-module, then by Theorem 16, $\mathrm{H}^d_\eta(T) \hookrightarrow E_T^r$ for some r. On the other hand, it is not difficult to see that $E_T = \mathrm{Ann}_{E_R} I \subset E_R$. Hence, $\mathrm{H}^d_\eta(T) \hookrightarrow E_T^r \subset E_R^r$. Let ϕ be any Frobenius morphism on $\mathrm{H}^d_\eta(T)$. As we saw before, this Frobenius map is induced from an S-linear map $S \otimes_R \mathrm{H}^d_\eta(T) \xrightarrow{\widetilde{\phi}} \mathrm{H}^d_\eta(T)$, where S is the ring R with the R-module structure given by the Frobenius action. Since R is regular, then $S \otimes_R \mathrm{H}^d_\eta(T) \hookrightarrow S \otimes_R E_R^r$ is also an injection, and since E_R^r is an injective R-module, there exists an S-linear map $\widetilde{\psi}$ such that the following diagram commutes:

$$\begin{array}{ccc} S \otimes_R \mathrm{H}^d_\eta(T) & \hookrightarrow & S \otimes_R E_R^r \\ \downarrow{\scriptstyle \widetilde{\phi}} & & \downarrow{\scriptstyle \widetilde{\psi}} \\ \mathrm{H}^d_\eta(T) & \hookrightarrow & E_R^r \end{array}$$

Thus, the Frobenius map $\psi : E_R^r \to E_R^r$, induced by the S-linear map $\widetilde{\psi}$, restricted to $\mathrm{H}^d_\eta(T)$

coincides with ϕ. But as we saw above, $\psi = u\theta$, for some $r \times r$ matrix. Hence, $\phi = u\theta|_{\mathrm{H}^d_\eta(T)}$, where $\theta|_{\mathrm{H}^d_\eta(T)}$ is precisely the natural Frobenius map on $\mathrm{H}^d_\eta(T)$. □

13.4 Tight Closure and Parameter Ideals

In this section we present some definitions and some results related with the Tight Closure Theory, that we will use later.

13.4.1 Tight Closure

Definition 17. Let R be a Noetherian ring of prime characteristic $p > 0$. Given $I \subset R$ an ideal, the *tight closure* of I denoted by I^*, is the ideal defined by the rule: $x \in I^*$ if there is $c \in R$ such that c does not belong to any minimal prime ideal, satisfying that $c \cdot x^{p^e} \in I^{[p^e]}$ for all sufficiently large integers e.

Notice that in the above definition, the element c depend on I and $x \in I^*$. However, as R is a Noetherian ring then I^* is finitely generated, and therefore the element c can be taken depending only on the ideal I.

Before to start taking about the properties of Tight Closure, we present the following proposition, which asserts that we can reduce the study of Tight Closure Theory to Noetherian domains of prime characteristic.

Proposition 11. *Let R be a Noetherian ring of prime characteristic $p > 0$, and assume that $P_1, \ldots, P_k$ are the minimal prime ideals of R. Let $I \subset R$ be an ideal, then $r \in I^*$ if and only if $r + [P_i] \in I^*(R/P_i)$ for every $i = 1, 2, \ldots, k$, where $r + [P_i]$ denotes the equivalence class of r in R/P_i.*

Proof. Suppose that $r + [P_i] \in I^*(R/P_i)$ for every $i = 1, 2, \ldots, k$. Then, for each i there is $c_i \notin P_i$ such that $c_i r^{p^e} \in I^{[p^e]} + P_i$ for $e >> 0$. By the prime avoidance theorem, we can find $d_i \notin P_i$ such that $d_i \in P_j$ for each $j \neq i$. Therefore, $c_i d_i r^{p^e} \in I^{[p^e]} + \mathrm{Nil}(R)$. Taking n with the property $\mathrm{Nil}(R)^n = 0$, we see that $(c_i d_i)^n r^{p^{ne}} \in I^{[p^{ne}]}$. Notice that if we call $s_i = (c_i d_i)^n$, then $s_i \notin P_i$ and $s_i \in P_j$ for each $j \neq i$. Hence, the element $c = s_1 + \cdots + s_k$ does not belong to any minimal prime P_j, and $cr^{p^{ne}} \in I^{[p^{ne}]}$. Thus, $r \in I^*$.
The reciprocal is clear. □

Some basic properties of Tight Closure are presented below:

Remark 15. Let R be a Noetherian ring of prime characteristic $p > 0$, and let I, J be ideals of R.

(1) $I^* \subset R$ is an ideal.

(2) $I \subset I^*$.

(3) $(I^*)^* = I^*$.

(4) If $I \subset J$, then $I^* \subset J^*$.

(5) When R is regular, $I^* = I$.

(6) If $R \subset S$ is a module-finite extension, $IS \cap R \subset I^*$.

(7) $(I \cap J)^* \subset I^* \cap J^*$.

(8) $(I + J)^* = (I^* + J^*)^*$.

(9) $(IJ)^* = (I^* J^*)^*$.

It is well known that for Cohen-Macaulay rings, the colon capturing property holds, in other words, if R is a Cohen-Macaulay ring and $x_1, \ldots, x_d$ is a system of parameters, then

$$((x_1, \ldots, x_i) : x_{i+1}) \subset (x_1, \ldots, x_i)$$

for all $i = 1, 2, \ldots, d-1$. There is a version of the colon capturing property of tight closure which is a kind of generalization of the colon capturing property, in the sense that it holds for more general rings, rings that do not have to be Cohen-Macaulay.

Proposition 12. *Let (R, m) be an equidimensional complete local ring. If $x_1, \ldots, x_d, x_{d+1}$ are parameters in R, then $((x_1, \ldots, x_d)^* : x_{d+1}) \subset (x_1, \ldots, x_d)^*$.*

Proof. See [38] for a proof. □

The last Proposition is more general, it is true for excellent rings, however in this chapter we focus on complete local rings. Every complete local ring is an excellent ring.

Now, the Frobenius functor $\mathcal{F}_R^e(\_)$ defined above, allows to extend the *Tight Closure* notion to modules.

Let R be a Noetherian ring of prime characteristic $p > 0$, and let M be an R-module. For $N \subset M$ an R-submodule, we define the R-module $N_M^{[p^e]}$, as the image of the map $\mathcal{F}^e(N) \to \mathcal{F}^e(M)$. The

tight closure N^*_M of N in M, is defined as the elements $x \in M$ for which there is $c \in R$ not in any minimal prime ideal, such that

$$cx^{p^e} \in N_M^{[p^e]} \subset \mathcal{F}_R^e(M)$$

for all sufficiently large e, where x^{p^e} denotes the image of x under the natural map $M \to \mathcal{F}^e(M)$ that sends $x \mapsto 1 \otimes x$, in other words, $x^{p^e} = 1 \otimes x \in \mathcal{F}^e(M)$. Therefore, with the above notation we see that $(rx)^{p^e} = r^{p^e} x^{p^e}$, for $r \in R$, $x \in M$.

Here are some properties of the *tight closure* for modules.

Remark 16. Let R be a Noetherian ring of prime characteristic $p > 0$.

(1) If $N \subset M$ are R-modules, then N^*_M is an R-module.

(2) If $N \subset M$ are R-modules, then $N \subset N^*_M$ and $(N^*_M)^*_M = N^*_M$.

(2) If $N \subset M \subset Q$ are R-modules, then $N^*_Q \subset M^*_Q$ and $N^*_M \subset N^*_Q$.

(3) If $I \subset R$ is an ideal and $N \subset M$ are R-modules, then $I^* N^*_M \subset (IN)^*_M$.

The following proposition allows to reduce problems related with the tight closure for modules to the study of the tight closure of the zero submodule.

Proposition 13. *Let R be a Noetherian ring of prime characteristic and let $N \subset M$ be R-modules. Then, the image of N^*_M/N in M/N coincides with the tight closure of the zero submodule in M/N, in other words, $N^*_M/N = O^*_{M/N}$ in M/N.*

Proof. As $\mathcal{F}^e(\_)$ is a covariant right exact functor, then the sequence

$$\mathcal{F}^e(N) \longrightarrow \mathcal{F}^e(M) \longrightarrow \mathcal{F}^e(M/N) \longrightarrow 0$$

is exact. By definition $N_M^{[p^e]}$ is the image of the first morphism, therefore

$$\mathcal{F}^e(M/N) \cong \mathcal{F}^e(M)/N_M^{[p^e]}. \tag{13.1}$$

Consider $\overline{x} \in O^*_{M/N}$, then there is $c \in R$ not in any minimal prime ideal, such that $c\overline{x}^{p^e} \in O_{M/N}^{[p^e]} = O$, for e sufficiently large, and by equation (13.1), this implies $cx^{p^e} \in N_M^{[p^e]}$ for $e >> 0$. Thus, $x \in N^*_M$, and therefore $\overline{x} \in N^*_M/N$.
Reciprocally, if $\overline{x} \in M/N$ with $x \in N^*_M$, then, there is $c \in R$ not in any minimal prime ideal such that $cx^{p^e} \in N_M^{[p^e]}$ for $e >> 0$. Therefore, $c\overline{x}^{p^e} = 0$ in $\mathcal{F}^e(M)/N_M^{[p^e]} \cong \mathcal{F}^e(M/N)$ for $e >> 0$. Hence, $\overline{x} \in O^*_{M/N}$. □

13.4.2 Test elements

In the definition of Tight Closure, we saw that the element c may depend on the ideal I and $x \in I^*$. However, for some special rings, it is possible to find an element c that works for any ideal I and any element $x \in I^*$. This kind of elements will be called *test elements*.

Definition 18. Let R be a Noetherian ring of prime characteristic $p > 0$. We say that $c \in R$ not in any minimal prime ideal is a *test element*, if for every finitely generated module M and every submodule N, $x \in N_M^*$ implies $cx^{p^e} \in N_M^{[p^e]}$ for all $e \geq 0$.

The set of test elements together with 0 form an ideal called the *test ideal*.

For reduced complete local rings, the following theorem assures the existence of test elements.

Theorem 18. *Let R be a reduced complete local ring of prime characteristic $p > 0$. Then, there always exist test elements.*

See [28], Theorem 6.1

Let (T, η) be a reduced equidimensional complete local ring of dimension d of prime characteristic $p > 0$. By the Cohen Structure Theorem, T is isomorphic to R/I where R is the power series ring over a field of prime characteristic $p > 0$.

We want to prove, that with the above notation, given $J = (x_1, \ldots, x_d)$ a system of parameters of T, for any element $u \in T$, $u \in J^*$ implies $v = [u + (x_1, \ldots, x_d)] \in O^*_{\mathrm{H}^d_\eta(T)}$, the tight closure of the zero submodule of $\mathrm{H}^d_\eta(T)$, and if $v = [u + (x_1^s, \ldots, x_d^s)] \in O^*_{\mathrm{H}^d_\eta(T)}$, then $u \in J^*$.

We need the following lemma:

Lemma 6. *With the above hypothesis,*

$$((x_1^q, \ldots, x_d^q)^* : x_1^t \cdots x_d^t) \subset (x_1^{q-t}, \ldots, x_d^{q-t})^*,$$

for all $t < q$.

Proof. By induction on t. For $t = 1$, suppose that $\alpha \in ((x_1^q, \ldots, x_d^q)^* : x_1 \cdots x_d)$, then $\alpha x_1 \cdots x_d \in (x_1^q, \ldots, x_d^q)^*$. Hence, if $c \in T$ is a test element, then $c\alpha^{p^e} x_1^{p^e} \cdots x_d^{p^e} \in (x_1^{qp^e}, \ldots, x_d^{qp^e})$, for all $e \geq 0$. Thus, $c\alpha^{p^e} x_1^{p^e} \cdots x_d^{p^e} = r_1 x_1^{qp^e} + \cdots + r_d x_d^{qp^e}$ and then $x_d^{p^e}(c\alpha^{p^e} x_1^{p^e} \cdots x_{d-1}^{p^e} - r_d x_d^{(q-1)p^e}) \in (x_1^{qp^e}, \ldots, x_{d-1}^{qp^e}) \subset (x_1^{qp^e}, \ldots, x_{d-1}^{qp^e})^*$. As $x_1^{qp^e}, \ldots, x_{d-1}^{qp^e}, x_d^{p^e}$ is also a system of parameters, then

by Proposition 12, $c\alpha^{p^e}x_1^{p^e}\cdots x_{d-1}^{p^e} - r_d x_d^{(q-1)p^e} \in (x_1^{qp^e},\ldots,x_{d-1}^{qp^e})^*$. Then, $c\alpha^{p^e}x_1^{p^e}\cdots x_{d-1}^{p^e} \in (x_1^{qp^e},\ldots,x_{d-1}^{qp^e})^* + (x_d^{(q-1)p^e}) \subset (x_1^{qp^e},\ldots,x_{d-1}^{qp^e},x_d^{(q-1)p^e})^*$ for every $e \geq 0$.

Therefore, $c\alpha^{p^e}x_1^{p^e}\cdots x_{d-1}^{p^e} \in ((x_1^q,\ldots,x_{d-1}^q,x_d^{q-1})^{[p^e]})^*$, and by multiplying by c we obtain that $c^2\alpha^{p^e}x_1^{p^e}\cdots x_{d-1}^{p^e} \in c((x_1^q,\ldots,x_{d-1}^q,x_d^{q-1})^{[p^e]})^* \subset (x_1^q,\ldots,x_{d-1}^q,x_d^{q-1})^{[p^e]}$, for every $e \geq 0$. Hence, $\alpha x_1\cdots x_{d-1} \in (x_1^q,\ldots,x_{d-1}^q,x_d^{q-1})^*$.

Arguing in the same way as about but now with the element x_{d-1}, we get that $\alpha x_1\cdots x_{d-2} \in (x_1^q,\ldots,x_{d-2}^q,x_{d-1}^{q-1},x_d^{q-1})^*$. Going on in this way, finally we obtain that $\alpha \in (x_1^{q-1},\ldots,x_d^{q-1})^*$, what proves the first step of the induction.

Now, assume the result holds for t, and let us see that it also holds for $t+1$. Indeed, consider $\alpha \in ((x_1^q,\ldots,x_d^q)^* : x_1^{t+1}\cdots x_d^{t+1})$, thus $\alpha x_1^{t+1}\cdots x_d^{t+1} \in (x_1^q,\ldots,x_d^q)^*$. Therefore, $\alpha x_1\cdots x_d \in ((x_1^q,\ldots,x_d^q)^* : x_1^t\cdots x_d^t)$, and hence, by the induction hypothesis, $\alpha x_1\cdots x_d \in (x_1^{q-t},\ldots,x_d^{q-t})^*$. This implies that $\alpha \in ((x_1^{q-t},\ldots,x_d^{q-t})^* : x_1\cdots x_d) \subset (x_1^{q-(t+1)},\ldots,x_d^{q-(t+1)})^*$. □

Theorem 19. *Let (T,η) be a reduced equidimensional complete local ring of prime characteristic $p>0$, and let $x_1,\ldots,x_d$ be a system of parameters of T. If $J=(x_1,\ldots,x_d)$, then $u \in J^*$ implies that $v=[u+(x_1,\ldots,x_d)] \in O^*_{H^d_\eta(T)}$, and if $v=[u+(x_1^s,\ldots,x_d^s)] \in O^*_{H^d_\eta(T)}$, then $u \in J^*$.*

Proof. Suppose that $v=[u+(x_1^s,\ldots,x_d^s)] \in O^*_{\mathrm{H}^d_\eta(T)}$. Then, by definition, there is $\lambda \in T$ not in any minimal prime, such that $\lambda\theta^e(v)=0$ in $\mathrm{H}^d_\eta(T)$, for $e >> 0$. In other words, $\lambda[u^{p^e}+(x_1^{sp^e},\ldots,x_d^{sp^e})] = [0]$, for $e >> 0$. Therefore, $\lambda x_1^t\cdots x_d^t u^{p^e} \in (x_1^{sp^e+t},\ldots,x_d^{sp^e+t})$, for some $t \geq 0$. This implies that $\lambda u^{p^e} \in ((x_1^{sp^e+t},\ldots,x_d^{sp^e+t}) : x_1^t\cdots x_d^t)$, and by Lemma 6, $\lambda u^{p^e} \in (x_1^{sp^e},\ldots,x_d^{sp^e})^* \subset ((x_1,\ldots,x_d)^{[p^e]})^*$. By multiplying by c, we obtain that $c\lambda u^{p^e} \in c((x_1,\ldots,x_d)^{[p^e]})^* \subset (x_1,\ldots,x_d)^{[p^e]}$, for $e >> 0$, what proves that $u \in J^*$.

Reciprocally, if $u \in J^*$, then $cu^{p^e} \in J^{p^e}$ for all $e \geq 0$. Thus, clearly $c[u^{p^e}+(x_1^{p^e},\ldots,x_d^{p^e})]=0$ for all $e \geq 0$. Hence, $v=[u+(x_1,\ldots,x_d)] \in O^*_{\mathrm{H}^d_\eta(T)}$. □

In the proof of the above theorem, the weak test element λ, actually can be taken as $\lambda = c$. Therefore, this implies that the test element $c \in T$ satisfies that $c^2\theta^e(v)=0$ in $\mathrm{H}^d_\eta(T)$, for $e >> 0$, for all $v \in O^*_{\mathrm{H}^d_\eta(T)}$, where $\theta : \mathrm{H}^d_\eta(T) \to \mathrm{H}^d_\eta(T)$ is the natural Frobenius map defined in Remark 13 (4). Hence, $O^*_{\mathrm{H}^d_\eta(T)}$ is the largest $R[\theta]$-submodule of $\mathrm{H}^d_\eta(T)$, annihilated by c^2. This module will be denoted by N_J.

13.5 Minimal Submodules $I_e(V)$

Definition 19. Let $R = K[x_1, \ldots, x_n]$ where K is a field of prime characteristic $p > 0$. Given an ideal $J \subset R$, define the ideal $I_e(J)$ as the unique smallest ideal I such that $J \subset I^{[p^e]}$.

Let us see how to construct the ideal $I_e(J)$.

We consider first the case $K^p = K$.

Assuming the existence of the ideal $I_e(\_)$, notice that for $J, K \subset R$ ideals, $I_e(J+K) = I_e(J)+I_e(K)$. Therefore, it is enough to prove the existence of $I_e(g)$ for $g \in R$, that is to say, for principal ideals. For $g \in R$, we can write g in a unique form as

$$g = \sum_{0 \leq \alpha_1, \ldots, \alpha_n < p^e} r_\alpha^{p^e} x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \quad \alpha = (\alpha_1, \ldots, \alpha_n).$$

We claim that $I_e(g) = \langle r_\alpha \rangle_{\{\alpha=(\alpha_1,\ldots,\alpha_n) \,:\, 0 \leq \alpha_1, \ldots, \alpha_n < p^e\}}$.

Indeed, if $\langle g \rangle \subset L^{[p^e]}$, suppose that $L = \langle h_1, \ldots, h_m \rangle$, then $g = \sum_{j=1}^m s_j h_j^{p^e}$. But each s_j can be written in a unique way as

$$s_j = \sum_{0 \leq \alpha_1, \ldots, \alpha_n < p^e} s_{j\alpha}^{p^e} x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

hence,

$$g = \sum_{j=1}^m \Big(\sum_{0 \leq \alpha_1, \ldots, \alpha_n < p^e} s_{j\alpha}^{p^e} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \Big) h_j^{p^e} = \sum_{0 \leq \alpha_1, \ldots, \alpha_n < p^e} \Big(\sum_{j=1}^m s_{j\alpha} h_j \Big)^{p^e} x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Therefore, $r_\alpha = \sum_{j=1}^m s_{j\alpha} h_j$. Thus, $\langle r_\alpha \rangle_{\{\alpha=(\alpha_1,\ldots,\alpha_n) \,:\, 0 \leq \alpha_1, \ldots, \alpha_n < p^e\}} \subset L$. This proves that $I_e(g) = \langle r_\alpha \rangle_{\{\alpha=(\alpha_1,\ldots,\alpha_n) \,:\, 0 \leq \alpha_1, \ldots, \alpha_n < p^e\}}$.

For the case $K^p \neq K$, we take a basis $\mathcal{B}$ for K as a K^{p^e}-vector space. It is not difficult to see that any element $g \in R$ can be written in a unique way as

$$g = \sum_{0 \leq \alpha_1, \ldots, \alpha_n < p^e} \sum_{\beta \in \mathcal{B}} \lambda_{\alpha,\beta}^{p^e} r_{\alpha,\beta}^{p^e} b x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \quad \lambda_{\alpha,\beta} \in K, \quad r_{\alpha,\beta} \in R.$$

It follows that $I_e(g) = \langle \lambda_{\alpha,\beta} r_{\alpha,\beta} \rangle$.

We have just shown the existence of the ideals $I_e(J)$, when R is the polynomial ring $R = K[x_1, \ldots, x_n]$. These ideals can be defined in more general rings (See [39]).

For instance, when R regular and free as R^{p^e}-module, we have the following characterization for the ideals $I_e(\_)$.

By a Theorem of Kunz (See [40]), for R a Noetherian ring of prime characteristic $p > 0$, R regular is equivalent to R reduced and flat as R^p-module.

Proposition 14. *Let R be a regular ring which is free as R^{p^e}-module, and let $e_1, \dots, e_n$ be a basis of R over R^{p^e}. Let $J \subset R$ be an ideal, and suppose that $J = \langle a_1, \dots, a_k \rangle$. If*

$$a_i = \sum_{j=1}^{n} r_{i,j}^{p^e} e_j$$

with $r_{i,j} \in R$, for $i = 1, 2, \dots, k$, then $I_e(J) = \langle r_{i,j} \rangle_{i \leq k,\ j \leq n}$.

Proof. Denote $I = \langle r_{i,j} \rangle_{i \leq k,\ j \leq n}$. Clearly $J = \langle a_1, \dots, a_k \rangle \subset \langle r_{i,j}^{p^e} \rangle_{i \leq k,\ j \leq n}$, thus $J \subset I^{[p^e]}$.
Suppose that $J \subset L^{[p^e]}$, for some ideal $L \subset R$. If $L = \langle l_1, \dots, l_s \rangle$, then

$$a_i = \sum_{j=1}^{s} t_{i,j} l_j^{p^e}$$

for $i = 1, 2, \dots, k$. Now, consider the dual basis $e_1^*, \dots, e_n^*$ for $\mathrm{Hom}_{R^{p^e}}(R, R^{p^e})$. As $e_i^*(e_j) = \delta_{i,j}$, then $e_m^*(a_i) = r_{i,m}^{p^e}$. On the other hand, $e_m^*(a_i) = \sum_{j=1}^{s} l_j^{p^e} e_m^*(t_{i,j}) \in L^{[p^e]}$. Hence, $r_{i,m}^{p^e} = \sum_{j=1}^{s} l_j^{p^e} e_m^*(t_{i,j})$. If $t_{i,j} = \sum_{k=1}^{l} b_k^{p^e} e_k$ then $e_m^*(t_{i,j}) = b_m^{p^e}$, therefore we conclude that $r_{i,m}^{p^e} = b^{p^e}$ for some $b \in L$. Since R is reduced we see that $r_{i,m} \in L$. This proves that $I \subset L$ and thus $I = \langle r_{i,j} \rangle_{i \leq k,\ j \leq n} = I_e(J)$. □

The next theorem, extends the definition of $I_e(\_)$ to completions and localizations of regular rings R.

Theorem 20. *Let R be a regular ring. Then, given $J \subset R$ an ideal:*

(1) If S is any multiplicative system in R, then $I_e(S^{-1}J) = S^{-1}I_e(J)$.

(2) If R is local and $\widehat{R}$ is its completion, then $I_e(J\widehat{R}) = I_e(J)\widehat{R}$.

In other words, the operation $I_e(\_)$ commutes with localization and completion.

Proof. (1): Notice that by definition $J \subset I_e(J)^{[p^e]}$, thus $S^{-1}J \subset S^{-1}I_e(J)^{[p^e]} = (S^{-1}I_e(J))^{[p^e]}$. Therefore, $I_e(S^{-1}J) \subset S^{-1}I_e(J)$.

On the other hand, the ideal $I_e(S^{-1}J) = S^{-1}I$ for some $I \subset R$ ideal. Now, by definition $S^{-1}J \subset (S^{-1}I)^{[p^e]} = S^{-1}(I^{[p^e]})$. As we saw in Remark 12, when R is a regular ring, $\mathcal{F}^e$ is exact, therefore, as $(I : s) = I$, for every $s \in S$, then $(I^{[p^e]} : s^{p^e}) = I^{[p^e]}$, for every $s \in S$. Thus, $(I^{[p^e]} : s) = I^{[p^e]}$, for every $s \in S$. Hence, the containment $S^{-1}J \subset S^{-1}(I^{[p^e]})$ implies $J \subset I^{[p^e]}$. As $I_e(J)$ is the smallest ideal with this property, then $I_e(J) \subset I$. Thus, $S^{-1}(I_e(J)) \subset S^{-1}I = I_e(S^{-1}J)$.

(2): As R is regular then R is flat as R^{p^e}-module. Since R is local we have that R is free over R^{p^e}. Now, if $e_1, \dots, e_n$ is a basis of R over R^{p^e}, notice that $e_1, \dots, e_n$ is also a basis of $\widehat{R}$ over $(\widehat{R})^{p^e}$. The result follows from Proposition 14.

□

Remark 17. Let R be a Noetherian ring of prime characteristic $p > 0$. Assume R is regular and $\mathcal{F}$-finite. Here $\mathcal{F}$-finite means that R is finitely generated as R^{p^e}-module. Given $J \subset R$, in order to compute $I_e(J)$, since R_Q is free as $R_Q^{p^e}$-module, then using Proposition 14 we can compute the ideal $I_e(JR_Q)$, and by the last theorem we have the ideal $I_e(J)$.

Now, the following theorem allows to extend the notion $I_e(\_)$ to submodules of free R-modules. For more details see [41].

Definition 20. Let R be a Noetherian ring of prime characteristic $p > 0$. Let $M \subset R^n$ be an R-submodule. We define $M^{[p^e]}$ as the R-submodule generated by $\{x^{p^e} : x \in M\}$

Notice that in the above definition the notation x^{p^e} makes sense, since for elements $x = (r_1, \dots, r_n) \in R^n$ we define $x^{p^e} = (r_1^{p^e}, \dots, r_n^{p^e})$.

The following theorem generalize the operation $I_e(\_)$ to submodules of free R-modules.

Theorem 21. *Let R be a ring for which the operation $I_e(\_)$ is well defined (for example R regular and $\mathcal{F}$-finite). Let $M \subset R^n$ be an R-submodule. Then, there is an R-submodule $L \subset R^n$ minimal with the property $M \subset L^{[p^e]}$. This module will be denoted by $I_e(M)$.*

Proof. Consider the projection homomorphisms $\pi_i : R^n \to R$, for $i = 1, 2, \dots, n$. For each $i = 1, \dots, n$ define $J_i = \{r \in R : r = \pi_i(x) \text{ for some } x \in M\}$. Clearly $J_i \subset R$ is an ideal and $M = J_1 \times \cdots \times J_n$. If $L = I_e(J_1) \times \cdots \times I_e(J_n)$, then $L \subset R^n$ is an R-submodule and $M \subset L^{[p^e]}$, since $J_i \subset I_e(J_i)^{[p^e]}$ for $i = 1, 2, \dots, n$.
Notice that $L = I_e(J_1) \times \cdots \times I_e(J_n)$ is the minimal submodule such that $M \subset L^{[p^e]}$, since if $M \subset T^{[p^e]}$ for some R-submodule $T \subset R^n$, then with the same notation as above, writing $T = T_1 \times \cdots \times T_n$ the containment $M = J_1 \times \cdots \times J_n \subset T^{[p^e]} = T_1^{[p^e]} \times \cdots \times T_n^{[p^e]}$ implies $J_i \subset T_i^{[p^e]}$ for all $i = 1, \dots, n$. Hence, $I_e(J_i) \subset T_i$ for every $i = 1, \dots, n$, and therefore $L = I_e(J_1) \times \cdots \times I_e(J_n) \subset T$. □

We have the analogous of Proposition 14 to submodules, we omit the proof since it follows exactly the same lines:

Proposition 15. *Let R be a regular ring which is free over R^{p^e}. Suppose that $e_1, \dots, e_m$ is a basis of R over R^{p^e}.*

(1) For any R-submodules $W_1, \ldots, W_k \subset R^n$, $I_e(W_1 + \cdots + W_k) = I_e(W_1) + \cdots + I_e(W_k)$.

(2) For $v = (v_1, \ldots, v_n) \in R^n$, if

$$v_i = \sum_{j=1}^{m} r_{i,j}^{p^e} e_j$$

is the unique expression for v_i, then

$$I_e(Rv) = \langle r_{1,j} \rangle_{j=1}^{m} \times \cdots \times \langle r_{n,j} \rangle_{j=1}^{m}$$

.

As we saw for the case of ideals, for R-submodules of R^n, the operation $I_e(\_)$ commutes with localization and completion. We omit the proof since it follows the same lines of Theorem 20.

Theorem 22. *Let R be regular and $\mathcal{F}$-finite and let $M \subset R^n$ be an R-submodule.*

(1) Let $S \subset R$ be a multiplicative system. Then $I_e(S^{-1}(M)) = S^{-1}(I_e(M))$.

(2) If R is local and $\widehat{R}$ denotes its completion, then $I_e(\widehat{M}) = \widehat{I_e(M)}$.

We finalize this section with a theorem that will be needed later.

Theorem 23. *Let R be regular and $\mathcal{F}$-finite. Let U be a $n \times n$ matrix with entries in R and let $M \subset R^n$ be an R-submodule. There is a unique R-submodule $W \subset R^n$ minimal with the property that $M \subset W$ and $UW \subset W^{[p]}$. The R-submodule W will be denoted by $M^{\star U}$.*

Proof. Consider $W_0 = M$ and for $i > 0$, $W_i = I_1(UW_{i-1}) + W_{i-1}$. Clearly $W_0 = M \subset W_1 \subset W_2 \subset \cdots \subset W_n \subset \cdots$. As R is Noetherian the last chain of submodules stabilizes at some N, i.e., $W_N = W_{N+j}$ for all $j \geq 0$. Denote W_N by W. As $W_N = W_{N+1}$, then $W = I_1(UW) + W$. It is clear that $M \subset W$, and $UW \subset W^{[p]}$ since $UW \subset I_1(UW)^{[p]}$ and as $W^{[p]} = I_1(UW)^{[p]} + W^{[p]}$, then $I_1(UW)^{[p]} \subset W^{[p]}$, and therefore $UW \subset W^{[p]}$.
Finally, let us see that W defined above is the minimal R-submodule such that $M \subset W$ and $UW \subset W^{[p]}$. In fact, suppose that $T \subset R^n$ is an R-submodule such that $M \subset T$ and $UT \subset T^{[p]}$. Notice that $I_1(UT) \subset T$, therefore we can see from the way we constructed W that $W_i \subset T$ for all $i \geq 0$, since $W_0 = M \subset T$, $W_1 = I_1(UM) + M \subset I_1(UT) + T \subset T$, and hence, if we suppose that $W_k \subset T$ then $W_{k+1} = I_1(UW_k) + W_k \subset I_1(UT) + T \subset T$. Thus, as $W = W_N$ for some N, we conclude that $W \subset T$. □

14. COMPUTATION OF THE F-RATIONAL LOCUS

We start fixing the notation. In this chapter A will be denoted the polynomial ring $K[x_1, \ldots, x_n]$ where K is a field of prime characteristic $p > 0$, $I \subset A$ a fixed ideal, R will denote the completion of the localization at a maximal ideal m of A, and $T = R/IR$.

With our notation, as $R = \widehat{A_m}$ where $A = K[x_1, \ldots, x_n]$ is the polynomial ring, then (R, m) is a regular local ring of dimension n, and therefore it is Gorenstein. Hence by Theorem 17,

$$\mathrm{H}^d_m(R/IR) \cong \mathrm{Ext}^{n-d}_R(R/IR, R)^\vee,$$

where $d = \dim(R/IR) = \dim(T)$.

Now, as we saw in Remark 13, the natural Frobenius map $\theta : A/I \to A/I$ induces the A-linear homomorphism $\widetilde{\theta} : A/I^{[p]} \to A/I$ given by the canonical map defined by the inclusion $I^{[p]} \subset I$. Let $P^\bullet \xrightarrow{B_\bullet} A/I \to 0$ be any free resolution of A/I. As $\mathcal{F}_A$ is an exact functor since A is regular, $\mathcal{F}_A(P^\bullet) \xrightarrow{B^{[p]}_\bullet} \mathcal{F}_A(A/I) \to 0$ is a free resolution of $\mathcal{F}_A(A/I) = A/I^{[p]}$. Thus, we have the following commutative diagram

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & P^2 & \xrightarrow{B_2} & P^1 & \xrightarrow{B_1} & P^0 & \xrightarrow{B_0} & A/I & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \widetilde{\theta}_2} & & \uparrow{\scriptstyle \widetilde{\theta}_1} & & \uparrow{\scriptstyle \widetilde{\theta}_0} & & \uparrow{\scriptstyle \widetilde{\theta}} & & \\
\cdots & \longrightarrow & \mathcal{F}_A(P^2) & \xrightarrow{B^{[p]}_2} & \mathcal{F}_A(P^1) & \xrightarrow{B^{[p]}_1} & \mathcal{F}_A(P^0) & \xrightarrow{B^{[p]}_0} & A/I^{[p]} & \longrightarrow & 0
\end{array} \tag{14.1}$$

where the map of complexes $\widetilde{\theta}_\bullet$ comes from a lifting of the map $\widetilde{\theta}$.

If $P^k = A^{b_k}$, then $\mathcal{F}_A(P^k) = A^{b_k}$, and the matrix D'_k that represents $\widetilde{\theta}_k : A^{b_k} \to A^{b_k}$ in the standard basis, can be computed explicitly.

On the other hand, we can compute $\mathrm{Ext}^{n-d}_A(A/I, A)$ using the complex $P^\bullet \to 0$ obtained by removing A/I from the free resolution $P^\bullet \xrightarrow{B_\bullet} A/I \to 0$, applying the functor $\mathrm{Hom}_A(\_, A)$ and taking the $(n-d)$-th homology. In the same way, we compute $\mathrm{Ext}^{n-d}_A(\mathcal{F}_A(A/I), \mathcal{F}_A(A))$, using the complex $\mathcal{F}_A(P^\bullet) \to 0$ obtained removing $\mathcal{F}_A(A/I)$ from the free resolution $\mathcal{F}_A(P^\bullet) \xrightarrow{B^{[p]}_\bullet} \mathcal{F}_A(A/I) \to$

0, applying the functor $\mathrm{Hom}_A(\_, A)$ and taking the $(n-d)$-th homology. Therefore, from the commutative diagram (14.1) we have the following morphism of complexes:

$$\begin{array}{ccccccc} \cdots & \longleftarrow & \mathrm{Hom}_A(P^{n-d}, A) & \longleftarrow & \mathrm{Hom}_A(P^{n-d-1}, A) & \longleftarrow & \cdots \\ & & \downarrow{\scriptstyle \widetilde{\theta}^*_{n-d}} & & \downarrow{\scriptstyle \widetilde{\theta}^*_{n-d-1}} & & \\ \cdots & \longleftarrow & \mathrm{Hom}_A(\mathcal{F}_A(P^{n-d}), A) & \longleftarrow & \mathrm{Hom}_A(\mathcal{F}_A(P^{n-d-1}), A) & \longleftarrow & \cdots \end{array} \tag{14.2}$$

where $\widetilde{\theta}^*_{n-d}$ is given in the standard basis by the transpose of the matrix D'_{n-d}, which we will denote by D_{n-d}. This morphism $\widetilde{\theta}^*_{n-d} : \mathrm{Hom}_A(P^{n-d-1}, A) \to \mathrm{Hom}_A(\mathcal{F}_A(P^{n-d}), A)$ induces a map between the homologies

$$D_{n-d} : \mathrm{Ext}^{n-d}_A(A/I, A) \to \mathrm{Ext}^{n-d}_A(\mathcal{F}_A(A/I), \mathcal{F}_A(A)). \tag{14.3}$$

We notice that since A is regular, then $\mathrm{Ext}^{n-d}_A(\mathcal{F}_A(A/I), \mathcal{F}_A(A))$ can be canonically identified with $\mathcal{F}_A(\mathrm{Ext}^{n-d}_A(A/I, A))$.

Now, from the free resolution $P^\bullet \xrightarrow{B_\bullet} A/I \to 0$, we can compute a presentation of $\mathrm{Ext}^{n-d}_A(A/I, A)$,

$$A^l \xrightarrow{\mathcal{E}_{s\times l}} A^s \longrightarrow \mathrm{Ext}^{n-d}_A(A/I, A) \longrightarrow 0\ . \tag{14.4}$$

As $\mathcal{F}_A$ is an exact functor, then applying this functor to the presentation (14.4) we obtain a presentation for $\mathcal{F}_A(\mathrm{Ext}^{n-d}_A(A/I, A))$:

$$A^l \xrightarrow{\mathcal{E}^{[p]}_{s\times l}} A^s \longrightarrow \mathcal{F}_A(\mathrm{Ext}^{n-d}_A(A/I, A)) \longrightarrow 0\ .$$

In this way, we obtain a commutative diagram

$$\begin{array}{ccccccc} A^l & \xrightarrow{\mathcal{E}_{s\times l}} & A^s & \longrightarrow & \mathrm{Ext}^{n-d}_A(A/I, A) & \longrightarrow & 0 \\ \downarrow{\scriptstyle C_{l\times l}} & & \downarrow{\scriptstyle U_{s\times s}} & & \downarrow{\scriptstyle D_{n-d}} & & \\ A^l & \xrightarrow{\mathcal{E}^{[p]}_{s\times l}} & A^s & \longrightarrow & \mathcal{F}_A(\mathrm{Ext}^{n-d}_A(A/I, A)) & \longrightarrow & 0 \end{array} \tag{14.5}$$

where the matrices $C_{l\times l}$ and $U_{s\times s}$ comes from a lifting of the map D_{n-d}.

As R is a flat A-module ($R = \widehat{A_m}$) then $R \otimes_A \mathrm{Ext}^{n-d}_A(A/I, A) \cong \mathrm{Ext}^{n-d}_R(R/IR, R)$. Also, as $\mathcal{F}_A(\mathrm{Ext}^{n-d}_A(A/I, A)) \cong \mathrm{Ext}^{n-d}_A(A/I^{[p]}, A)$, then again as R is flat as A-module we have that $R \otimes_A \mathrm{Ext}^{n-d}_A(A/I^{[p]}, A) \cong \mathrm{Ext}^{n-d}_R(R/I^{[p]}R, R) \cong \mathcal{F}_R(\mathrm{Ext}^{n-d}_R(R/IR, R))$.

Hence, applying the functor $R \otimes_A \_\_$ to (14.5) we obtain the following commutative diagram:

$$\begin{array}{ccccccc} R^l & \xrightarrow{\mathcal{E}_{s\times l}} & R^s & \longrightarrow & \mathrm{Ext}^{n-d}_R(R/I, R) & \longrightarrow & 0 \\ \downarrow{\scriptstyle C_{l\times l}} & & \downarrow{\scriptstyle U_{s\times s}} & & \downarrow{\scriptstyle D_{n-d}} & & \\ R^l & \xrightarrow{\mathcal{E}^{[p]}_{s\times l}} & R^s & \longrightarrow & \mathcal{F}_R(\mathrm{Ext}^{n-d}_R(R/I, R)) & \longrightarrow & 0 \end{array} \tag{14.6}$$

Note that if we have an A-linear map $A^l \overset{\mathcal{E}_{s\times l}}{\to} A^s$ given by the matrix $\mathcal{E}_{s\times l}$ in the standard bases of A^l and A^s, then when we apply $R\otimes_A \_\_$ we get an R-homomorphism $R\otimes_A A^l \overset{Id\otimes\mathcal{E}_{s\times l}}{\to} R\otimes_A A^s$, but identifying $R\otimes_A A^k$ with R^k, the last R-homomorphism corresponds to $R^l \overset{\mathcal{E}_{s\times l}}{\to} R^s$.

Now, applying the Matlis dual $(\_)^\vee = \mathrm{Hom}_R(\_\_, E_R)$, where E_R denotes the injective hull of the residue field R/mR, to the diagram (14.6) we obtain the following commutative diagram:

$$\begin{array}{ccccccc} E_R^l & \xleftarrow{\mathcal{E}_{s\times l}^t} & E_R^s & \longleftarrow & \mathrm{Ext}_R^{n-d}(R/IR,R)^\vee & \longleftarrow & 0 \\ {\scriptstyle C_{l\times l}^t}\uparrow & & \uparrow{\scriptstyle U_{s\times s}^t} & & {\scriptstyle D_{n-d}^t}\uparrow & & \\ E_R^l & \xleftarrow{(\mathcal{E}_{s\times l}^{[p]})^t} & E_R^s & \longleftarrow & \mathcal{F}_R(\mathrm{Ext}_R^{n-d}(R/I,R))^\vee & \longleftarrow & 0, \end{array} \tag{14.7}$$

Notice that if the R-linear map $R^l \overset{\mathcal{E}_{s\times l}}{\to} R^s$ is given by the matrix $\mathcal{E}_{s\times l}$ in the standard bases of R^l and R^s, then after applying $(\_)^\vee = \mathrm{Hom}_R(\_\_, E_R)$ we obtain the R-linear map $\mathrm{Hom}_R(R^s, E_R) \overset{\lambda}{\to} \mathrm{Hom}_R(R^l, E_R)$, where $\lambda(\varphi) = \varphi\circ\mathcal{E}_{s\times l}$. Now, $\mathrm{Hom}_R(R^k, E_R) \cong E_R^k$, where the isomorphism is given by $\varphi \mapsto (\varphi(e_1),\ldots,\varphi(e_k))$, and with this last identification, the R-homomorphism $\lambda : \mathrm{Hom}_R(R^s,E_R)\to\mathrm{Hom}_R(R^l,E_R)$ correspond to the R-homomorphism $E_R^s \overset{\widetilde{\lambda}}{\to} E_R^l$, where $\widetilde{\lambda}$ is given by the matrix $\mathcal{E}_{s\times l}^t$, and $\mathcal{E}_{s\times l}^t$ denotes the transpose of the matrix $\mathcal{E}_{s\times l}$. This is not difficult to see, since $\widetilde{\lambda}(\varphi(e_1),\ldots,\varphi(e_s)) = (\varphi(\mathcal{E}_{s\times l}\cdot e_1),\ldots,\varphi(\mathcal{E}_{s\times l}\cdot e_l))$, and if $\mathcal{E}_{s\times l} = [a_{i,j}]_{i=1,\ldots,s,\ j=1,\ldots,l}$, then $\mathcal{E}_{s\times l}\cdot e_k = (a_{1,k},\ldots,a_{s,k})$. Thus, $(\varphi(\mathcal{E}_{s\times l}\cdot e_1),\ldots,\varphi(\mathcal{E}_{s\times l}\cdot e_l)) = (a_{1,1}\varphi(e_1)+\cdots+a_{s,1}\varphi(e_s),\ldots,a_{1,l}\varphi(e_1)+\cdots+a_{s,l}\varphi(e_s))$. Therefore, $\widetilde{\lambda}(\varphi(e_1),\ldots,\varphi(e_s)) = \mathcal{E}_{s\times l}^t\cdot(\varphi(e_1),\ldots,\varphi(e_s))$.

On the other hand, by Proposition 10, $\mathcal{F}_R(\mathrm{Ext}_E^{n-d}(R/IR,R))^\vee$ can be canonically identified with $\mathcal{F}_R(\mathrm{Ext}_E^{n-d}(R/IR,R)^\vee)$. Hence, by Proposition 9, D_{n-d}^t, the transpose of D_{n-d}, defines a Frobenius map on $\mathrm{Ext}_R^{n-d}(R/IR,R)^\vee$.

Since local duality is an isomorphism of functors, i.e., the two functors $\mathrm{H}_m^d(\_\_)$ and $\mathrm{Ext}_R^{n-d}(\_\_,R)^\vee$ are isomorphic, then the following diagram commutes:

$$\begin{array}{ccc} \mathrm{H}_m^d(R/IR) & \xrightarrow{\ \sim\ } & \mathrm{Ext}_R^{n-d}(R/IR,R)^\vee \\ {\scriptstyle\widetilde{\theta}}\uparrow & & \uparrow{\scriptstyle D_{n-d}^t} \\ \mathcal{F}_R(\mathrm{H}_m^d(R/IR)) & \xrightarrow{\ \sim\ } & \mathcal{F}_R(\mathrm{Ext}_R^{n-d}(R/IR,R)^\vee) \end{array}$$

where the arrow on the left is the natural Frobenius map on $\mathrm{H}_m^d(R/IR)$, as defined in Remark 13 (4). Now, as R is a regular local ring, then $\mathcal{F}_R(\mathrm{H}_m^d(R/IR)) = S\otimes_R \mathrm{H}_m^d(R/IR) \cong \mathrm{H}_m^d(S\otimes_R R/IR) \cong \mathrm{H}_m^d(R/I^{[p]}R)$. In the same way, $\mathcal{F}_R(\mathrm{Ext}_R^{n-d}(R/IR,R)^\vee) = S\otimes_R \mathrm{Ext}_R^{n-d}(R/IR,R)^\vee \cong$

$\mathrm{Ext}_R^{n-d}(S \otimes_R R/IR, R)^\vee \cong \mathrm{Ext}_R^{n-d}(R/I^{[p]}R, R)^\vee$. Therefore,

$$\begin{array}{ccc} \mathrm{H}_m^d(R/IR) & \xrightarrow{\sim} & \mathrm{Ext}_R^{n-d}(R/IR, R)^\vee \\ \uparrow{\scriptstyle \widetilde{\theta}} & & \uparrow{\scriptstyle D_{n-d}^t} \\ \mathrm{H}_m^d(R/I^{[p]}R) & \xrightarrow{\sim} & \mathrm{Ext}_R^{n-d}(R/I^{[p]}R, R)^\vee \end{array} \tag{14.8}$$

is commutative. We have proved the following theorem:

Theorem 24. *(With notation as above) The natural Frobenius map on $H_m^d(R/IR)$ is isomorphic to the Frobenius map induced by D_{n-d}^t on $Ext_R^{n-d}(R/IR, R)^\vee$.*

Consider $N_J = 0^*_{\mathrm{H}_m^d(R/IR)}$. Recall that when R/IR is reduced and equidimensional, N_J is the smallest $R[\theta]$-submodule of $\mathrm{H}_m^d(R/IR)$ that is annihilated by c^2. Applying $(\_)^\vee$ to the inclusion $N_J \hookrightarrow \mathrm{H}_m^d(R/IR)$ we obtain a surjection

$$\mathrm{H}_m^d(R/IR)^\vee \to N_J^\vee \to 0.$$

As $\mathrm{H}_m^d(R/IR) \cong \mathrm{Ext}_R^{n-d}(R/IR, R)^\vee$, then by the Matlis duality (Theorem 16), $\mathrm{H}_m^d(R/IR)^\vee \cong \mathrm{Ext}_R^{n-d}(R/IR, R)$. Therefore we have a surjection

$$\mathrm{Ext}_R^{n-d}(R/IR, R) \to \mathcal{N}_J^\vee \to 0,$$

where $\mathcal{N}_J$ denotes the image of N_J in $\mathrm{Ext}_R^{n-d}(R/IR, R)^\vee$. Clearly, since $c^2 N_J = 0$ then $c^2 \mathcal{N}_J^\vee = 0$, and from (14.8), we see that $\mathcal{N}_J^\vee$ is the largest $R[D_{n-d}^t]$-submodule of $\mathrm{Ext}_R^{n-d}(R/IR, R)^\vee$ that is annihilated by c^2.

Looking at the diagram (14.6), we observe that $\mathrm{Ext}_R^{n-d}(R/IR, R) \cong R^s/\mathrm{im}(\mathcal{E}_{s\times l})$, and $\mathcal{F}_R(\mathrm{Ext}_R^{n-d}(R/IR, R)) \cong R^s/\mathrm{im}(\mathcal{E}_{s\times l}^{[p]})$. Thus, $R^s/\mathrm{im}(\mathcal{E}_{s\times l}) \xrightarrow{\psi} \mathcal{N}_J^\vee \to 0$, and therefore we have the following presentation for $\mathcal{N}_J^\vee$:

$$\begin{array}{ccccccc} R^w & \xrightarrow{Q} & R^s & \xrightarrow{\psi\circ\pi} & \mathcal{N}_J^\vee & \longrightarrow & 0 \\ \downarrow & \nearrow & & & & & \\ \ker(\psi\circ\pi) & & & & & & \end{array}$$

for some $s \times w$ matrix Q. Hence, $\mathcal{N}_J^\vee \cong R^s/\mathrm{im}(Q)$. Therefore, we have the following commutative diagram:

$$\begin{array}{ccccccccc} R^l & \xrightarrow{\mathcal{E}_{s\times l}} & R^s & \xrightarrow{\pi} & R^s/\mathrm{im}(\mathcal{E}_{s\times l}) & \xrightarrow{\psi} & \mathcal{N}_J^\vee & \longrightarrow & 0 \\ \downarrow{\scriptstyle C_{l\times l}} & & \downarrow{\scriptstyle U_{s\times s}} & & \downarrow{\scriptstyle D_{n-d}} & & \downarrow{\scriptstyle d} & & \\ R^l & \xrightarrow{\mathcal{E}_{s\times l}^{[p]}} & R^s & \xrightarrow{\pi} & R^s/\mathrm{im}(\mathcal{E}_{s\times l}^{[p]}) & \xrightarrow{\widetilde{\psi}} & \mathcal{F}_R(\mathcal{N}_J^\vee) & \longrightarrow & 0 \end{array} \tag{14.9}$$

where $d = (D^t_{n-d}|_{\mathcal{N}_J})^\vee$, and $\mathcal{N}_J^\vee \cong R^s/\mathrm{im}(Q)$, $\mathcal{F}_R(\mathcal{N}_J^\vee) \cong R^s/\mathrm{im}(Q^{[p]})$.
Clearly, $\mathrm{im}(Q) \subset \mathrm{im}(\mathcal{E}_{s\times l})$, and as $c^2\mathcal{N}_J^\vee = 0$ then $c^2R^s \subset \mathrm{im}(Q)$. Hence, $c^2R^s + \mathrm{im}(\mathcal{E}_{s\times l}) \subset \mathrm{Q}$. Now, since d is induced by $U_{s\times s}$ on the cokernels, we see that $U\mathrm{im}(Q) \subset \mathrm{im}(Q^{[p]})$. Summarizing, if $\Omega = \mathrm{im}(Q)$, then

$$c^2R^s + \mathrm{im}(\mathcal{E}_{s\times l}) \subset \Omega, \quad U\Omega \subset \Omega^{[p]}, \quad \text{and} \quad \mathcal{N}_J^\vee \cong R^s/\Omega. \tag{14.10}$$

We want to find the way to compute the module Ω, what allows us to compute R^s/Ω which is precisely $(O^*_{\mathrm{H}_m(R/IR)})^\vee$.
Denote $M = c^2R^s + \mathrm{im}(\mathcal{E}_{s\times l})$. Since R is a regular local ring, then R is free as $R^p - module$, and by Theorem 23, there is a unique R-submodule $M^{\star U}$ minimal with the property that $M \subset M^{\star U}$ and $UM^{\star U} \subset (M^{\star U})^{[p]}$. Note that $c^2R^s/M^{\star U} = 0$ since $c^2R^s \subset M^{\star U}$, which implies that $c^2(R^s/M^{\star U})^\vee = 0$. On the other hand, since $\mathrm{im}(\mathcal{E}_{s\times l}) \subset M^{\star U}$, then we have a surjection $R^s/\mathrm{im}(\mathcal{E}_{s\times l}) \to R^s/M^{\star U} \to 0$. Notice that the condition $UM^{\star U} \subset (M^{\star U})^{[p]}$, makes it possible to define a map $\lambda : R^s/M^{\star U} \to R^s/(M^{\star U})^{[p]}$ such that the diagram

$$\begin{array}{ccccccccc}
R^l & \xrightarrow{\mathcal{E}_{s\times l}} & R^s & \xrightarrow{\pi} & R^s/\mathrm{im}(\mathcal{E}_{s\times l}) & \xrightarrow{\psi} & R^s/M^{\star U} & \longrightarrow & 0 \\
\downarrow{\scriptstyle C_{l\times l}} & & \downarrow{\scriptstyle U_{s\times s}} & & \downarrow{\scriptstyle D_{n-d}} & & \downarrow{\scriptstyle \lambda} & & \\
R^l & \xrightarrow{\mathcal{E}^{[p]}_{s\times l}} & R^s & \xrightarrow{\pi} & R^s/\mathrm{im}(\mathcal{E}^{[p]}_{s\times l}) & \xrightarrow{\widetilde{\psi}} & R^s/(M^{\star U})^{[p]} & \longrightarrow & 0
\end{array}$$

commutes, in other words, D_{n-d} induces the map λ. Therefore, applying the Matils dual $(\_)^\vee$ we obtain the following commutative diagram

$$\begin{array}{ccccc}
0 & \longrightarrow & (R^s/M^{\star U})^\vee & \longrightarrow & (R^s/\mathrm{im}(\mathcal{E}_{s\times l}))^\vee \\
 & & \uparrow{\scriptstyle \lambda^\vee} & & \uparrow{\scriptstyle D^t_{n-d}} \\
0 & \longrightarrow & (R^s/(M^{\star U})^{[p]})^\vee & \longrightarrow & (R^s/\mathrm{im}(\mathcal{E}^{[p]}_{s\times l}))^\vee
\end{array}$$

where $\lambda^\vee = D^t_{n-d}|_{(R^s/(M^{\star U})^{[p]})^\vee}$. Hence, $(R^s/M^{\star U})^\vee$ is a $R[D^t_{n-d}]$-submodule of $(R^s/\mathrm{im}(\mathcal{E}_{s\times l}))^\vee$ that is annihilated by c^2.
Now, by the minimality of $M^{\star U}$, $M^{\star U} \subset \Omega$. Thus we have a surjective map $R^s/M^{\star U} \to R^s/\Omega \to 0$, and therefore an injection $0 \to (R^s/\Omega)^\vee \to (R^s/M^{\star U})^\vee$. But $(R^s/\Omega)^\vee = \mathcal{N}_J$ is the largest $R[D^t_{n-d}]$-submodule annihilated by c^2, which implies that $(R^s/\Omega)^\vee \cong (R^s/M^{\star U})^\vee$. We have just proved that computing the R-submodule $M^{\star U}$, we are also computing $\mathcal{N}_J^\vee \cong (O^*_{\mathrm{H}^d_m(R/IR)})^\vee$.

Finally, by the persistence of tight closure under localization and completion (See [33], pages 41,48),

in order to compute the test element $c \in R/IR$, it is enough to compute a test element $c \in A/I$. Therefore, we can assume that $c \in A/I$.
Now, consider the A-submodule $W = c^2A^s + \mathrm{im}(\mathcal{E}_{s\times l}) \subset A^s$ (recall that the matrix $\mathcal{E}_{s\times l}$ has coefficients in A). In order to compute the R-module $M^{\star U}$, we need first to compute the R-module $I_1(M)$, where remind that $M = c^2R^s + \mathrm{im}(\mathcal{E}_{s\times l}) \subset R^s$. By Theorem 22, since $M = WR$, we have that $I_1(M) = I_1(W)R$. Therefore, it is enough to compute $I_1(W)$, where $W = c^2A^s + \mathrm{im}(\mathcal{E}_{s\times l})$. As we saw in the proof of Theorem 23, we constructed the A-submodule $W^{\star U}$, definining the submodules $W_i = I_1(UW_{i-1}) + W_{i-1}$ and taking $W^{\star U} = W_N$, where N is an integer such that $W_{N+i} = W_N$ for all $i \geq 0$. Hence, it follows that $M^{\star U} = W^{\star U}R$.

Now we state our main theorem.

Theorem 25. *Let $A = K[x_1, \ldots, x_n]$ be the polynomial ring in n-variables over a field K of prime characteristic $p > 0$, and let $I \subset A$ be an ideal such that A/I is reduced and equidimensional. Let $\theta : A/I \to A/I$ be the natural Frobenius map on A/I, and let $\widetilde{\theta} : A/I^{[p]} \to A/I$ be the corresponding A-linear map induced by θ, defined by the inclusion of ideals $I^{[p]} \subset I$. Let $D_{n-d} : Ext_A^{n-d}(A/I, A) \to Ext_A^{n-d}(A/I^{[p]}, A)$ be the map constructed in (14.3), and let $U_{s\times s}, C_{l\times l}$ and $\mathcal{E}_{s\times l}$ be matrices as in (14.5). Then, for any maximal ideal $m \subset A$, if R denotes the completion $R = \widehat{A_m}$, the Matlis dual over R of the tight closure of zero $O^*_{H^d_m(R/IR)}$ in $H^d_m(R/IR)$ can be computed globally as the cokernel $W^{\star U}$, i.e., $(O^*_{H^d_m(R/IR)})^\vee \cong R^s/W^{\star U}R$, where $W = c^2A^s + im(\mathcal{E}_{s\times l})$.*

Proof. The result follows immediately from the discussion above. □

Definition 21. A Noetherian ring R of prime characteristic $p > 0$ is said to be $\mathcal{F}$-rational if the ideals generated by parameters are tightly closed. By parameters in R we mean a sequence of elements $x_1, \ldots, x_k$ in R such that for each prime ideal $P \subset R$ containing them, their images in R_P form part of a system of parameters.

Now, in the following theorem we present two important properties of $\mathcal{F}$-rational rings. (See [28], Theorem 4.2, and [29])

Theorem 26. *(1) A local ring which is a homomorphic image of a C-M ring is $\mathcal{F}$-rational iff it is equidimensional and the ideal generated by one system of parameters is tightly closed.*

(2) If R is an excellent local ring (for example R a local complete ring) and J is an ideal generated by parameters of R then $J^*S^{-1}R = (JS^{-1}R)^*$ for any multiplicative system S of R.

As a consequence of Theorem 25, and Theorem 26, we have the following Corollary:

Corollary 4. *Let $A = K[x_1, \ldots, x_n]$ be the polynomial ring in n-variables over a field K of prime characteristic $p > 0$, and let $I \subset A$ be an ideal such that A/I is reduced and equidimensional. Then the $\mathcal{F}$-rational locus of A/I is open. Moreover, this locus can be defined as the complement of the support of $A^s/W^{\star U}$ in the Zariski Topology, where $W = c^2A^s + im(\mathcal{E}_{s\times l})$.*

Proof. Denote $N = A^s/W^{\star U}$ and $J = \mathrm{Ann}_A(N)$. The support of N is determined by $V(J) = \{J \subset P \ : \ P \subset A \text{ prime ideal}\}$. Let P be a prime ideal of A that does not contain J, i.e., $P \in V(J)^c$, and let us show that $(A/I)_P$ is an $\mathcal{F}$-rational ring. Since A/I is a finitely generated algebra over a field, P is the intersection of the maximal ideals that contains it. Thus we may choose a maximal ideal m in A that contains P and such that J is not contained in m. Therefore, $(A^s/W^{\star U})_m = 0$ which implies that $R^s/W^{\star U}R = 0$, where R is the completion of A_m with respect to the maximal ideal m, and by Theorem 25, $0^*_{\mathrm{H}^d_m(R/IR)} = 0$. Hence, R/IR is $\mathcal{F}$-rational, and this implies that A_m/IA_m is $\mathcal{F}$-rational (See [33], page 48), thus $(A/I)_m$ is $\mathcal{F}$-rational, and therefore $(A/I)_P$ is $\mathcal{F}$-rational, since being $\mathcal{F}$-rational descends to localization (See [33], page 41). Reciprocally, assume that $(A/I)_P \cong A_P/IA_P$ is $\mathcal{F}$-rational. If R denotes the completion of A_P with respect to the maximal ideal PA_P, then R/IR is also $\mathcal{F}$-rational (See [33], page 48). Therefore, $0^*_{\mathrm{H}^d_{PR}(R/IR)} = 0$, where $d = \dim(R/IR)$. Hence, by Theorem 25, $R^s/W^{\star U}R^s = 0$. Notice that $R^s/W^{\star U}R^s \cong (A^s/W^{\star U})_P \otimes_A \widehat{A}^P$ and $\widehat{A}^P$ is faithfully flat as A-module, then $(A^s/W^{\star U})_P = 0$. Thus, $P \notin V(J)$.
This proves that the $\mathcal{F}$-rational locus of A/I is $V(J)^c$, which is open in the Zariski topology. □

14.1 An algorithm for the computation of the $\mathcal{F}$-rational locus

Let $A = \mathbb{Z}_p[x_1, \ldots, x_n]$ be the polynomial ring over the field $\mathbb{Z}_p$, and let $Q \subset A$ be a prime ideal. Suppose that A/Q has dimension d.
In this section, we show how to compute algorithmically the $\mathcal{F}$-rational locus of A/Q.
We divide the procedure in several steps:

(1) We compute a free resolution of A-modules for A/Q:

$$\cdots \longrightarrow P_k \xrightarrow{B_r} P_{k-1} \xrightarrow{B_{k-1}} \cdots \longrightarrow P_1 \xrightarrow{B_1} P_0 \xrightarrow{B_0} A/Q \longrightarrow 0$$

where $P_i = A^{b_i}$.

(2) Since A is a regular ring, then $\mathcal{F}_A(\_\_)$ is an exact functor, and therefore by applying the functor $\mathcal{F}_A(\_\_)$ to the last resolution, we obtain a free resolution of A-modules for $A/Q^{[p]}$:

$$\cdots \longrightarrow P_k \xrightarrow{B_r^{[p]}} P_{k-1} \xrightarrow{B_{k-1}^{[p]}} \cdots \longrightarrow P_1 \xrightarrow{B_1^{[p]}} P_0 \xrightarrow{B_0^{[p]}} A/Q^{[p]} \longrightarrow 0$$

(3) Remember that the Frobenius map $\widetilde{\theta} : A/Q^{[p]} \to A/Q$ is the A-linear map induced by the inclusion of ideals $Q^{[p]} \subset Q$. In this step we construct a lifting of the map $\widetilde{\theta}$:

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P^2 & \xrightarrow{B_2} & P^1 & \xrightarrow{B_1} & P^0 & \xrightarrow{B_0} & A/Q & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \widetilde{\theta}_2} & & \uparrow{\scriptstyle \widetilde{\theta}_1} & & \uparrow{\scriptstyle \widetilde{\theta}_0} & & \uparrow{\scriptstyle \widetilde{\theta}} & & \\ \cdots & \longrightarrow & P^2 & \xrightarrow{B_2^{[p]}} & P^1 & \xrightarrow{B_1^{[p]}} & P^0 & \xrightarrow{B_0^{[p]}} & A/Q^{[p]} & \longrightarrow & 0 \end{array} \tag{14.11}$$

Notice that we can compute the matrices that represent the morphisms $\widetilde{\theta}_i$ in the canonical bases of $P_i = A^{b_i}$. To be more precise, the morphism $\widetilde{\theta}_0 = id$, and hence, the first square on the right of (14.11) looks like:

$$\begin{array}{ccccc} A & \xrightarrow{\pi} & A/Q & \longrightarrow & 0 \\ \uparrow{\scriptstyle id} & & \uparrow{\scriptstyle \widetilde{\theta}} & & \\ A & \xrightarrow{\pi} & A/Q^{[p]} & \longrightarrow & 0 \end{array}$$

If $Q = (f_1, \ldots, f_b)$, then the second morphism $\widetilde{\theta}_1$ is given in the canonical basis of A^b by the $b \times b$ matrix

$$V_1 = \begin{bmatrix} f_1^{p-1} & 0 & 0 & \cdots & 0 \\ 0 & f_2^{p-1} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & f_b^{p-1} \end{bmatrix}$$

In other words, the square

$$\begin{array}{ccc} A^b & \xrightarrow{B_1} & A \\ \uparrow{\scriptstyle V_1} & & \uparrow{\scriptstyle id} \\ A^b & \xrightarrow{B_1^{[p]}} & A \end{array}$$

commutes, where $B_1 = [f_1, \ldots, f_b]$, and $B_1^{[p]} = [f_1^p, \ldots, f_b^p]$.
Going on in this way, we compute the matrix V_i that represent the morphism $\widetilde{\theta}_i$. Hence, we obtain a commutative diagram

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & A^{b_2} & \xrightarrow{B_2} & A^{b_1} & \xrightarrow{B_1} & A & \xrightarrow{\pi} & A/Q & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle V_2} & & \uparrow{\scriptstyle V_1} & & \uparrow{\scriptstyle id} & & \uparrow{\scriptstyle \widetilde{\theta}} & & \\ \cdots & \longrightarrow & A^{b_2} & \xrightarrow{B_2^{[p]}} & A^{b_1} & \xrightarrow{B_1^{[p]}} & A & \xrightarrow{\pi} & A/Q^{[p]} & \longrightarrow & 0 \end{array} \tag{14.12}$$

(4) By removing A/Q and $A/Q^{[p]}$, and applying the functor $\mathrm{Hom}_A(\_\_, A)$ in the above diagram, we obtain the following commutative diagram:

$$\begin{array}{ccccccc} \cdots & \longleftarrow & \mathrm{Hom}_A(A^{b_{n-d}}, A) & \xleftarrow{B^t_{n-d}} & \mathrm{Hom}_A(A^{b_{n-d-1}}, A) & \longleftarrow & \cdots \\ & & \downarrow{\scriptstyle V^t_{n-d}} & & \downarrow{\scriptstyle V^t_{n-d-1}} & & \\ \cdots & \longleftarrow & \mathrm{Hom}_A(A^{b_{n-d}}, A) & \xleftarrow{(B^t_{n-d})^{[p]}} & \mathrm{Hom}_A(A^{b_{n-d-1}}, A) & \longleftarrow & \cdots \end{array}$$

where V^t_{n-d} is the transpose of the matrix V_{n-d} computed in (3), and B^t_{n-d} is the transpose of the matrix B_{n-d}.

The matrix V^t_{n-d} induces a map in the homologies

$$D_{n-d} : \mathrm{Ext}^{n-d}_A(A/Q, A) \to \mathrm{Ext}^{n-d}_A(A/Q^{[p]}, A).$$

(5) From the free resolution $P^\bullet \xrightarrow{B_\bullet} A/Q \to 0$, using Groebner bases (see [3], page 366), we can compute a presentation of $\mathrm{Ext}^{n-d}_A(A/Q, A)$,

$$A^l \xrightarrow{\mathcal{E}_{s\times l}} A^s \longrightarrow \mathrm{Ext}^{n-d}_A(A/Q, A) \longrightarrow 0\ . \tag{14.13}$$

As $\mathcal{F}_A(\_\_)$ is an exact functor, then applying this functor to the presentation (14.13) we obtain a presentation for $\mathrm{Ext}^{n-d}_A(A/Q^{[p]}, A)$:

$$A^l \xrightarrow{\mathcal{E}^{[p]}_{s\times l}} A^s \longrightarrow \mathrm{Ext}^{n-d}_A(A/Q^{[p]}, A) \longrightarrow 0\ .$$

In this way, we obtain a commutative diagram

$$\begin{array}{ccccccc} A^l & \xrightarrow{\mathcal{E}_{s\times l}} & A^s & \longrightarrow & \mathrm{Ext}^{n-d}_A(A/Q, A) & \longrightarrow & 0 \\ \downarrow{\scriptstyle C_{l\times l}} & & \downarrow{\scriptstyle U_{s\times s}} & & \downarrow{\scriptstyle D_{n-d}} & & \\ A^l & \xrightarrow{\mathcal{E}^{[p]}_{s\times l}} & A^s & \longrightarrow & \mathrm{Ext}^{n-d}_A(A/Q^{[p]}, A) & \longrightarrow & 0 \end{array} \tag{14.14}$$

where the matrices $C_{l\times l}$ and $U_{s\times s}$ comes from a lifting of the map D_{n-d}.

(6) In this step we compute the test element c. Since A/Q is a domain that is finitely generated as a $\mathbb{Z}_p$-algebra, and $\mathbb{Z}_p$ is a perfect field ($\mathbb{Z}_p^p = \mathbb{Z}_p$), then if $Q = (f_1, \ldots, f_b)$, any nonzero element of the ideal $\mathcal{J}(A/Q)$ generated by the $(n-d)\times(n-d)$ minors of the Jacobian matrix $[\partial f_i/\partial x_j]$ is a test element of A/Q. Furthermore, this remains after localization and completion (See [31], page 195).

Therefore, we can take c as any nonzero element of the ideal $\mathcal{J}(A/Q)$ defined above, and this

element is a test element of A/Q. If $m \subset A$ is any maximal ideal, and if we denote R the completion at m of A_m, then c is also a test element of R/QR.

(7) Consider $W = c^2A^s + \mathrm{im}(\mathcal{E}_{s\times l}) \subset A^s$. Let us see how to compute the module $W^{\star U_{s\times s}}$. Using Groebner bases we find generators $g_1, \ldots, g_k$ for W. Since $I_1(W) = I_1(g_1) + \cdots + I_1(g_k)$, it is enough to compute $I_1(h)$ for any $h \in A^s$. Suppose that $h = (h_1, \ldots, h_s)$ where $h_i \in A$, for $i = 1, \ldots, s$.

Suppose that

$$h_i = \sum_{\alpha=(\alpha_1,\ldots,\alpha_n)} (a_{\alpha,i}) x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

using the division algorithm, any monomial of h_i can be written as $(a_{\alpha,i})x_1^{\beta_1 p} \cdots x_n^{\beta_n p} x_1^{\gamma_1} \cdots x_n^{\gamma_n} = (a_{\alpha,i}x_1^{\beta_1} \cdots x_n^{\beta_n})^p x_1^{\gamma_1} \cdots x_n^{\gamma_n}$, where $\gamma_j < p$ for $j = 1, 2, \ldots, n$, since $\mathbb{Z}_p^p = \mathbb{Z}_p$. Therefore,

$$h_i = \sum_{\substack{\gamma=(\gamma_1,\ldots,\gamma_n) \\ \gamma_i<p}} r_{\gamma,i}^p x_1^{\gamma_1} \cdots x_n^{\gamma_n},$$

where $r_{\gamma,i} \in A$.

As we discuss in section 13.5, this writing is unique, and $I_1(h) = \langle r_{\gamma,1}\rangle_\gamma \times \cdots \times \langle r_{\gamma,s}\rangle_\gamma$. This shows how to compute the module $I_1(W) \subset A^s$. Finally, in Theorem 23, we saw that the module $W^{\star U_{s\times s}}$ can be constructed taking $W_0 = W$, $W_1 = I_1(W) + W$, ..., $W_i = I_1(W_{i-1}) + W_i$, and we have just seen that the ideals $I_1(W_i)$ can be computed algorithmically. Therefore, we can compute the modules $W_0 \subset W_1 \subset \cdots \subset W_k \subset \cdots$. Since A^s is Noetherian, there is $N > 0$ such that $W_N = W_{N+j}$ for all $j \geq 0$. Also notice that if $W_i = W_{i+1}$ for some i, then $W_i = W_{i+j}$ for all $j \geq 0$. Hence, we can check algorithmically if $W_0 = W_1$ or $W_1 = W_2$ or ....$W_N = W_{N+1}$. In this way we can find $N > 0$ such that $W_N = W_{N+1}$, and $W_N = W^{\star U_{s\times s}}$.

(8) By Corollary 4, $W^{\star U_{s\times s}}$ defines the $\mathcal{F}$-rational locus of A/Q.

BIBLIOGRAPHY

[1] Cadavid, C., Molina, S., & Vélez, J. D. (2013). Limits of quotients of bivariate real analytic functions. Journal of Symbolic Computation, 50, 197-207.

[2] W. Fulton, *Algebraic Curves, An introduction to algebraic geometry*, Addison-Wesley, 2008.

[3] D. Eisenbud, *Commutative Algebra with a view towards Algebraic Geometry*, Springer-Verlag, 1994.

[4] H. Whitney, *Elementary Structure of Real Algebraic Varieties*, Annals of Mathematics, Second Series, Vol. 66, No. 3 (Nov., 1957), pp. 545-556.

[5] M.E. Alonso, G. Niesi, T. Mora, M. Raimondo, *Local Parametrization of Space Curves at Singular Points,* Computer Graphics and Mathematics (B. Falcidieno, I. Herman, C. Pienovi, eds.), Eurographic Seminar Series, Springer Verlag, 1992, 61-90.

[6] M.E. Alonso, T. Mora, M. Raimondo, *A Computational Model for Algebraic Power Series*, J. Pure Appl. Alg 77 (1992) 1-38.

[7] S. Basu, R. Pollack, M-F., Roy, *Algorithms in Real Algebraic Geometry*, Springer Verlag 2003.

[8] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[9] F. Cucker, L.Pardo, T.Recio, M.F.Roy, and M.Raimondo. *On the computation of the local and global branches of real algebraic curves*, Proc. AAECC 6, number 356, in Lect. Notes in Comp. Sci., pages 161-181. Springer-Verlag, 1989.

[10] D. Mond, M. Saia, (ed.) *Real and Complex Singularities*, Lecture Notes in Pure and Applied Mathematics 232, Marcel Dekker, (2003).

[11] B. Salvy and J. Shackell. *Symbolic Asymptotics: Multiseries of inverse functions*, J. of Symbolic computation, 27 (6):543-563, June 1999.

[12] M. Greuel, C. Lossen, E. Shustin, *Introduction to Singularities and Deformations*, Springer-Verlag, 2007.

[13] D. Gruntz, *A New Algorithm for Computing Asymptotic Series.* ISSAC 1993, 239-244.

[14] D. Gruntz, *Computing Limits in Computing Algebra Systems*, in Computer Algebra Systems: a Practical guide, ed. by M. J. Wester, John Wiley & Sons, Chichester, U.K., pp. 153-170, 1999.

[15] D. Gruntz, *On computing Limits in a Symbolic Manipulation System*, ETH Diss 11432, 1996.

[16] S. Lang, *Algebra,* Addison-Wesley Publishing Company Inc., 1984.

[17] Edwards, C. M., Lewis, J. T. (1969). Twisted group algebras I. Communications in Mathematical Physics, 13(2), 119-130.

[18] Edwards, C. M., Lewis, J. T. (1969). Twisted group algebras II. Communications in Mathematical Physics, 13(2), 131-141.

[19] Wills, L. A. (2008). Finite group graded lie algebraic extensions and trefoil symmetric relativity, standard model, yang mills and gravity theories (Doctoral dissertation).

[20] Wills-Toro, L. A. (2001). Trefoil symmetries I. Clover extensions beyond Coleman-Mandula theorem. Journal of Mathematical Physics, 42, 3915-3934.

[21] Wills-Toro, L. A., Sanchez, L. A., Osorio, J. M., Jaramillo, D. E. (2001). Trefoil symmetry II. Another clover extension. Journal of Mathematical Physics, 42, 3935-3946.

[22] Wills-Toro, L. A. (2001). Trefoil symmetry III. The full clover extension. Journal of Mathematical Physics, 42(8), 3947-3964.

[23] Wills-Toro, L. A., Sanchez, L. A., Leleu, X. (2003). Trefoil symmetry IV: Basic enhanced superspace for the minimal vector clover extension. International Journal of Theoretical Physics, 42(1), 57-72.

[24] Wills-Toro, L. A., Sanchez, L. A., Bleecker, D. (2003). Trefoil Symmetry V: Class Representations for the Minimal Clover Extension. International Journal of Theoretical Physics, 42(1), 73-83.

[25] Brown, K. S. (1982). Cohomology of groups (No. 87). Springer.

[26] Vélez Juan D. Wills-Toro and Agudelo Natalia, On the classification of G-Graded Twisted Algebras, Journal for Algebra and Number Theory Academia, Volume 4, Issue 1, February 2014, Pages 1-20.

[27] Vélez, J. D. (1995). Openness of the F-rational locus and smooth base change. Journal of Algebra, 172(2), 425-453.

[28] Hochster, M., and Huneke, C. (1994). F-regularity, test elements, and smooth base change. Transactions of the American Mathematical Society, 1-62.

[29] I. ABERBACH, M. HOCHSTER, AND C. HUNEKE, Localizations of tight closure and modules of finite projective dimension, J. Reine Angew. Math. 432 (1993), 67-114. Birkhoff and S. MacLane, "A Brief Survey of Modern Algebra," 2nd ed., Macmillan Co., New York, 1965.

[30] Huneke, C., and Swanson, I. (2006). Integral closure of ideals, rings, and modules (Vol. 13). Cambridge University Press.

[31] Hochster, M. (2005). Tight closure theory and characteristic p methods. Mathematical Sciences Research Institute Publications, 181.

[32] Hochster, M. (2011). Local cohomology. unpublished notes.

[33] Hochster, M., and Huneke, C. (1990). Tight closure, invariant theory, and the Brianon-Skoda theorem. Journal of the American Mathematical Society, 31-116.

[34] Huneke, C. (2007). Lectures on local cohomology. In Contemporary Mathematics.

[35] Brodmann, M. P., and Sharp, R. Y. (2012). Local cohomology: an algebraic introduction with geometric applications (Vol. 136). Cambridge university press.

[36] Huneke, C., and Swanson, I. (2006). Integral closure of ideals, rings, and modules (Vol. 13). Cambridge University Press.

[37] Lyubeznik, G. (1997). F-modules: applications to local cohomology and D-modules in characteristic p¿ 0. Journal fr die reine und angewandte Mathematik (Crelles Journal), 1997(491), 65-130.

[38] Smith, K. E. (1994). Tight closure of parameter ideals. Inventiones mathematicae, 115(1), 41-60.

[39] Blickle, M., Mustata, M., and Smith, K. E. (2006). Discreteness and rationality of F-thresholds. arXiv preprint math/0607660.

[40] Kunz, E. (1969). Characterizations of regular local rings of characteristic p. American Journal of Mathematics, 772-784.

[41] Katzman, M., and Zhang, W. (2014). Annihilators of Artinian modules compatible with a Frobenius map. Journal of Symbolic Computation, 60, 29-46.

[42] Guillemin, V., and Pollack, A. (2010). Differential topology (Vol. 370). American Mathematical Soc..

[43] Matsumura, H. (1989). *Commutative ring theory* (Vol. 8). Cambridge university press.

[44] Hartshorne, R. (1977). *Algebraic geometry* (Vol. 52). Springer Science & Business Media.