Annihilated elements in the homology of powers of infinite complex projective space.

Al-Hajjaj, Haitham Abdulsada R

Annihilated Elements in the Homology of Powers of Infinite Complex Projective Space

Haitham Abdulsada R. Al-Hajjaj

Submitted to Swansea University in fulfilment of the requirements for the Degree of Doctor of Philosophy

Swansea University
2013

Declaration

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed .. .. (candidate)

Date .04./.07../..2013...........

Statement 1

This thesis is the result of my own investigations, except where otherwise stated. Other sources are acknowledged by explicit references. A bibliography is appended.

Signed ... . (candidate)

Date .04../.07../.2013.............

Statement 2

I hereby give consent for my thesis, if accepted, to be available for photocopying and inter-library loan, and for the title and summary to be made available to outside organisations.

Signed .... (candidate)

Date .04../.07./2013............

Contents

Acknowledgements

I would like to thank my supervisor, Martin Crossley, for his patient advice and his encouragements during my study time as a Ph.D. student. I would also like to thank my sponsorship the Iraqi ministry of Higher Education and Scientific Research for providing the funding which without it this work does not undertaking.

I have to express my gratitude to my colleague Simon Fairfax, for the useful mathematical discussions and his language support. I am very thankful to my friends for everything from the first time that I arrived to Swansea up to date also my colleagues in our office.

I am thankful to Mathematics department in Swansea University and the staff for their kindness as well as the department of Mathematics in the University of Sheffield for their offers to attend the TTT conference on two occasions.

I would like to thank the external examiner prof. Ian J. Leary and the internal examiner Dr. Edwin Beggs for their advices to enhance this thesis.

Finally, my special thanks to whom wait me until she passed away as well as my family for every kind of support to complete this work.

Abstract

In this work we proved that $M_n(k) \neq 0$ for $n < p^k + \cdots + p + 1 - k$ as well as the first $M_n(k) = 0$ occurs when $n = p^k + \cdots + p + 1 - k$. We calculated the dimension of $M_n(3)$ for all odd prime where $n < p^2$, and provided a basis elements for $M_n(3)$ for the degrees $n \leq 2p - 1$. For $p = 3$ we described the formula of the the elements of $M_*(3)$ in a higher degrees and proved some result concerning this case. We considered $L_*(k)$ and constructed a general formula for its generators in case $k \leq p$, and calculated the dimension and the basis elements for $L_*(3)$ in some cases.

Chapter 1

Introduction

" We do not know even the dimension of the vector space $QP_k^n = (\mathbb{F}_2 \otimes_{\mathcal{A}(p)} P_k)^n$ for $k = 4$" Kameko said 1998 [12].

In algebraic topology the problem which asks for the minimal set of generators for $H^*(BV_k; \mathbb{F}_p)$ as an $\mathcal{A}(p)$-module is known by the **hit problem**[1] where BV_k is the classifying space of an elementary abelian p-group V_k of rank k, in other word; the underlying group of a k-dimensional vector space over a field $\mathbb{F}_p$ of characteristic p. Alternatively, the aim of this problem is to calculate the basis of the vector space $QP_k^n = (\mathbb{F}_p \otimes_{\mathcal{A}(p)} P_k)^n = P_k^n / \mathcal{A}^+(p) P_k^n$ where P_k^n (the set of all homogeneous polynomials of degree n) is the subset of a polynomial algebra in k-variables over $\mathbb{F}_p$ which is isomorphic to the cohomology of the classifying space of V_k with coefficients in $\mathbb{F}_p$ if $p = 2$ and each variable of degree 1. While when p is an odd prime and each variable of degree 2, then it is isomorphic to the cohomology of the k-fold of infinite complex projective spaces with coefficients in $\mathbb{F}_p$.

That was the *Peterson*'s observation in 1987 in his paper [14] and in the same work, he found the basis of QP_1^n and QP_2^n where $p = 2$. At odd primes it was *Crossley* who addressed this problem for the same values of k in [10]. *Peterson* in the same article had a conjecture which asked about in what degree of n we do not need to look for generators for QP_k^n i.e. $P_k^n = \mathcal{A}^+(p) P_k^n$. In 1988 *R. M. Wood* answered this conjecture in [30], see theorem 4.2.4, and that answer was generalised by *Singer* [21] . The same question may be asked at odd prime (*Peterson* conjecture), but the situation here is more complicated than in case of $p = 2$. *Chen* and *Shen* in [20] and *Crossley* [8] gave some pointers to address this question. In chapter four of this thesis we prove that in the degrees less than $p^k + \cdots + p + 1 - k$ at least there is a generator.

Kameko in 1990 in his Ph.D. thesis [11] and after that in [12] solved the hit problem for $k = 3$ where $p = 2$, and he had a conjecture about the maximum number of the generators in QP_k^n which states that:

[1]Hit problem was termed by W. Singer

Conjecture 1.0.1 (Kameko). *For every non-negative integer n,*

$$dim(\mathbb{F}_2 \otimes_{\mathcal{A}(p)} P_k)^n \leq \prod_{i=1}^{k}(2^i - 1).$$

Kameko's conjecture is true for $k = 1, 2, 3, 4$ according to the results of *Peterson* [14], *Kameko* [11] and *Kameko* [13] and *Nguyễn Sum* in [25][2]. After 20 years in 2010 *Nguyễn Sum* [26] gave a counter example for the *Kameko*'s conjecture for $k \geq 5$. *Crossley* in [8] formulated an analogous conjecture for all odd primes. Additionally, he showed that the number of generators for $H^*(BV_k; \mathbb{F}_p)$ as $\mathcal{A}(p)$- module has to be bounded and this bound depends on the rank of V_k and certainly on p. Similarly, this bound exists in the case of $p = 2$ see [4]. The hit problem particularly when $p = 2$ has been considered from several mathematical areas in many and different aspects.

Turning to the dual case, the dual form of the hit problem is the problem of determining the subring $M_*(k)$ of the *Pontrjagin* ring $H_*(BV_k; \mathbb{F}_p)$ that consists of all elements that annihilated by the right action of $\mathcal{A}(p)$ on $H_*(BV_k; \mathbb{F}_p)$ which is defined by

$$\langle \xi\theta, \zeta \rangle = \langle \xi, \theta\zeta \rangle$$

such that $\theta \in \mathcal{A}(p)$, $\zeta \in H^*(BV_k; \mathbb{F}_p)$ and $\xi \in H_*(BV_k; \mathbb{F}_p)$, i.e. calculate the intersection of $Ker\theta$ for all $\theta \in \mathcal{A}^+(p)$ where $\mathcal{A}^+(p)$ is the set of elements of positive degree of *Steenrod* algebra $\mathcal{A}(p)$ see [17].

The dual approach has been established in 1990 by *Alghamdi*[1], *Crabb* and *Hubbuck* in [2]. In previous work the authors calculated the basis of $M_*(k)$ where $k = 1, 2, 3$ by utilising the generators of the subring $L_*(k)$ of $M_*(k)$ which is known as subring of lines. The significant observation in their work was that $M_n(k) = L_n(k)$ for $k = 1, 2, 3$ except in the degrees $n = 2^{t+3} + 2^{t+1} + 2^t - 3$ such that $t \geq 0$, where the divergence between the dimension of $M_n(3)$ and $L_n(3)$ is 1. Later the subring of lines $L_*(k)$ has been studied extensively by *Crabb* and *Hubbuck* in [5] and *Repka* and *Selick* in [19]. The results of [5] are extended by *Tran Ngoc Nam* in [18]. *Walker* and *Wood* in their work [27] based on [5] and they used the *Schubert* cell decomposition of the flags to give the dimension of $L_n(k)$ for some n, and so a lower bound for $M_n(k)$. All the aforementioned works have performed with $p = 2$.

At odd prime the only study that we see in the dual case was achieved by *Crossley* in 1995 in his Ph.D. thesis [6] and later in [7]. He gave a complete description for $M_*(1)$ and $M_*(2)$ provided with an explicit formula for the basis elements of them.

This thesis involves two parts, the first part consists of two chapters, and there are four chapters in the second one. The first and the second chapters in the first part are

[2]This work consists of 240 pages manuscript. On behalf Dr.*Martin* the author would like to thank *Nguyễn Sum* for sending the description for some cases of calculation QP_4^n.

dedicated for the necessary background that is needed during the current study. In the first one (chapter two), many definitions are stated to introduce the definition of Steenrod algebra and some of its properties.

While the second one (chapter 3) concentrates on the projective spaces from many different points of view, the infinite complex projective space, its cohomology and homology and the action of *Steenrod* operations and their dual on them respectively.

In the second part of the thesis, the objects $M^*(k)$ and $M_*(k)$ are considered in chapter 4 which involves two section. In the first one we introduce the main objects of this work $M_*(k)$ with the motivations behind the study of this objects. While the second one begins with definition of a spike in $H_*(k)$ and its properties which led us to say that there is at least a spike in $H_n(k)$ for $n < p^k + \cdots + p + 1 - k$, and hence $M_n(k) \neq 0$ for those degrees.

Chapter five is divided into two sections. In the first section we calculate the dimension of $M_n(3)$ where $n < p^2$, and giving a basis for $M_n(3)$ where $n \leq 2p - 1$. The second section is devoted to the specific case of $M_*(3)$ where the odd prime is $p = 3$. The results in this section extend the results in the previous one for $p = 3$ and they indicate some pointers to compute whole $M_*(3)$ in a future study for $p = 3$.

The subring of lines $L_*(k)$ is considered in chapter six which consists of two sections. We exploit the right action of $GL(k, \mathbb{F}_p)$ on $H_*(k)$ which commutes with the right action of dual *Steenrod* operations to construct a general formula for the generators of this ring such that $k \leq p$. Motivated by the results in first section, in the second one some cases of $L_n(3)$ are computed.

Ultimately, chapter seven is devoted for general discussion on $M_*(3)/L_*(3)$ with comparing with a achievement works and the difficulties in our case, this chapter is ended by *Crossley*'s conjecture and our computer calculations.

" While much has been written about this problem for $p = 2$, there seems to be little known about the odd primary case. We attempt to redress this imbalance." *Crossley* said 1995 [7].

Part I

Basic concepts of Algebra, and Projective Spaces

Chapter 2

Algebraic concepts

2.1 Algebras

Definition 2.1.1 (R-algebra). Let R be a commutative ring with a unit. An **R-algebra A** is a ring A together with a ring morphism $h : R \longrightarrow A$, such that

$$(r * x) \bullet y = x \bullet (r * y) = r * (x \bullet y), \quad r \in R \text{ and } x, y \in A \tag{2.1}$$

where the operation $\bullet$ is the multiplication of A and the action $* : R \times A \longrightarrow A$ is defined to be $*(r, x) = h(r) \bullet x$. An R-algebra A is called a **commutative R-algebra** if A is a commutative ring, and if it provides an identity element then it is said to be **unital R-algebra**.

There are other languages are used to define the R-algebra, one of them is by commutative diagrams. This definition arises from the fact that any algebraic structure [1] represents a map(s) from the Cartesian product of the underlying set(s) to itself.

According to the previous definition of R-algebra, someone easily can regarded A as R-module by defining the structure map $\varphi : R \times A \longrightarrow A$ by $\varphi(r, x) = h(r) \bullet x$. While, if A is considered as an R-module, relation (2.1) turns the multiplication map (ring multiplication) $\bullet : A \times A \longrightarrow A$ to be R-bilinear map, and the last one determined uniquely R-module homomorphism, namely

$$\mu_A : A \otimes_R A \longrightarrow A.$$

Hence, now we can redefine R-algebra A by the following way.

An R-module A with an R-module homomorphism $\mu_A : A \otimes_R A \longrightarrow A$ is called **nonassociative R-algebra**, and μ_A is often said to be the **multiplication map**. The commutativity of the following diagram

[1] Sometimes this term refers to the underlying set(s) together with the operation(s), here we mean just the operation(s).

$$\begin{array}{ccccc} & & A\otimes_R A & & \\ & \overset{\mu_A\otimes id}{\nearrow} & & \overset{\mu_A}{\searrow} & \\ A\otimes_R A\otimes_R A & & & & A, \\ & \underset{id\otimes\mu_A}{\searrow} & & \underset{\mu_A}{\nearrow} & \\ & & A\otimes_R A & & \end{array}$$

makes A an **associative R-algebra**. Furthermore, the existence of the R-module homomorphism $\eta_A : R \longrightarrow A$ and the commutativity of the following diagram

$$\begin{array}{ccc} A\otimes_R R & & \\ \downarrow{\scriptstyle id\otimes\eta_A} & \overset{\approx}{\searrow} & \\ A\otimes_R A & \xrightarrow{\mu_A} & A \\ \uparrow{\scriptstyle \eta_A\otimes id} & \underset{\approx}{\nearrow} & \\ R\otimes_R A, & & \end{array}$$

provide A with a unit; η_A is called the **unit map**, if such a map is given, then it will be unique. The **structure maps** of an R-algebra A are the multiplication and the unit maps. Finally, the **commutativity** of A is determined by the existence of the **twisting map** which is defined by $\tau(a\otimes b) = b\otimes a$ and the following diagram to be commute

$$\begin{array}{ccc} A\otimes_R A & & \\ \downarrow{\scriptstyle \tau} & \overset{\mu_A}{\searrow} & \\ A\otimes_R A & \xrightarrow{\mu_A} & A. \end{array}$$

Clearly, any ring R is itself R-algebra.

Remark 2.1.2. It is often denoted to a unital R-algebra A by the triple (A, μ_A, η_A).

Definition 2.1.3 (Opposite R-algebra)**.** Let A be an R-algebra with multiplication map μ_A, and τ be the twisting map. The module A over R togather with multiplication map defined by $\mu_A \circ \tau$ is said to be the **opposite R-algebra** of A and denoted A^{op}.

Note that $A = A^{op}$ if, and only if, A is a commutative R-algebra since $\mu_A \circ \tau = \mu_A$ see the definition of commutative R-algebra .

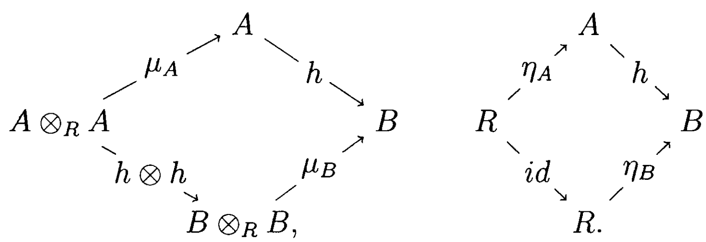
Definition 2.1.4 (Homomorphism of R-algebra)**.** A map $h : A \longrightarrow B$ between a given R-algebras is said to be a **homomorphism of R-algebra** if it satisfies:

1) $h(x + y) = h(x) + h(y)$,

2) $h(xy) = h(x)h(y)$,

3) $h(rx) = rh(x)$.

It is clear that the first and the second conditions make h to be a ring homomorphism. On the other hand, it is an R-module homomorphism or a linear map according to the conditions (1) and (3). The definition of R-algebra homomorphism forces the following diagrams to be commute if, and only if, h is an R-algebra homomorphism



In that case the necessary and sufficient condition that turns h to a homomorphism of R-algebra is $h \circ \mu_A = \mu_B \circ h \otimes h$ and $h \circ \eta_A = \eta_B$.

2.2 Graded algebras

Definition 2.2.1 (Graded module[2]). A **graded** (positively graded)[3] **R-module** M is a family of R-modules $\{M_n\}_{\forall n \in \mathbb{N}}$ such that $M = \bigoplus_{n \in \mathbb{N}} M_n$. Every member in M is said to be a component, and if x an element in the component M_l, then it is called a homogeneous element of degree (dimension) l, which is usually written by $|x| = l$.

Remark 2.2.2. We say M has trivial grading (trivially graded R-module M) when $M = M_0$ and $M_k = 0$ for $k > 0$. Hence, any underlying ring R is trivially graded R-module (put $R = R_0$).

Definition 2.2.3 (Graded R-module homomorphism). A **homomorphism of graded R-module of degree** d between a given graded R-modules M and N is defined to be the following family of R-module homomorphisms

$$h_n : M_n \longrightarrow N_{n+d}, \qquad n \geq 0$$

Remark 2.2.4. If we do not indicate the degree of a homomorphism that means a homomorphism has degree 0, i.e. $h_l(M_l) \subseteq N_l$.

Definition 2.2.5. We define the **tensor product** of two graded R-modules M and N which is also a graded R-module by $(M \otimes_R N)_n = \sum_{r+s=n} M_r \otimes_R N_s$. Thus, the degree of a homogeneous element $m \otimes n$ will be *deg m+deg n*.

[2] We will consider graded module over a graded algebra later, in definition 2.2.13.

[3] The generalisation of the terminology positively graded R-module is $\mathbb{Z}$-graded R-module that is defined by $M = \{M_n\}_{\forall n \in \mathbb{Z}}$, so the case of graded R-module will be the subsequence of the positive part of $\mathbb{Z}$-graded R-module, see [16] page 175 for more details in this case. While, the general definition can be found in [3].

Definition 2.2.6 (Graded R-algebra)**.** A graded R-module A that is equipped with an R-module homomorphism $\mu_A : A \otimes_R A \longrightarrow A$ that preserves the grading, i.e. $\mu_A((A \otimes_R A)_n) \subset A_n$ is said to be **graded R-algebra** and μ_A is known as a **multiplication** or **product** of A.

In the graded case, A is **associative** if $\mu_A \circ (1_A \otimes_R \mu_A) = \mu_A \circ (\mu_A \otimes_R 1_A) : A \otimes_R A \otimes_R A \longrightarrow A$. While, the **commutativity** property is satisfied by existence the twisting map of graded version which is defined by $\tau(x \otimes y) = (-1)^{|x||y|} y \otimes x$, and the property $\mu_A \circ \tau = \mu_A : A \otimes_R A \longrightarrow A$. Finally, the unit element in a graded algebra A has to be homogeneous of degree 0 if the unit is exist.

Remark 2.2.7.

1. According to definitions 2.2.6 and 2.2.2, R itself is a graded R-algebra with the trivial grading and the natural isomorphism $\mu_R : R \otimes_R R \longrightarrow R$ as a product. Clearly, it is unital with unit given by $\eta_R = id_R$.

2. The definition of a homomorphism of graded R-algebra can be deduced from the definitions 2.1.4 and 2.2.3.

Definition 2.2.8 (Augmented algebra)**.** An R-algebra homomorhpism $\varepsilon : A \longrightarrow R$ is said to be **augmentation of** A, while A in such case is called **augmented graded R-algebra**.

Note that if A is an augmented unital graded R-algebra, then for any augmentation ε we have $\varepsilon \circ \eta_A = id_R$.

Definition 2.2.9 (Connected R-algebra)**.** A graded R-algebra A is called a **connected** if there is an isomorphism $c : R \longrightarrow A_0$.

Remark 2.2.10. Any connected graded R-algebra is augmented graded R-algebra by the augmentation $c^{-1} : A \longrightarrow R$.

We define the structure maps $\mu_{A\otimes_R B}$ and $\eta_{A\otimes_R B}$ for $A \otimes B$ where (A, μ_A, η_A), and (B, μ_B, η_B) are graded R-algebras by the following way.

Definition 2.2.11 ($A \otimes_R B$ R-algebra)**.** For a given graded R-algebras (A, μ_A, η_A) and (B, μ_B, η_B). Let $A \otimes B$ be the graded R-module that is defined in 2.2.5. Now, defining the multiplication map $\mu_{A\otimes B}$ to be the following composition

$$(A \otimes_R B) \otimes_R (A \otimes_R B) \xrightarrow{id_A \otimes \tau \otimes id_B} A \otimes_R A \otimes_R B \otimes_R B \xrightarrow{\mu_A \otimes \mu_B} A \otimes_R B,$$

while; define $\eta_{A\otimes_R B}$ to be the following composition

$$R \xrightarrow{\approx} R \otimes_R R \xrightarrow{\eta_A \otimes \eta_B} A \otimes_R B.$$

Example 2.2.12 (Graded algebra)**.** An example of a connected unital graded algebra is the polynomial algebra over a field $\mathbb{F}$ in k variables $x_1, \cdots, x_k$ which is usually denoted by

$$P(k) = \mathbb{F}[x_1, \cdots, x_k].$$

If we consider $P^d(k)$ to be the vector space of homogeneous polynomials of degree d, then $P(k) = \sum_{d \geq 0} P^d(k)$, and $P(k)$ is graded by d. The monomials $x_1^{d_1} \cdots x_k^{d_k}$ where $d_1 + \cdots + d_k = d$ and $d_i \geq 0$ for $1 \leq i \leq k$ will be the basis of $P^d(k)$, if for all i in that range $d_i = 0$, then this is the unit 1 of $P(k)$, clearly; $1 \in P^0(k)$. Identifying $P^0(k)$ with $\mathbb{F}$ enable us to define the identity map $I : \mathbb{F} \longrightarrow P^0(k)$, and hence $P(k)$ is a connected. In the case when $k = 0$, we set $P(0) \approx \mathbb{F}$.

Definition 2.2.13 (Graded module over graded algebra A)**.** Let A be a graded R-algebra and M an A-module. M is called **graded A-module** if there exists a sequence $\{M_n\}_{n\in\mathbb{Z}}$ of R-submodules of M such that $M = \oplus_n M_n$, and $A_m \cdot M_n \subseteq M_{m+n}$ for all m, n.

2.3 Coalgebras

Definition 2.3.1 (R-coalgebra)**.** An R-module C that is provided with an R-linear map $\psi_C : C \longrightarrow C \otimes_R C$ is said to be **R-coalgebra**. The map ψ_C is often called the **comultiplication map**, **coproduct** or **diagonal map**.

Firstly, an R-coalgebra C is a **coassociative** if the following diagram

$$\begin{array}{ccccc} & & C \otimes_R C & & \\ & \nearrow^{\psi_C \otimes id} & & \searrow^{\psi_C} & \\ C & & & & C \otimes_R C \otimes_R C, \\ & \searrow_{id \otimes \psi_C} & & \nearrow_{\psi_C} & \\ & & C \otimes_R C & & \end{array}$$

commutes. Alternatively, $(\psi_C \otimes_R id_C) \circ \psi_C = (id_C \otimes_R \psi_C) \circ \psi_C$.

Furthermore, it is a **cocommutative** R-coalgebra if the twisting map exist, and satisfies $\tau \circ \psi_C = \psi_C$, i.e. the following digram has to be commutative;

$$\begin{array}{ccc} & & C \otimes_R C \\ & \nearrow^{\psi_C} & \big\downarrow \tau \\ C & \xrightarrow{\psi_C} & C \otimes_R C. \end{array}$$

Finally, if there is a linear form $\varepsilon_C : C \longrightarrow R$ such that the following diagrams commute individually,

$$\begin{array}{ccc} C & & \\ \downarrow{\scriptstyle \psi_C} & \searrow^{\approx} & \\ C \otimes_R C & \xrightarrow{\varepsilon_C \otimes id} & R \otimes_R C, \end{array} \qquad \begin{array}{ccc} C & & \\ \downarrow{\scriptstyle \psi_C} & \searrow^{\approx} & \\ C \otimes_R C & \xrightarrow{id \otimes \varepsilon_C} & C \otimes_R R. \end{array}$$

In other word, if $C \otimes_R R$ and $R \otimes_R C$ are identified, then we should have $(\varepsilon_C \otimes id) \circ \psi_C = id_C = (\varepsilon_C \otimes id) \circ \psi_C$. In the case of existence ε_C, then it has to be unique which is called **counit map**, and C is said to be **counital R-coalgebra**.

The term of **structure maps of R-coalgebra** C usually refers to the maps ψ_C, and ε_C.

Remark 2.3.2. Often the triple $(C, \psi_C, \varepsilon_C)$ use as a notation for the unital R-coalgebra.

Definition 2.3.3 (Homomorphism of R-coalgebra). An R-module homomorphism $h : C \longrightarrow D$ between a given coalgebras C and D, such that the following diagrams commute

$$\begin{array}{ccccc} & & D & & \\ & \nearrow^{h} & & \searrow^{\psi_D} & \\ C & & & & D \otimes_R D \\ & \searrow_{\psi_C} & & \nearrow_{h \otimes h} & \\ & & C \otimes_R C. & & \end{array} \qquad \begin{array}{ccccc} & & D & & \\ & \nearrow^{h} & & \searrow^{\varepsilon_D} & \\ C & & & & R \\ & \searrow_{\varepsilon_C} & & \nearrow_{id} & \\ & & R & & \end{array}$$

is called **homomorphism of R-coalgebra**. That is, h is an R-coalgebra homomorphism if, and only if, it satisfies $\psi_D \circ h = (h \otimes h) \circ \psi_D$ and $\varepsilon_D \circ h = \varepsilon_C$.

Definition 2.3.4 (Graded R-coalgebra). An graded R-module C with comultiplication that satisfies $\psi_C(C_n) \subset \bigoplus_{r+s=n} C_r \otimes_R C_s$, is called a graded R-coalgebra, i.e. ψ_C has to preserve the gradation of C.

Remark 2.3.5. One can regard R itself as the graded R-coalgebra with gradation given by $R_0 = R$, $R_k = 0$ for $k > 0$, such that the diagonal map is the natural isomorphism $\psi_R : R \longrightarrow R \otimes_R R$, and the counit map is $\varepsilon_R = id_R : R \longrightarrow R$.

Definition 2.3.6 (Augmented R-coalgebra). An R-coalgebra C is said to be **augmented R-coalgebra**, if there exist an R-coalgebra homomorphism $\varphi : R \longrightarrow C$, which is called **augmentation of C**.

Notice that for any augmentation of C, $\varepsilon_C \circ \varphi = id_R : R \longrightarrow R$

Definition 2.3.7 (Connected R-coalgebra). An augmented R-coalgebra C is said to be **connected R-coalgebra**, if its augmentation is isomorphism.

By the same way as we have regarded the tensor product of two given R-algebras as R-algebra (definition 2.2.11), we may construct the structure maps of the tensor product of a given R-coalgebras from their structure maps as follows

Definition 2.3.8 ($C \otimes_R D$ R-coalgebra)**.** Let $(C, \psi_C, \varepsilon_C)$ and $(D, \psi_D, \varepsilon_D)$ are R-coalgebras, then 2.2.5 implies that $C \otimes_R D$ is graded R-module. The comultiplication map $\psi_{C \otimes D}$ might be defined by the following composition

$$A \otimes_R B \xrightarrow{\psi_A \otimes \psi_B} A \otimes_R A \otimes_R B \otimes_R B \xrightarrow{id_A \otimes \tau \otimes id_B} (A \otimes_R B) \otimes_R (A \otimes_R B),$$

and the counit map $\varepsilon_{C \otimes D}$ is given by

$$C \otimes_R D \xrightarrow{\varepsilon_C \otimes \varepsilon_D} R \otimes_R R \xrightarrow{\approx} R.$$

2.4 Hopf algebra

Definition 2.4.1 (R-Hopf algebra)**.** [4] A graded R-module H that is provided by a structure maps of graded algebra, that is; (H, μ_H, η_H) is graded R-algebra, as well as a structure maps of a graded R-coalgebra i.e. $(H, \psi_H, \varepsilon_H)$ is graded R-coalgebra such that the following diagram

$$\begin{array}{ccccc}
H \otimes_R H & \xrightarrow{\mu_H} & H & \xrightarrow{\psi_H} & H \otimes_R H \\
\downarrow{\scriptstyle \psi_H \otimes \psi_H} & & & & \uparrow{\scriptstyle \mu_H \otimes \mu_H} \\
H \otimes_R H \otimes_R H \otimes_R H & & \xrightarrow{id \otimes \tau \otimes id} & & H \otimes_R H \otimes_R H \otimes_R H
\end{array}$$

commutes , is said to be **Hopf algebra over** R, and it is denoted by $(H, \mu_H, \psi_H, \eta_H, \varepsilon_H)$.

Remark 2.4.2. The maps μ_H, ψ_H, η_H and ε_H are said to be **multiplication** or **product**, **comultiplication** or **coproduct**, **unit** and **counit** of R-Hopf algebra respectively, and together the are called **structure maps**.

On examining the above diagram we have that ψ_H is a homomorphism of R-algebra or μ_H is homomorphism of R-coalgebra. Regarding the definition, it is clear to see that (H, μ_H, η_H) is augmented R-algebra by ε_H, while; η_H can be viewed as coaugmentation of $(H, \psi_H, \varepsilon_H)$.

An R-Hopf algebra is called **associative** or **coassociative** if the underlying R-algebra is associative or if the underlying R-coalgebra is coassociative respectively, and when both properties are satisfied it is said to be **biassociative**.

Similarly, if the underlying R-algebra or R-coalgebra is a commutative or cocommutative, then we say there R-Hopf algebra is **commutative** or **cocommutative** respectively, and by **bicommutative** if it is commutative and cocommutative. While, for the connectivity property we need either the underlying R-algebra or R-coalgebra to be connected, since they are equivalence.

[4] We follow Milnor and Moore in their work [15] to give the definition of R-Hopf algebra.

Definition 2.4.3 (Homomorphism of R-Hopf algebra)**.** Let H and G are Hopf algebras over R. A linear map $h : H \longrightarrow G$ is called a **Hopf algebra homomorphism** or **Hopf map**, if h is an R-algebra homomorphism as well as it is a homomorphism of R-coalgebra.

Remark 2.4.4. The tensor product $H \otimes G$ of a given R-Hopf algebras A and B is, as expected, an Hopf algebra over R whose structure maps is given in definitions 2.2.11 and 2.3.8.

Example 2.4.5 ($H^*(X;R)$ and $H_*(X;R)$ as R-*Hopf* algebra)**.** In many literatures see [23], a H-space is defined to be a pointed topological space (X, e) where e is a basis point, that is equipped with a continuous map $\mu : X \times X \longrightarrow X$ which satisfies $\mu \circ i_1 \simeq id_X$ and $\mu \circ i_2 \simeq id_X$, where $i_1(x) = (c(x), x) : X \longrightarrow X \times X$, $i_2(x) = (x, c(x)) : X \longrightarrow X \times X$ and $c : X \longrightarrow X$ is the constant map $c(X) = \{e\}$.

The map μ is called a multiplication, and is said to be homotopy associative if $\mu \circ (id_X \times \mu)$ homotopic to $\mu \circ (\mu \times id_X)$. A continuous map $\eta : X \longrightarrow X$ is said to be a homotopy inverse if $\mu \circ (id, \eta)$ and $\mu \circ (\eta, id)$ are homotopic to c. A multiplication μ is called homotopy commutative if $\mu \simeq \mu \circ \tau$ where $\tau(x_1, x_2) = (x_2, x_1)$.

Recall that $H^*(X \times X;R) \approx H^*(X;R) \otimes H^*(X;R)$, and that $H_*(X \times X;R) \approx H_*(X;R) \otimes H_*(X;R)$ from *Künneth* formula for cohomology and homology when R is given to be a field. Assume that is the case. Now, consider the continuous maps

$$\{e\} \xrightarrow{i} X \xrightarrow{c} \{e\} \qquad \textit{and} \qquad X \xrightarrow{\Delta} X \times X \xrightarrow{\mu} X,$$

where $\Delta(x) = (x, x), \quad \forall x \in X$ which are induce the following homomorphisms

$$R \xleftarrow{i^*} H^*(X;R) \xleftarrow{c^*} R, \qquad H^*(X;R) \xleftarrow{\Delta^*} H^*(X;R) \otimes H^*(X;R) \xleftarrow{\mu^*} H^*(X;R),$$

and

$$R \xrightarrow{i_*} H_*(X;R) \xrightarrow{c_*} R, \qquad H_*(X;R) \xrightarrow{\Delta_*} H_*(X;R) \otimes H_*(X;R) \xrightarrow{\mu_*} H_*(X;R).$$

A straightforward calculation shows that $(H_*(X;R), \mu_*, \Delta_*, i_*, c_*)$ and $(H^*(X;R), \Delta^*, \mu^*, c^*, i^*)$ are Hopf algebras over the field R.

2.5 The mod 2 Steenrod algebra

The natural transformation

$$Sq^i : H^n(X;\mathbb{F}_2) \longrightarrow H^{n+i}(X;\mathbb{F}_2)$$

where $i, n \geq 0$ and $H^*(X;\mathbb{F}_2)$ is the cohomology of the topological space X with coefficients in a field of characteristic 2, that satisfies the following axioms:

1) $Sq^0 = id$,

2) If $|x| = n$, then $Sq^n(x) = x^2$,

3) If $i > |x|$, then $Sq^i(x) = 0$,

4) $Sq^k(x \cdot y) = \sum_{r+s=k} Sq^r(x) \cdot Sq^s(y)$, (*Cartan formula*),

5) $Sq^a Sq^b = \sum_{j=0}^{[a/2]} \binom{b-1-j}{a-2j} Sq^{a+b-j} Sq^j$, (*Adem relation*), where $0 < a < 2b$,

6) Sq^1 is the *Bockstein* homomorphism β of the coefficient sequence

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{2id} \mathbb{Z}_4 \xrightarrow{i} \mathbb{Z}_2 \longrightarrow 0,$$

is called **Steenrod square**.

Let $R = \mathbb{F}_2$ and $M_i = \{0, Sq^i\}$, so it is clear that M_i is $\mathbb{F}_2$-module for all $i \geq 0$, $M_0 = \{0, id\} \approx \mathbb{F}_2$ and $M = \bigoplus_{n=0}^{\infty} M_n$ is graded $\mathbb{F}_2$-module. Now, define the tensor algebra of M which is denoted by $\Gamma(M)$ for a fixed k by the following way, set $\Gamma^0(M) = \mathbb{F}_2$, $\Gamma^1(M) = M$ and $\Gamma^k(M) = M \otimes \cdots \otimes M$, k-times. Then,

$$\Gamma(M) = \bigoplus_{k=0}^{\infty} \Gamma^k(M) = \bigoplus_{k=0}^{\infty} \left(\bigoplus_{i_1, \cdots, i_k = 0}^{\infty} M_{i_1} \otimes \cdots \otimes M_{i_k} \right).$$

Definition 2.5.1 (Steenrod algebra mod 2). The **Steenrod algebra mod 2**, is the connected graded associative $\mathbb{F}_2$-algebra $\Gamma(M)$, subject to *Adem* relations which is denoted by $\mathcal{A}(2)$. Formally, $\mathcal{A}(2) = \Gamma(M)/Q$, where Q is the ideal generated by *Adem* relation.

Definition 2.5.2 (Admissible monomial). A given vector $I = (i_1, \cdots, i_k)$ whose entries are the non-negative integers, is said to be **admissible** if its entries satisfy the conditions $i_{s-1} \geq 2i_s$, for $2 \leq s \leq k$, and $i_k \geq 1$. The corresponding monomial $Sq^I = Sq^{i_1} Sq^{i_2} \cdots Sq^{i_k}$ is called **admissible monomial**. By convention Sq^0 is admissible.

Theorem 2.5.3. *The set of all monomials Sq^I such that I is admissible, form a basis for $\mathcal{A}(2)$ as $\mathbb{F}_2$-module.*

Definition 2.5.4 (Decomposable and indecomposable *Steenrod* square). A *Steenrod* square Sq^i is called **decomposable** if $Sq^i = \sum_{t<i} d_t Sq^t$, such that d_t is a sequence of *Steenrod* squares. Otherwise, Sq^i is **indecomposable**.

Hence, Sq^i is decomposable if it can be written as a linear combination of monomials such that at least one of them contains Sq^t, and $t < i$.

Lemma 2.5.5. *Sq^i is indecomposable if, and only if, i is a power of 2.*

Theorem 2.5.6. *Sq^{2^t} for all $t \geq 0$ generate $\mathcal{A}(2)$ as an $\mathbb{F}_2$-algebra.*

Note that the indecomposable elements do not freely generate $\mathcal{A}(2)$; for instance, $Sq^1Sq^1 = 0$ and $Sq^2Sq^2 = Sq^3Sq^1 = Sq^1Sq^2Sq^1$.

We have introduced $\mathcal{A}(2)$ as an algebra over the field $\mathbb{F}_2$, now we consider it as a $\mathbb{F}_2$-Hopf algebra by defining the map on generators

$$\psi(Sq^k) = \sum_{i=0}^{k} Sq^{k-i} \otimes Sq^i,$$

that is extended to be a homomorphism of algebras which is considered as a coproduct of $\mathcal{A}(2)$. Hence,

$$\psi : \mathcal{A}(2) \longrightarrow \mathcal{A}(2) \otimes \mathcal{A}(2)$$

Theorem 2.5.7. *$\mathcal{A}(2)$ is a connected, biassociative and cocommutative graded Hopf algebra over $\mathbb{F}_2$.*

2.6 The Steenrod algebra mod p

The natural transformation

$$\mathcal{P}^i : H^n(X;\mathbb{F}_p) \longrightarrow H^{n+2i(p-1)}(X;\mathbb{F}_p),$$

for all integers $i, n \geq 0$ where $H^*(X;\mathbb{F}_p)$ is the cohomology of the topological space X with coefficients in a field of characteristic p is said to be ***Steenrod* reduced power**, if the following axioms are hold:

1) $\mathcal{P}^0 = id$,

2) $\mathcal{P}^n(x) = x^p$, if $|x| = 2n$,

3) $\mathcal{P}^n(x) = 0$, if $|x| < 2n$,

4) $\mathcal{P}^n(x \cdot y) = \sum_{i+j=n} Sq^i(x) \cdot Sq^j(y)$, (*Cartan formula*),

5) (*Adem relations*).

A-1) $\mathcal{P}^a\mathcal{P}^b = \sum_{j=0}^{[a/p]} (-1)^{a+j} \binom{(p-1)(b-j)-1}{a-jp} \mathcal{P}^{a+b-j}\mathcal{P}^j$, if $a < pb$,

A-2) $\mathcal{P}^a\beta\mathcal{P}^b = \sum_{j=0}^{[a/p]} (-1)^{a+j} \binom{(p-1)(b-j)}{a-jp} \beta\mathcal{P}^{a+b-j}\mathcal{P}^j +$

$$\sum_{j=0}^{[(a-1)/p]} (-1)^{a+j-1} \binom{(p-1)(b-j)-1}{a-jp-1} \mathcal{P}^{a+b-j}\beta\mathcal{P}^j, \qquad \text{if } a \leq b.$$

Now, let

$$\beta : H^n(X;\mathbb{F}_p) \longrightarrow H^{n+1}(X;\mathbb{F}_p),$$

be the *Bockstein* coboundary operator with coefficient sequence

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{pid} \mathbb{Z}_{p^2} \xrightarrow{i} \mathbb{Z}_p \longrightarrow 0.$$

Then, β is natural for mappings of spaces, $\beta^2 = 0$ and $\beta(xy) = \beta(x)y + (-1)^{|x|}x\beta(y)$. By the same techniques that have been used in mod 2 case can be used for this case as the following.

Definition 2.6.1 (The mod p Steenrod algebra). The ***Steenrod* algebra mod p** which is denoted by $\mathcal{A}(p)$ is the graded associative algebra over $\mathbb{F}_p$ generated by β of degree 1 and the *Steenrod* reduced power $\mathcal{P}^i, \forall i \geq 0$ of degree $2i(p-1)$, with respect to the $\beta^2 = 0$, $\mathcal{P}^0 = id$ and *Adem relations.*

Then, according to the construction of $\mathcal{A}(p)$, each monomial in $\mathcal{A}(p)$ might be given by the form

$$\beta^{j_0}\mathcal{P}^{i_1}\beta^{j_1}\cdots\mathcal{P}^{i_k}\beta^{j_k},$$

such that $j_m = 0, 1$ and $i_n = 1, 2, \cdots$, where $0 \leq m \leq k$ and $1 \leq n \leq k$. We need the following definitions and facts to show how the generators of $\mathcal{A}(p)$ are.

Definition 2.6.2 (Admissible monomial). A vector $I = (j_0, i_1, j_1, \cdots, i_k, j_k)$ is called **admissible** if its entries are non-negative integers and $i_n - j_n \geq i_{n+1}p$ for $1 \leq n \leq k-1$. If I is an admissible vector, $\mathcal{P}^I = \beta^{j_0}\mathcal{P}^{i_1}\beta^{j_1}\cdots\mathcal{P}^{i_k}\beta^{j_k}$ is called **admissible monomial**. $\mathcal{P}^0$ is an admissible monomial by convention.

Proposition 2.6.3. *$\mathcal{A}(p)$ is spanned by the admissible monomials, i.e. if $\theta \in \mathcal{A}(p)$, then θ is written as a linear combination of admissible monomials.*

Proposition 2.6.4. *The set of all admissible monomials is linearly independent.*

Obviously, the last two propositions implies the following theorem.

Theorem 2.6.5. *The admissible monomials form a basis for $\mathcal{A}(p)$ as a vector space over $\mathbb{F}_p$.*

As expected, the definition of decomposable and indecomposable are as same as in the mod 2 case.

Definition 2.6.6 (Decomposable and indecomposable *Steenrod* reduce power). Any $\mathcal{P}^i$ is said to be **indecomposable**, if it cannot be written as linear combination from factors i.e. $\mathcal{P}^i \neq \sum_{t<i} d_t\mathcal{P}^t$ where d_t is a sequence of *Steenrod* reduce power. Otherwise, $\mathcal{P}^i$ is called **decomposable**.

Lemma 2.6.7. *$\mathcal{P}^i$ is indecomposable if, and only if, $i = p^k$ for $k = 0, 1, \cdots$.*

Theorem 2.6.8. *$\mathcal{A}(p)$ as algebra over $\mathbb{F}_p$ is generated by β, $\mathcal{P}^0$ and $\mathcal{P}^{p^k}$ $\forall k \geq 0$.*

Now, consider the map on generators

$$\psi(\beta) = \beta \otimes id + id \otimes \beta,$$

and

$$\psi(\mathcal{P}^k) = \sum_{0 \le i \le k} \mathcal{P}^{k-i} \otimes \mathcal{P}^i$$

extends to a homomorphism of algebras which is represented the comultiplication map of $\mathbb{F}_p$-coalgebra $\mathcal{A}(p)$. Thus

$$\psi : \mathcal{A}(p) \longrightarrow \mathcal{A}(p) \otimes \mathcal{A}(p).$$

Theorem 2.6.9. *$\mathcal{A}(p)$ is a connected, biassociative and cocommutative graded $\mathbb{F}_p$-Hopf algebra.*

Chapter 3

Projective Spaces $\mathbb{F}P^n$

3.1 $\mathbb{R}P^n$, $\mathbb{C}P^n$ and $\mathbb{H}P^n$

3.1.1 Topological viewpoint

Let $\mathbb{F} = F_d$ to be one of topological fields $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$ (not necessary commutative). We denote by $d_{\mathbb{F}}$ to the dimension of the $\mathbb{R}$-algebra $\mathbb{F}$, and since $\mathbb{R} = \langle 1 \rangle, \mathbb{C} = \langle 1, i \rangle$ and $\mathbb{H} = \langle 1, i, j, k \rangle$; thus $d_{\mathbb{F}} = d = 1, 2$ or 4 respectively according as $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$. Define $\mathbb{F}^n$ to be the right vector space of *n-tuples* over $\mathbb{F}$, with the usual inner product $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i \bar{y}_i$, where $\mathbf{x} = (x_1, \cdots, x_n)$, $\mathbf{y} = (y_1, \cdots, y_n)$; $x_i, y_i \in \mathbb{F}$ and $\bar{y}_i$ is the conjugate of y_i, then $\mathbb{F}^n$ an inner product space, i.e. for $\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{y}_2 \in \mathbb{F}^n$, and $\lambda \in \mathbb{F}$.,

1. $\langle \mathbf{x}_1 \lambda, \mathbf{y}_1 \rangle = \langle \mathbf{x}_1, \mathbf{y}_1 \rangle \lambda$; $\quad \langle \mathbf{x}_1, \mathbf{y}_1 \lambda \rangle = \langle \mathbf{x}_1, \mathbf{y}_1 \rangle \bar{\lambda}$,
2. $\langle \mathbf{x}_1 + \mathbf{x}_2, \mathbf{y}_1 \rangle = \langle \mathbf{x}_1, \mathbf{y}_1 \rangle + \langle \mathbf{x}_2, \mathbf{y}_1 \rangle$,
3. $\langle \mathbf{x}_1, \mathbf{y}_1 + \mathbf{y}_2 \rangle = \langle \mathbf{x}_1, \mathbf{y}_1 \rangle + \langle \mathbf{x}_1, \mathbf{y}_2 \rangle$,
4. $\langle \mathbf{x}_1, \mathbf{y}_1 \rangle = \langle \overline{\mathbf{y}_1, \mathbf{x}_1} \rangle$.

Consider the following subspace from $\mathbb{F}$:

$$G_{\mathbb{F}} = \{u \in \mathbb{F} | u\bar{u} = 1\},$$

so that; $G_{\mathbb{R}} = S^0$, $G_{\mathbb{C}} = S^1$ and $G_{\mathbb{H}} = S^3$, moreover; $G_{\mathbb{F}}$ is a topological group. Consider also S^{dn-1} the unit sphere that is contained in $\mathbb{F}^n$ i.e.

$$S^{dn-1} = \{\mathbf{x} \in \mathbb{F}^n | \langle \mathbf{x}, \mathbf{x} \rangle = 1\}.$$

Now, consider the scalar multiplication that is define by $\mathbf{x} \cdot u = (x_1 u, \cdots, x_n u)$, such that $\mathbf{x} \in S^{dn-1}$ and $u \in G_{\mathbb{F}}$. Note that from the first property of the inner product we have $\langle \mathbf{x}u, \mathbf{x}u \rangle = \langle \mathbf{x}, \mathbf{x} \rangle u\bar{u} = 1$. Thus, the previous scalar multiplication preserves the definition of S^{dn-1}, for that reason we can define the following action;

$$\varphi : S^{dn-1} \times G_{\mathbb{F}} \longrightarrow S^{dn-1}, \qquad \varphi(\mathbf{x}, u) = \mathbf{x}u.$$

In this context, the group $G_\mathbb{F}$ acts on the right of S^{dn-1}, and since an action gives a partition and so an equivalence relation. We say that $\mathbf{x}$ and $\mathbf{y}$ are equivalent if there is an $u \in G_\mathbb{F}$ such that $\mathbf{y} = \mathbf{x} \cdot u$.

Definition 3.1.1 (Projective spaces). The quotient space $S^{dn-1}/\sim$, where $\sim$ is the equivalence relation that has been defined above, is said to be **(n-1)th real, complex** and **quaternionic projective space** according as the $\mathbb{F}$ is $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. It is denoted by $\mathbb{F}P^{n-1}$.

3.1.2 Algebraic definition

If we regard the equivalence relation $\sim$ as a relation among $\mathbb{F}^n$s vectors, that is; $v \sim u \iff u = \lambda v$, such that $\lambda \in \mathbb{F}$ and u, v are non-zero vector. Then the vectors of $\mathbb{F}^n$ are classified to a set of equivalence classes by this equivalence relation. We denoted by $[v]$ to the class of vectors containing vector v.

From the first glance we can see that the set of all vectors in $[v]$ are just multiples of v, that means; they are a vector space of dimension one with a single basis element v. From this we can define $\mathbb{F}P^{n-1}$ to be the set of all one dimensional vector subspaces from $\mathbb{F}^n$. In fact this definition is just particular case for $\mathbb{F}^n$. The general one is the following.

Definition 3.1.2 (Projective space of a vector space). The set of all one dimensional vector subspaces of a vector space V of dimension n over an arbitrary field F is said to be the **projective space of** V, and is denoted by $P^{n-1}(\mathbb{V})$.

Let V be an n-dimensional vector space equipped with the complete flag, namely; $V_1 \subset V_2 \subset \cdots \subset V_n$, and suppose $v_1, v_2, \cdots, v_n$ an adapted basis for V. Now, consider the algebraic definition of the projective space, we denote to the elements of this space by $[v]$ and we called the non-zero vector v the **representative vector** for the element $[v] \in P^{n-1}(\mathbb{V})$. Since V is an n-dimensional vector space, then v can be uniquely written as

$$v = x_1 v_1 + \cdots + x_n v_n$$

where $\{v_1, \cdots, v_n\}$ be a given basis for V. Therefore, the coefficients x_i where $i = 1, 2, \cdots n$ are uniquely determined, so we set $[x_1, x_2, \cdots, x_n] = [v]$. Note if λv is given to be another representative vector then $[\lambda v] = [v]$, similarly; $[\lambda x_1, \lambda x_2, \cdots, \lambda x_n] = [x_1, x_2, \cdots, x_n]$. The notation $[x_1, x_2, \cdots, x_n]$ are known a **homogeneous coordinate**. The reason behind construction of the homogeneous coordinate is the following.

To describe $\mathbb{P}^{n-1}(V)$, assume that W_n is given to be the subset from $\mathbb{P}^{n-1}(V)$ with homogeneous coordinates $[x_1, x_2, \cdots, x_n]$ such that $x_n \neq 0$, then each one of them can be rewritten as

$$\begin{aligned}[x_1, x_2, \cdots, x_n] =& [x_1/x_n, x_2/x_n, \cdots, 1], \\ =& [y_1, y_2, \cdots, y_{n-1}, 1] \cong V_{n-1}.\end{aligned}$$

However, this gives a part of $\mathbb{P}^n(V)$, because we do not describe the vectors whose corresponding homogeneous coordinates having the form $[x_1, x_2, \cdots, x_{n-1}, 0]$, but these are homogeneous coordinates to the corresponding vectors which are written by:

$$\hat{v} = x_1 v_1 + x_2 v_2 + \cdots + x_{n-1} v_{n-1},$$

it is clear that $\hat{v}$ is an element in $\mathbb{P}^{n-2}(V)$. Consequently,

$$\mathbb{P}^{n-1}(V) = V_{n-1} \cup \mathbb{P}^{n-2}(V).$$

3.1.3 Geometric description

Geometrically the previous equivalence relation can be regards as the equation of $\mathbb{F}$-line through the origin of $\mathbb{F}^n$, in other word; $l = \{\lambda \mathbf{x} | \lambda \in \mathbb{R}, \mathbb{C} \text{ or } \mathbb{H}, \text{ and } \mathbf{x} \in \mathbb{R}^n, \mathbb{C}^n \text{ or } \mathbb{H}^n\}$. Hence, we can define the projective space by the following way.

Definition 3.1.3 (Projective space). **The n-th real, complex quaternionic projective space** $\mathbb{F}P^n$ is the set of all $\mathbb{F}$-lines through the origin in the space $\mathbb{F}^{n+1}$. In that case,

$$\mathbb{F}P^n = \mathbb{F}^{n+1} - 0/\sim \qquad \text{such that} \qquad \mathbf{x} \sim \mathbf{y} \Longleftrightarrow \mathbf{x} = \lambda \mathbf{y}$$

where $\mathbf{x}, \mathbf{y} \in \mathbb{F}^{n+1}$ and $\lambda \in \mathbb{F}$.

3.2 Infinite complex projective space

As we have seen that $\mathbb{C}P^m = S^{2m+1}/S^1$. Let $[z_0, z_1, \cdots, z_m]$ an element in $\mathbb{C}P^m$, then we can define the inclusion map $i : \mathbb{C}P^m \longrightarrow \mathbb{C}P^{m+1}$ by

$$i([z_0, z_1, \cdots, z_m]) = [z_0, z_1, \cdots, z_m, 0].$$

The **infinite complex projective space** which is denoted by $\mathbb{C}P^\infty$ is define to be the union of all finite complex projective spaces

$$\mathbb{C}P^\infty = \bigcup_{m=0}^{\infty} \mathbb{C}P^m.$$

We denote by $(\mathbb{C}P^\infty)^k$ to the *Cartesian* product of k copies of infinite complex projective spaces $\mathbb{C}P^\infty \times \cdots \times \mathbb{C}P^\infty$.

The CW-complex structure of $\mathbb{C}P^\infty$ is

$$\mathbb{C}P^\infty = e^0 \cup_f e^2 \cup_f \cdots \cup_f e^{2m} \cup_f \cdots \tag{3.1}$$

i.e a single cell in each dimension $2i$ for $i \geq 0$ and no cells in odd dimension. This cell structure can be obtained by induction and the following fact.

Theorem 3.2.1. *For each integer $n > 0$, $\mathbb{C}P^n = \mathbb{C}P^{n-1} \cup_f e^{2n}$ such that the attaching map $f : S^{2n-1} \longrightarrow \mathbb{C}P^{n-1}$ is given by $f(z_0, \cdots, z_{n-1}) = [z_0, \cdots, z_{n-1}]$.*

Proof. Sketch of proof, define

$$h : \mathbb{C}P^{n-1} \cup_f e^{2n} \longrightarrow \mathbb{C}P^n,$$

by $h([z_0, \cdots, z_{n-1}]) = [z_0, \cdots, z_{n-1}, 0]$ if $[z_0, \cdots, z_{n-1}] \in \mathbb{C}P^{n-1}$, and for $(z_0, \cdots, z_{n-1}) \in e^{2n}$ take $h(z_0, \cdots, z_{n-1}) = [z_0, \cdots, z_{n-1}, \sqrt{1 - |z_0|^2 - \cdots - |z_{n-1}|^2}]$. First, h is a well defined map, the continuity of h is clear since it is a continuous on $\mathbb{C}P^{n-1}$ and e^{2n}. Furthermore, because $\mathbb{C}P^{n-1}$ and e^{2n} are both compact, implies $\mathbb{C}P^{n-1} \cup_f e^{2n}$ is a compact. Finally, $\mathbb{C}P^n$ is a *Hausdorff* topological space and h is a continuous bijective, then h is a homeomorphism. □

Regarding the cohomology and the homology of $\mathbb{C}P^\infty$, according to 3.1 we can deduce the n-dimensional celluar chains which are given by

$$C_n(\mathbb{C}P^\infty) = \begin{cases} je^{2n} \cong \mathbb{Z}, & \text{if } n \text{ is even, such that } j \in \mathbb{Z}; \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

By the same way we can obtain the n-dimensional celluar cochains which are

$$C^n(\mathbb{C}P^\infty) = \begin{cases} 0, & \text{if } n \text{ is odd;} \\ je^{2n} \cong \mathbb{Z}, & \text{if } n \text{ is even, such that } j \in \mathbb{Z}. \end{cases}$$

While, the boundary and the coboundary operators of such sequences are automatically defined to be the zero maps, since they are homomorphisms from or to trivial.

Now, assume $\mathbb{F}$ an arbitrary field or a commutative ring with unit, then the previous chain complex and cochain complex of $\mathbb{C}P^\infty$ implies the following sequences

$$\cdots \longrightarrow 0 \xrightarrow{d_{n+1}} \mathbb{F} \xrightarrow{d_n} 0 \xrightarrow{d_{n-1}} \mathbb{F} \longrightarrow \cdots \longrightarrow \mathbb{F} \xrightarrow{d_2} 0 \xrightarrow{d_1} \mathbb{F}.$$

$$\cdots \longleftarrow 0 \xleftarrow{d^{n+1}} \mathbb{F} \xleftarrow{d^n} 0 \xleftarrow{d^{n-1}} \mathbb{F} \longleftarrow \cdots \longleftarrow \mathbb{F} \xleftarrow{d^2} 0 \xleftarrow{d^1} \mathbb{F}.$$

Thus

$$H_n(\mathbb{C}P^\infty; \mathbb{F}) = \begin{cases} \mathbb{F}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd ,} \end{cases}$$

and

$$H^n(\mathbb{C}P^\infty; \mathbb{F}) = \begin{cases} 0, & \text{if } n \text{ is odd ;} \\ \mathbb{F}, & \text{if } n \text{ is even.} \end{cases}$$

Theorem 3.2.2. *The ring $H^*(\mathbb{C}P^\infty;\mathbb{F}_p) \cong \mathbb{F}_p[x]$, where x has degree 2.*

Proof. Sketch of proof. If x is taken to be a generator for $H^2(\mathbb{C}P^\infty;\mathbb{F}_p)$, then the non-zero element $x^2 = x \smile x \in H^4(\mathbb{C}P^\infty;\mathbb{F}_p)$ can be chosen to be a generator for $H^4(\mathbb{C}P^\infty;\mathbb{F}_p)$, and so $x^n = x \smile \cdots \smile x$ (n-times) is the non-zero element that generates $H^{2n}(\mathbb{C}P^\infty;\mathbb{F}_p)$. Thus as graded algebra over $\mathbb{F}_p$, $H^*(\mathbb{C}P^\infty;\mathbb{F}_p) \cong \mathbb{F}_p[x]$. □

Recall that if $\mathbb{F}$ is a field or $H^i(X;\mathbb{F})$ is free module for $\mathbb{F}$, then from the *Künneth* formula for cohomology we have $H^*(X \times X;\mathbb{F}) \approx H^*(X;\mathbb{F}) \otimes H^*(X;\mathbb{F})$, so that

$$H^*(\mathbb{C}P^\infty \times \mathbb{C}P^\infty;\mathbb{F}_p) \approx H^*(\mathbb{C}P^\infty;\mathbb{F}_p) \otimes H^*(\mathbb{C}P^\infty;\mathbb{F}_p),$$

and from tensor product properties we have $\mathbb{F}_p[x] \otimes \mathbb{F}_p[y] \approx \mathbb{F}_p[x,y]$. From that we can deduce, the cohomology of the *Cartesian* product of k-folds of infinite complex projective spaces with coefficients in a field of characteristic p is a polynomial algebra over that field in k-variables, i.e.

$$H^*(\mathbb{C}P^\infty \times \cdots \times \mathbb{C}P^\infty;\mathbb{F}_p) \approx \mathbb{F}_p[x_1, x_2, \cdots, x_k], \tag{3.2}$$

such that each variable x_i has dimension 2, where $i = 1, \cdots, k$.

Now, we wish to investigate the action of $\mathcal{A}(p)$ on $H^*((\mathbb{C}P^\infty)^k;\mathbb{F}_p)$ which is easily described when we know the action of *Steenrod* reduce power $\mathcal{P}^i$ on the generators x_j of $H^*((\mathbb{C}P^\infty)^k;\mathbb{F}_p)$. Then *Cartan* argument illustrates that if we have two or more generators x_1, x_2, x_3, then $\mathcal{P}^i(x_1x_2x_3) = \sum_{r+s+t=i} \mathcal{P}^r(x_1)\mathcal{P}^s(x_2)\mathcal{P}^t(x_3)$. The following lemma shows the action of $\mathcal{P}^i$ and β on a generator x_j.

Lemma 3.2.3. *Let $x_j \in H^2((\mathbb{C}P^\infty)^k;\mathbb{F}_p)$, then for an integer $k > 0$,*

a) $\beta(x_j^k) = 0$,

b) $\mathcal{P}^i(x_j^k) = \binom{k}{i} x_j^{k+i(p-1)}$ *where the binomial coefficient is reduced* mod$p$.

Proof. a) From the definition of *Bockstein* homomorphism (chapter two section 6) we have $\beta(x_j^k) = (\beta(x_j))^k$ and

$$\beta : H^n(X;\mathbb{F}_p) \longrightarrow H^{n+1}(X;\mathbb{F}_p),$$

so since $|x_j| = 2$ this implies $|\beta(x_j)| = 3$. But the construction of $H^*(\mathbb{C}P^\infty;\mathbb{F}_p)$ shows that $H^3(\mathbb{C}P^\infty;\mathbb{F}_p) = 0$. Thus $\beta(x_j) = 0$ for any component j in the *Cartesian* product. Hence $\beta(x_j^k) = (\beta(x_j))^k = 0$.

b) See [24] for the proof of this part of the lemma. An alternative proof for this fact is, if $i > k$ then the result holds from axiom 3 (2.6). When $i \leq k$, then applying *Cartan* formula implies this

$$\mathcal{P}^i(x_j^k) = \mathcal{P}^i(\overbrace{x_j x_j \cdots x_j}^{k-times}) = \sum_{t_1+\cdots+t_k=i} \mathcal{P}^{t_1}(x_j)\cdots\mathcal{P}^{t_k}(x_j).$$

since $k \geq i$, in the string $t_1 + t_2 + \cdots + t_k = i$ there are at least $k - i$ of $t_n = 0$ such that $n = \{1, 2, \cdots, k\}$, but we do not know which they are. Therefore, we need to pick out i of t_n (which are may be non-zero) from k, thus the previous expression can be reduced and rearranged as follows

$$\mathcal{P}^i(x_j^k) = \binom{k}{i} x_j^{k-i} \sum_{t_{n_1}+\cdots+t_{n_i}=i} \mathcal{P}^{t_{n_1}}(x_j) \cdots \mathcal{P}^{t_{n_i}}(x_j).$$

Now unless $t_{n_1} = t_{n_2} = \cdots = t_{n_i} = 1$, the right hand side of the previous relation is zero according to axiom 3 (2.6), hence we get from axiom 2 (2.6) that

$$\sum_{t_{n_1}+\cdots+t_{n_i}=i} \mathcal{P}^{t_{n_1}}(x_j) \cdots \mathcal{P}^{t_{n_i}}(x_j) = x_j^{ip},$$

so the lemma is proven. □

As we have seen in above discussion that $H^*(\mathbb{C}P^\infty; \mathbb{F}_p)$ is an $\mathbb{F}_p$-algebra. To view this algebra as an *Hopf* algebra we need to define a coproduct on $H^*(\mathbb{C}P^\infty; \mathbb{F}_p)$ which is given by $\Delta(x) = x \otimes 1 + 1 \otimes x$.

The homology $H_*(\mathbb{C}P^\infty; \mathbb{F}_p)$ may be regarded as a dual of the *Hopf* algebra $H^*(\mathbb{C}P^\infty; \mathbb{F}_p)$. In this case the additional structure is carried, while the product in $H_*(\mathbb{C}P^\infty; \mathbb{F}_p)$ induces from the coproduct of $H^*(\mathbb{C}P^\infty; \mathbb{F}_p)$. In other word, if Δ is the comultiplication map, then $\Delta : H^*(\mathbb{C}P^\infty; \mathbb{F}_p) \longrightarrow H^*(\mathbb{C}P^\infty; \mathbb{F}_p) \otimes H^*(\mathbb{C}P^\infty; \mathbb{F}_p)$. The dualisation of that map gives the following one $\Delta^* : H_*(\mathbb{C}P^\infty; \mathbb{F}_p) \otimes H_*(\mathbb{C}P^\infty; \mathbb{F}_p) \longrightarrow H_*(\mathbb{C}P^\infty; \mathbb{F}_p)$, so our aim is finding $\Delta^*(x \otimes y)$ which is denoted by $x \cdot y$, from the known one Δ.

We treat a basis $\{1, v_1, v_2, \cdots\}$ of $H_*(\mathbb{C}P^\infty; \mathbb{F}_p)$ such that $v_n \in H_{2n}(\mathbb{C}P^\infty; \mathbb{F}_p)$ that satisfies

$$\langle v_n, x^m \rangle = \begin{cases} 1, & \text{if } m = n; \\ 0, & \text{otherwise.} \end{cases}$$

where x^m is a basis element in $H^{2m}(\mathbb{C}P^\infty; \mathbb{F}_p)$.

Assume that $v_j \cdot v_k$ is dual to taking the coproduct in $H^*(\mathbb{C}P^\infty; \mathbb{F}_p)$ which is given by:

$$\Delta(x) = x \otimes 1 + 1 \otimes x, \tag{3.3}$$

and then

$$\Delta(x^m) = \sum_{i=0}^{m} \binom{m}{i} x^i \otimes x^{m-i},$$

so $v_j \cdot v_k$ is the element in degree $2j + 2k$ (In fact $H_{2(j+k)}(\mathbb{C}P^\infty; \mathbb{F}_p) = \{\xi v_{j+k} : \xi \in \mathbb{F}_p\}$) that satisfies

$$\langle v_j \cdot v_k, x^m \rangle = \langle v_j \otimes v_k, \Delta(x^m) \rangle$$

since $v_j \cdot v_k$ has degree $2(j+k)$, this will be non-zero only if $m = j+k$ in which case

$$\begin{aligned}\langle v_j \cdot v_k, x^m\rangle =& \langle v_j \otimes v_k, \Delta(x^m)\rangle \\ =& \langle v_j \otimes v_k, \sum_{i=0}^{j+k} \binom{j+k}{i} x^i \otimes x^{j+k-i}\rangle \\ =& \langle v_j \otimes v_k, \binom{j+k}{j} x^j \otimes x^k\rangle \\ =& \binom{j+k}{j}.\end{aligned}$$

If $j+k < p$, then $\binom{j+k}{j} \not\equiv 0 \bmod p$. Thus

$$v_j \cdot v_k = \binom{j+k}{j} v_{j+k}, \tag{3.4}$$

so easily someone can check that the multiplication which is derived in equation 3.4 is a commutative and associative.

For that we can interpret the basis $\{1, v_1, v_2, \cdots\}$ of $H_*(\mathbb{C}P^\infty; \mathbb{F}_p)$ to other language as follows. We denote by $v_1^0 = 1$, $v_1 = v_1$ and by $v_1^r = v_1 \cdot \cdots \cdot v_1$ (r-times) where $r < p$, for example; $v_1^2 = v_1 \cdot v_1 = 2v_2$, by using the induction and 3.4 we get; if $v_1^{r-1} = (r-1)! v_{r-1}$, then $v_1^r = r! v_r$. Then v_1 can be introduced as a generator for $H_{T_1}(\mathbb{C}P^\infty; \mathbb{F}_p)$ where $T_1 \leq 2p-2$.

The reason why we do not extend v_1 to be a generator for whole $H_*(\mathbb{C}P^\infty; \mathbb{F}_p)$ like x in the cohomology case is because $v_1^p = p! v_p \equiv 0 \bmod p$. That is, we need to pick a generator for $H_{2p}(\mathbb{C}P^\infty; \mathbb{F}_p)$. Set v_p to be a generator for $H_{2p}(\mathbb{C}P^\infty; \mathbb{F}_p)$. Using the same notations that have been used in previous paragraph, observe that according to *Lucas's* theorem we have $v_{ip} \cdot v_{jp} = \binom{i+j}{j} v_{(i+j)p}$ and so $v_p^r = r! v_{rp}$, implies that $\{v_1, v_p\}$ can be regarded as generators for $H_{T_2}(\mathbb{C}P^\infty; \mathbb{F}_p)$ if we exclude v_1^p where $T_2 \leq 2(p^2-1)$.

Repeating the same argument inducts that the set $\{v_1, v_p, v_{p^2}, \cdots\}$ such that $v_{p^n}^p = 0$ for all integer $n \geq 0$ generates $H_*(\mathbb{C}P^\infty; \mathbb{F}_p)$, in other word; $H_*(\mathbb{C}P^\infty; \mathbb{F}_p)$ is a truncated polynomial algebra over $\mathbb{F}_p$ that generates by v_{p^n}, $\forall n \geq 0$ which are truncated at power p for each generator i.e.

$$H_*(\mathbb{C}P^\infty; \mathbb{F}_p) = \mathbb{F}_p[v_1, v_p, \ldots]/[v_1^p, v_p^p, \ldots].$$

Similarly, applying *Künneth* formula for homology implies

$$H_*((\mathbb{C}P^\infty)^k; \mathbb{F}_p) = H_*(\mathbb{C}P^\infty; \mathbb{F}_p) \otimes \cdots \otimes H_*(\mathbb{C}P^\infty; \mathbb{F}_p) \qquad (k\text{-times})$$

and from the following property of tensor product

$$\mathbb{F}_p[x_1, x_p, \ldots]/[x_1^p, x_p^p, \ldots] \otimes \mathbb{F}_p[y_1, y_p, \ldots]/[y_1^p, y_p^p, \ldots] = \mathbb{F}_p[x_1, y_1, x_p, y_p \ldots]/[x_1^p, y_1^p, x_p^p, y_p^p, \ldots]$$

we deduce the $\mathbb{F}_p$-homology of the k-copies of infinite complex projective space

$$H_*((\mathbb{C}P^\infty)^k;\mathbb{F}_p) = \frac{\mathbb{F}_p[(x_1)_1,\cdots,(x_k)_1,(x_1)_p,\ldots,(x_k)_p,\cdots]}{[(x_1)_1^p,\cdots,(x_k)_1^p,(x_1)_p^p,\ldots,(x_k)_p^p,\cdots]}. \tag{3.5}$$

3.3 The action of $A(p)$ on $H_*((\mathbb{C}P^\infty)^k;\mathbb{F}_p)$

The same ideas that have been used to derive the multiplication map of $H_*(\mathbb{C}P^\infty;\mathbb{F}_p)$ which is induced by the comultiplication of $H^*(\mathbb{C}P^\infty;\mathbb{F}_p)$, can be developed here. From the left action of the opposite algebra $\mathcal{A}^{op}(p)$ of *Steenrod* algebra $\mathcal{A}(p)$

$$\mathcal{P}^i : H^*(\mathbb{C}P^\infty;\mathbb{F}_p) \longrightarrow H^*(\mathbb{C}P^\infty;\mathbb{F}_p).$$

We can determine the action of the operations dual, to be the right action of $\mathcal{A}(p)$ on $H_*(\mathbb{C}P^\infty;\mathbb{F}_p)$ which is defined by

$$\langle x^m, (v_k)\mathcal{P}^i\rangle = \langle \mathcal{P}^i(x^m), v_k\rangle$$

where $x^m \in H^*(\mathbb{C}P^\infty;\mathbb{F}_p), v_k \in H_*(\mathbb{C}P^\infty;\mathbb{F}_p)$ and $\mathcal{P}^i \in \mathcal{A}^{op}(p)$. We denote to $(v_k)\mathcal{P}^i$ by $\mathcal{P}_i(v_k)$ to keep in our mind this is the action of the dual operation of $\mathcal{P}^i$. In this context,

$$\mathcal{P}_i : H_*(\mathbb{C}P^\infty;\mathbb{F}_p) \longrightarrow H_*(\mathbb{C}P^\infty;\mathbb{F}_p).$$

Furthermore, we can detect *Cartan* argument conduct for these new operations. Finally, these two ideas enable us to describe the right action of the of *Steenrod* algebra over $\mathbb{F}_p$ on $H_*((\mathbb{C}P^\infty)^k;\mathbb{F}_p)$

The following lemma is the same as lemma 3.2.3 but in dual case, in this lemma we will show the action of $\mathcal{P}_i$ on the basis $\{1, v_1, v_2, \cdots\}$ of $H_*(\mathbb{C}P^\infty;\mathbb{F}_p)$. The proposition that follows the lemma is devoted to the action of $\mathcal{P}_i$ on the the generators $v_{p^r}^n$ where $r \geq 0$ and $0 \leq n \leq p-1$ of $H_*(\mathbb{C}P^\infty;\mathbb{F}_p)$.

Lemma 3.3.1. *For any integers $i, k > 0$ and $v_k \in H_{2k}(\mathbb{C}P^\infty;\mathbb{F}_p)$ then*

$$\mathcal{P}_i(v_k) = \binom{k-i(p-1)}{i} v_{k-i(p-1)}.$$

where the binomial coefficient is reduced mod$p$.

Proof. From the action of $\mathcal{P}^i$ on an element $x^m \in H^{2m}(\mathbb{C}P^\infty;\mathbb{F}_p)$ (lemma 3.2.3), we will find the action of its dual $\mathcal{P}_i$ on v_k. Recall $\langle x^m, v_k\rangle = 1$ when $k = m$ and 0 if $k \neq m$. That is

$$\begin{aligned}\langle x^m, \mathcal{P}_i(v_k)\rangle =&\langle \mathcal{P}^i(x^m), v_k\rangle,\\ =&\langle \binom{m}{i} x^{m+i(p-1)}, v_k\rangle,\\ =&\binom{m}{i}\langle x^{m+i(p-1)}, v_k\rangle,\\ =&\binom{m}{i}\langle x^m, v_{k-i(p-1)}\rangle,\\ =&\binom{k-i(p-1)}{i}\langle x^m, v_{k-i(p-1)}\rangle.\end{aligned}$$

Thus

$$\mathcal{P}_i(v_k) = \binom{k-i(p-1)}{i} v_{k-i(p-1)}.$$

□

From the first glance for lemma 3.3.1 we see that if $k \leq i(p-1)$, then $\mathcal{P}_i(v_k) = 0$.

Proposition 3.3.2. *For t, r are non-negative integers and $0 \leq n \leq p-1$.*

$$\mathcal{P}_1(v_{p^r}^n) = \begin{cases} n v_1 v_p^{n-1}, & \text{if } r = 1;\\ (-1)^{r-1} n v_1 v_p^{p-1}\cdots v_{p^{r-1}}^{p-1} v_{p^r}^{n-1}, & \text{if } r > 1.\end{cases}$$

$$\mathcal{P}_{p^t}(v_{p^r}^n) = \begin{cases} 0, & \text{if } t > r-1;\\ n v_{p^{r-1}} v_{p^r}^{n-1}, & \text{if } t = r-1;\\ (-1)^{r-t-1} n v_{p^t} v_{p^{t+1}}^{p-1}\cdots v_{p^{r-1}}^{p-1} v_{p^r}^{n-1}, & \text{if } t < r-1.\end{cases}$$

Before starting the proof of the proposition we need the following preliminaries:

Definition 3.3.3. Any positive integers n and m are said to be complement to each other with respect to the p-adic expansion if $\forall i$ either $a_i = 0$ or $b_i = 0$, where a_i, b_i are the coefficients of p^i in the p-adic expansion of n and m respectively. We said m has p-adic expansion complement to the p-adic expansion of m or conversely.

Lemma 3.3.4. *Let i and j are positive integers, such that i is complement to j with respect to the p-adic expansion, then $v_i\ v_j = v_{i+j}$.*

Proof. Assume that $i = a_0 + a_1 p + \cdots + a_n p^n$ and $j = b_0 + b_1 p + \cdots + b_m p^m$ are the p-adic expansion for i and j respectively. Take $t = max(n, m)$ since i has p-adic expansion complement to j, then easily we infer the p-adic expansion of $i + j$ which is given by $i + j = (a_0 + b_0) + (a_1 + b_1)p + \cdots + (a_t + b_t)p^t$. Now, applying *Lucas's* theorem to calculate the following binomial coefficient, if $t = n$ implies

$$\binom{i+j}{i} = \binom{a_0+b_0}{a_0}\binom{a_1+b_1}{a_1}\cdots\binom{a_n+b_n}{a_n} \equiv 1 \bmod p,$$

because each binomial coefficient in the right hand side is written by either $\binom{a_k}{a_k} = 1$ or by $\binom{b_k}{0} = 1$ where $0 \le k \le n$. Thus, $v_i v_j = \binom{i+j}{i} v_{i+j} = v_{i+j}$. Similarly, if $t = m$, then we can use the same argument, so the lemma is proven. □

Corollary 3.3.5. *For any positive integer i, $v_i = v_{a_0} v_{a_1 p} v_{a_2 p^2} \cdots v_{a_n p^n}$, where $a_0, a_1, \cdots, a_n$ are the coefficients of the p-adic expansion of i.*

Proof. From the assumption of the corollary we have $v_i = v_{a_0 + a_1 p + a_2 p^2 \cdots + a_n p^n}$. Immediately, from the previous lemma we get the result, just we need to observe that each component of any p-adic expansion is complement to the other components with respect to the p-adic expansion. □

During the following proof we will use the corollary 3.3.5 without comment.

Proof. [proposition 3.3.2] In fact, lemma 3.3.1, the relation $v_{p^r}^n = n! v_{np^r}$ and *Lucas's* theorem are the keys of the proof of this proposition. Starting with $\mathcal{P}_1(v_{p^r}^n)$ when $r = 1$, then

$$\begin{aligned}
\mathcal{P}_1(v_p^n) = \mathcal{P}_1(n! v_{np}) =& n! \mathcal{P}_1(v_{np}) \\
=& n! \binom{np - (p-1)}{1} v_{np-(p-1)} \\
=& n! \binom{1}{1} \binom{n-1}{0} v_{1+(n-1)p} \\
=& n! v_1 v_{(n-1)p} \\
=& \frac{n!}{(n-1)!} v_1 v_p^{n-1} \\
=& n v_1 v_p^{n-1}
\end{aligned}$$

If $r > 1$, then $\mathcal{P}_1(v_{p^r}^n) = n! \binom{np^r - (p-1)}{1} v_{np^r - (p-1)}$, but the p-adic expansion of $np^r - (p-1)$ is given by $np^r - (p-1) = 1 + (p-1)p + (p-1)p^2 + \cdots + (p-1)p^{r-1} + (n-1)p^r$, so that;

$$\begin{aligned}
\mathcal{P}_1(v_{p^r}^n) =& n! \binom{1}{1} \binom{p-1}{0} \binom{p-1}{0} \cdots \binom{p-1}{0} \binom{n-1}{0} v_{1+(p-1)p+(p-1)p^2+\cdots+(p-1)p^{r-1}+(n-1)p^r} \\
=& n! v_1 v_{(p-1)p} v_{(p-1)p^2} \cdots v_{(p-1)p^{r-1}} v_{(n-1)p^r}
\end{aligned}$$

Now, using the fact $v_{(p-1)p^s} = \frac{1}{(p-1)!} v_{p^s}^{p-1}$ for $1 \le s \le r-1$, and *Wilson's* Theorem $(p-1)! = -1$, gives

$$\mathcal{P}_1(v_{p^r}^n) = (-1)^{r-1} n v_1 v_p^{p-1} v_{p^2}^{p-1} \cdots v_{p^{r-1}}^{p-1} v_{p^r}^{n-1}.$$

Turning to the case $\mathcal{P}_{p^t}(v_{p^r}^n) = n! \binom{np^r - p^t(p-1)}{p^t} v_{np^r - p^t(p-1)}$. Firstly, when $t > r-1$, then $np^r - p^t(p-1) \le 0$, so that; $\mathcal{P}_{p^t}(v_{p^r}^n) = 0$. Secondly, if $t = {}^{p-1}_{p^{r-1}} v_{p^r}^{n-1}$ ıen

$$\begin{aligned}
\mathcal{P}_{p^t}(v_{p^r}^n) = n! \mathcal{P}_{p^{r-1}}(v_{p^r}^n) =& n! \binom{np^r - p^{r-1}(p-1)}{p^{r-1}} v_{np^r - p^{r-1}(p-1)} \\
=& n! \binom{1}{1} \binom{n-1}{0} v_{p^{r-1}+(n-1)p^r} \\
=& n v_{p^{r-1}} v_{p^r}^{n-1}.
\end{aligned}$$

Finally, when $t < r-1$, so $\mathcal{P}_{p^t}(v_{p^r}^n) = n!\binom{np^r-p^t(p-1)}{p^t}v_{np^r-p^t(p-1)}$, however; the p-adic expansion of $np^r - p^t(p-1) = p^t + (p-1)p^{t+1} + (p-1)p^{t+2} + \cdots + (p-1)p^{r-1} + (n-1)p^r$, implies

$$\begin{aligned}\mathcal{P}_{p^t}(v_{p^r}^n) =& n!\binom{np^r - p^t(p-1)}{p^t}v_{np^r-p^t(p-1)}\\ =& n!\binom{1}{1}\binom{p-1}{0}\binom{p-1}{0}\cdots\binom{p-1}{0}\binom{n-1}{0}v_{p^t+(p-1)p^{t+1}+\cdots+(p-1)p^{r-1}+(n-1)p^r}\\ =& n!v_{p^t}v_{(p-1)p^{t+1}}v_{(p-1)p^{t+2}}\cdots v_{(p-1)p^{r-1}}v_{(n-1)p^r}\\ =& (-1)^{r-t-1}nv_{p^t}v_{p^{t+1}}^{p-1}v_{p^{t+2}}^{p-1}\cdots v_{p^{r-1}}^{p-1}v_{p^r}^{n-1}.\end{aligned}$$

□

While, *Cartan* argument for the dual case is constructed by the following way:

$$\begin{aligned}\langle\mathcal{P}_i(u\otimes v), x\otimes y\rangle =& \langle u\otimes v, \mathcal{P}^i(x\otimes y)\rangle\\ =& \langle u\otimes v, \sum_{n=0}^{i}\mathcal{P}^{i-n}(x)\otimes\mathcal{P}^n(y)\rangle\\ =& \sum_{n=0}^{i}\langle u\otimes v, \mathcal{P}^{i-n}(x)\otimes\mathcal{P}^n(y)\rangle\\ =& \sum_{n=0}^{i}\langle u, \mathcal{P}^{i-n}(x)\rangle\langle v, \mathcal{P}^n(y)\rangle\\ =& \sum_{n=0}^{i}\langle\mathcal{P}_{i-n}(u), x\rangle\langle\mathcal{P}_n(v), y\rangle\\ =& \sum_{n=0}^{i}\langle\mathcal{P}_{i-n}(u)\otimes\mathcal{P}_n(v), x\otimes y\rangle\\ =& \langle\sum_{n=0}^{i}\mathcal{P}_{i-n}(u)\otimes\mathcal{P}_n(v), x\otimes y\rangle,\end{aligned}$$

therefore; $\mathcal{P}_i(u\otimes v) = \sum_{n=0}^{i}\mathcal{P}_{i-n}(u)\otimes\mathcal{P}_n(v)$. Now, using the following isomorphism on the generators $\alpha(u_r\otimes v_s) = u_rv_s$ which have been used implicitly, we get $\mathcal{P}_i(uv) = \sum_{n=0}^{i}\mathcal{P}_{i-n}(u)\mathcal{P}_n(v)$.

Part II

Annihilated Elements $M_*(k)$ and the Subring of Lines $L_*(k)$.

Chapter 4

On $M_*(k)$ and $M^*(k)$

4.1 Motivation

Let $H_*(k)$ be the graded truncated polynomial algebra over $\mathbb{F}_p$ where p is an odd prime number, which is defined in relation 3.5. That is to say, $H_*(k) = \bigotimes_{i=1}^k H(x_i)$ where $H(x_i) = \mathbb{F}_p[(x_i)_1, (x_i)_p, \dots]/[(x_i)_1^p, (x_i)_p^p, \dots]$, and from the previous chapter we have seen that $H_*(k) \cong H_*(\underbrace{\mathbb{C}P^\infty \times \cdots \times \mathbb{C}P^\infty}_{k-times}; \mathbb{F}_p)$. Moreover, *Steenrod* algebra mod p, which is denoted by $\mathcal{A}(p)$ has an action on the right of $H_*((\mathbb{C}P^\infty)^k; \mathbb{F}_p)$, thus on $H_*(k)$ given by proposition 3.3.2] and *Cartan* formula. That is $\mathcal{A}^*(p) \otimes H_*(k) \longrightarrow H_*(k)$, this action allows us to view $H_*((\mathbb{C}P^\infty)^k; \mathbb{F}_p)$ as an algebra over *Hopf* algebra $\mathcal{A}^*(p)$.

The main object in our study is the ring $M_*(k)$ which consists of the elements of $H_*(k)$ which are mapped to zero by all elements of strictly positive degree of $\mathcal{A}(p)$. In other word, $M_*(k)$ is obtained from the intersection of $Ker\theta$ for all $\theta \in \mathcal{A}^+(p)$. According to [6] we can reformulate this problem as follows. From *Steenrod* algebra $\mathcal{A}(p)$ properties, we need to consider the action of (the dual operations) $\mathcal{P}_j$ and β^* which are defined in chapter 3.3 previously. Lemma 3.2.3.a shows that *Bockstein* homomorphism acts trivially on $H^*((\mathbb{C}P^\infty)^k; \mathbb{F}_p)$, by duality the right action of *Bockstein* homomorphism β also trivial on $H_*(k)$, so $Ker\beta^* = H_*(k)$, thus we do not need to regard the action of β^*.

On the other hand, if β is disregarded then the remaining generators for $\mathcal{A}(p)$ are $\mathcal{P}^{p^k}$ where $k = 0, 1, 2, \cdots$, in addition; $\mathcal{P}^0 = 1$. Obviously, the reason why $\mathcal{P}^0$ is excluded is $Ker\mathcal{P}^0 = 0$ this implies $M_*(k) = 0$. For that we need only to consider the right action of $\mathcal{P}^{p^k}$ which we denote by $\mathcal{P}_{p^k}$ for the same values of k. Therefore, the object $M_*(k)$ now obviously means

$$H_d(k) \supseteq M_d(k) = \bigcap_{t \geq 0} Ker\mathcal{P}_{p^t}.$$

The problem of calculating the subalgebra of $H_*(k)$, which is denoted by $M_*(k)$ that contains the annihilated elements by the set of all $\mathcal{P}_{p^k}$, where $k = 0, 1, \cdots$ important problem for many different aspects, for the following reasons:

- It is the corresponding (dual) problem to what is known the **hit problem**. The problem of finding $M^*(k) = P(k)/\mathcal{A}_p^+ P(k)$, where $P(k)$ is the polynomial algebra in k-variables, $\mathcal{A}_p^+$ is the augmentation ideal in *Steenrod* algebra $\mathcal{A}(p)$, and $\mathcal{A}_p^+ P(k)$ is the notation of the set of all elements in the image of $\mathcal{A}_p^+$ that are called **hits**. However, $M_*(k)$ has stronger structure than $M^*(k)$ because the former is subalgebra of $H_*(k)$, the object $M^*(k)$ has various application in many mathematics subjects such stable homotopy theory, representation theory, and in from where this problem had been arisen, that is; finding the set of minimal generators for $H^*(BV, \mathbb{F}_p)$ as $\mathcal{A}(p)$-module [14]. For more details see [9].

- The second reason emerges from Wood's observation in [29] for the representation of $GL(k, \mathbb{F}_p)$ which states that all irreducible representations of $GL(V)(GL(k, \mathbb{F}_p))$ might be found in $M_*(k)$. That is to say, an enormous chunk will be disregarded when $M_*(k) = 0$, and for those where $M_*(k) \neq 0$ the dimensions will be known. In [6] and [7] *Crossley* gives a complete description in case of $GL(2, \mathbb{F}_p)$.

Recall that $\mathcal{P}_i : H_n((\mathbb{C}P^\infty)^k, \mathbb{F}_p) \longrightarrow H_{n-i(p-1)}((\mathbb{C}P^\infty)^k, \mathbb{F}_p)$ and the previous discussion admits $i = p^t$ for $t \geq 0$, where our aim is to calculate $M_*(k)$, so $\mathcal{P}_{p^t} : H_n((\mathbb{C}P^\infty)^k, \mathbb{F}_p) \longrightarrow H_{n+p^t-p^{t+1}}((\mathbb{C}P^\infty)^k, \mathbb{F}_p)$ gives a hint that is for a specific degree n we are not required to find the $Ker\mathcal{P}_{p^t}$ for all $t \geq 0$, but for some t.

The t's that we need are those satisfy the inequality $p^{t+1} < n + p^t$, while; otherwise i.e. $p^{t+1} \geq n + p^t$ the image of $\mathcal{P}_{p^t}$ automatically will be zero. For instance, $M_n(k) = H_n((\mathbb{C}P^\infty)^k, \mathbb{F}_p)$ for $1 \leq n \leq p-1$, because there is no $t \geq 0$ satisfies $n + p^t > p^{t+1}$.

4.2 The Spikes in $H_*(k)$

The first appearance of the term spike was in *William M. Singer*'s work in 1991, see [21]. In an analogous way, but in dual case we give the following definition of a spike.

Definition 4.2.1 (Spike). A monomial
$S = (x_1)_1^{p-1}(x_1)_p^{p-1}\dots(x_1)_{p^{i_1}}^{a_1}(x_2)_1^{p-1}(x_2)_p^{p-1}\dots(x_2)_{p^{i_2}}^{a_2}\dots(x_k)_1^{p-1}(x_k)_p^{p-1}\dots(x_k)_{p^{i_k}}^{a_k} \in H_*(k)$, such that $i_1, \dots, i_k \geq 0$ and $0 \leq a_1, \dots, a_k \leq p-1$ is called **spike**.

Note, the degree of a spike $(x_1)_1^{p-1}(x_2)_1^{p-1}\dots(x_k)_1^{p-1}\dots(x_1)_{p^{i_1}}^{a_1}(x_2)_{p^{i_2}}^{a_2}\dots(x_k)_{p^{i_k}}^{a_k}$ is given by $d = (a_1+1)p^{i_1} + (a_2+1)p^{i_2} + \dots (a_k+1)p^{i_k} - k$, and the permute of any $(p^{i_n}, a_n), (p^{i_m}, a_m)$ between x_n and x_m produces another spike in this degree, unless $p^{i_n} = p^{i_m}$ and $a_n = a_m$, thus the set of all such permutations gives all spikes in this degree which have the same degree form. Particularly, a spike in $H_*(1)$ is given by $x_1^{p-1}x_p^{p-1}\dots x_{p^i}^a$.

Theorem 4.2.2 (Crossley). *The basis for $M_d(1)$ where $d = (a+1)p^i - 1$, such that $i \geq 0$ and $1 \leq a \leq p-1$ is given by $x_1^{p-1}x_p^{p-1}\dots x_{p^i}^a$. Otherwise $M_d(1) = 0$.*

Proposition 4.2.3. *If there is a spike of degree d in $H_*(k)$, then it is in $M_d(k)$.*

Proof. Assume
$S = (x_1)_1^{p-1}(x_1)_p^{p-1}\dots(x_1)_{p^{i_1}}^{a_1}(x_2)_1^{p-1}(x_2)_p^{p-1}\dots(x_2)_{p^{i_2}}^{a_2}\dots(x_k)_1^{p-1}(x_k)_p^{p-1}\dots(x_k)_{p^{i_k}}^{a_k}$ a spike in $H_*(k)$, then for $t \geq 0$

$$\mathcal{P}_{p^t}(S) = \mathcal{P}_{p^t}\left((x_1)_1^{p-1}(x_1)_p^{p-1}\dots(x_1)_{p^{i_1}}^{a_1}(x_2)_1^{p-1}(x_2)_p^{p-1}\dots(x_2)_{p^{i_2}}^{a_2}\dots(x_k)_1^{p-1}(x_k)_p^{p-1}\dots(x_k)_{p^{i_k}}^{a_k}\right).$$

Applying *Cartan* formula implies

$$\mathcal{P}_{p^t}(S) = \sum_{n_1+n_2+\dots+n_k=p^t} \mathcal{P}_{n_1}\left((x_1)_1^{p-1}(x_1)_p^{p-1}\dots(x_1)_{p^{i_1}}^{a_1}\right)\dots\mathcal{P}_{n_k}\left((x_k)_1^{p-1}(x_k)_p^{p-1}\dots(x_k)_{p^{i_k}}^{a_k}\right),$$

according to theorem 4.2.2, we have $\mathcal{P}_{n_j}\left((x_j)_1^{p-1}(x_j)_p^{p-1}\dots(x_j)_{p^{i_j}}^{a_j}\right) = 0$, for $n_j > 0$, so each summand in the above expression will be zero, and this shows $\mathcal{P}_{p^t}(S) = 0$ for any integer $t \geq 0$. Hence, $S \in M_d(k)$. □

In addition to the previous proposition, if such spike exist in $M_d(k)$, then it will be a basis element (obviously, because it is a monomial). In fact, the significant difference between the case when $p = 2$ and p is given to be odd prime is that in the former if $M_d(k) \neq 0$, then there is at least a spike. By contrast, when p is odd it is not necessary to see that. For instance, (see [6], [7]) for the annihilated elements $M_{p^{s+2}+(i+1)p^{s+1}+p^s-2}(2)$ such that $0 \leq i \leq j \leq p-3$ and $s \geq 0$, similarly; our calculations expose that the annihilated elements in degree $n = p^{s+3} + 2p^{s+2} + p^{s+1} + 2p^s - 3$ does not involve a spike.

As we have seen one of the important application of $M_*(k)$ and $M^*(k)$ is to detect whether $M_d(k) = 0$ ($M^d(k) = 0$) or not, that means; in which degree d all polynomials will be hits, that is $\mathcal{A}^+(p)P(k) = P(k)$. On the other side, in which degrees the $Ker\theta$ are disjoint sets $\forall\theta \in \mathcal{A}(p)$.

In fact, the answer of these questions states according as $\mathcal{A}(2)$, or $\mathcal{A}(p)$ where $p > 2$. In the case of $\mathcal{A}(2)$, the complete answer was the proof of *Frank Peterson* conjecture 1987 [14] by *R.M.W Wood* in 1988 [30] which states

Theorem 4.2.4 (Wood). *$M^d(k) = 0 \iff \alpha(d+k) > k$, where $\alpha(n)$ is the number of digits in 2-adic expansion of n.*

Turning to case $\mathcal{A}(p)$, here it seems to be there were many efforts to address this problem, the first one was in the work of *Chen* and *Shen* in 1990 Barcelona conference on algebraic topology [20]. Followed by *Crossley* in [8] with the following theorem:

Theorem 4.2.5 (Crossley). *If d and k satisfy one of the following conditions, then $M^d(k) = 0$.*

1. $\alpha_p(d+k) > k(k+1)(p-1)/2$,
2. $\alpha_p((d+k)(p-1)) > k(p-1)$.

where $\alpha_p(n) = \sum_{i\geq 0} n_i$, such that n_i be the digits in p-adic expansion of n.

Theorem 4.2.6. *Let d be an integer such that $0 < d \leq p^k + p^{k-1} + \cdots + p - k$ then $M_d(k)$ is non-trivial. Moreover, the first $M_d(k) = 0$ occurs when $d = p^k + p^{k-1} + \cdots + p + 1 - k$.*

Proof. For $0 < d \leq p-1$, it is clear that each d can be represented by $d = (a+1) - 1$ such that $0 < a \leq p-1$, and theorem 4.2.2 implies that $M_d(k) \neq 0$. Now, assume that $p \leq d \leq p^k + p^{k-1} + \cdots + p - k$. Then d lies in one of the following inequalities $p^i + p^{i-1} + \cdots + p - i < d \leq p^{i+1} + p^i + \cdots + p - (i+1)$; where $i = 1, 2, \ldots, k-1$. That is to say, for each i

$$0 < d - \left(p^i + p^{i-1} + \cdots + p - i\right) \leq p^{i+1} - 1$$

so, can be written as

$$d - \left(p^i + p^{i-1} + \cdots + p - i\right) = a_i p^i + a_{i-1} p^{i-1} + \cdots + a_1 p + a_0$$

i.e.

$$\begin{aligned} d =& (a_i + 1)p^i + (a_{i-1} + 1)p^{i-1} + \cdots + (a_1 + 1)p + a_0 - i \\ =& (a_i + 1)p^i - 1 + (a_{i-1} + 1)p^{i-1} - 1 + \cdots + (a_1 + 1)p - 1 + (a_0 + 1) - 1 \end{aligned}$$

such that $0 \leq a_0, \ldots a_i \leq p-1$, unless $a_1 = a_2 = \ldots a_i = 0$, then $1 \leq a_0 \leq p-1$ since $p^{i+1} - 1 > 0$, and $i \leq k-1$. Theorem 4.2.2 reveals if $d_* = (a_n + 1)p^n - 1$, then $M_{d_*}(1) \neq 0$. Thus, we get that $M_d(k)$ contains at least one element for any d in that range which comes from the multiplication of $i+1$ different elements each one of them belongs to $M_{(a_i+1)p^i-1}(1)$ for $i = 0, 1, \cdots, k-1$, in other word; any degree contains at least a spike.

The previous discussion show that $M_d(k) \neq 0$ for any $d \leq p^k + \cdots + p - k$. Now consider,

$$d = p^k + \cdots + p + 1 - k$$

So,

$$\alpha_p((d+k)(p-1)) = (k+1)(p-1)$$

according to the second condition in theorem (5.2.5) we get $M^d(k) = 0$ in this degree or correspondingly, $M_d(k) = 0$. □

Chapter 5

Some results On $M_d(3)$

5.1 Calculation of $M_d(3)$.

For the rest of this chapter we will deal with $H_*(3)$, unless otherwise it will mentioned. As we defined $H(k)$ with slightly difference in the notation, we define $H_*(3)$, and use x, y, z instead of x_1, x_2, x_3, i.e.,

$$\begin{aligned} H(3) =& \mathbb{F}_p[x_1, y_1, z_1, x_p, y_p, z_p, \cdots]/[x_1^p, y_1^p, z_1^p, x_p^p, y_p^p, z_p^p, \ldots] \\ \cong& H_*(\mathbb{C}P^\infty \times \mathbb{C}P^\infty \times \mathbb{C}P^\infty, \mathbb{F}_p). \end{aligned}$$

The following theorem and the next one are the main results in this section. We use the same techniques used in [2] and [6].

Theorem 5.1.1. *The dimension of $M_n(3)$ for $1 \leq n < p^2$ is given according to the following table:*

Table 5.1: *Dim* $M_n(3)$

$Degree, n$	Dim $M_n(3)$	
$1 \leq n \leq p-1$	$\frac{(n+1)(n+2)}{2}$	
$n = a + p$, $0 \leq a \leq p-1$.	$(a+2)(p-1) + \frac{p(p-1)}{2}$	if $a \neq p-1$
	$p^2 + 2 + \frac{p(p-1)}{2}$	if $a = p-1$
$n = a + bp$, $0 \leq a \leq p-1$, $1 < b \leq p-1$.	$bp(p-1) + \frac{b(b-a)(a+2)-(p-a-2)(p-a-3)}{2}$	if $a < b$
	$bp(p-1) + \frac{(a+2)(a+1)-(p-a-2)(p-a-3)}{2}$	if $a \geq b$ and $a \neq p-1$
	$bp(p-1) + \frac{p(p+1)+b(b+3)}{2}$	if $a = p-1$

Proof. As we have observed in the last paragraph of section 4.1 that $M_n(3) = H_n(3)$ for $1 \leq n \leq p-1$, so it is easy to detect the basis here since each element of degree n in this range can be written as a linear combination from the monomials $x_1^m y_1^{k-m} z_1^{n-k}$ where $0 \leq k \leq n$ and $0 \leq m \leq k$, so that; dimension $M_n(3) = \frac{(n+1)(n+2)}{2}$.

In general we consider only the homogeneous polynomial in $H_*(3)$ because the image of homogeneous terms under $\mathcal{P}_{p^t}$ for $t \geq 0$ is either zero or homogeneous terms, so if there is a cancellation between these images, then it comes from those homogeneous terms. Furthermore, for $p \leq n < p^2$ calculation of $M_n(3)$ requires to find only $Ker\mathcal{P}_1$ since the argument in section 4.1 indicates that the only values of t that satisfy $n + p^t > p^{t+1}$ are $t = 0, 1$ for the degrees $(p-1)p < n < p^2$, otherwise only $t = 0$. On the other hand, proposition 3.3.2 tell us; the operation $\mathcal{P}_p$ send any monomial of degree less than p^2 to zero, so the only consideration operation in this case will be $\mathcal{P}_1$.

In fact, any polynomial of degree n where $p \leq n < p^2$ consists of $\{x_1, y_1, z_1, x_p, y_p, z_p\}$, and because it is a homogeneous, the sum of the exponent of x_1, y_1, z_1 must be a constant mod$p$. Let a to be that constant, then the total power of x_1, y_1, z_1 will be a, $p + a$ or $2p + a$. Now, observe that if we apply $\mathcal{P}_1$ on a monomial whose total power of x_1, y_1, z_1 is a, then the image (if it does not equal zero) it will be monomial(s) each one has total power of x_1, y_1, z_1 $a + 1$.

Similarly, for the remaining cases we will get $p+a+1$ and $2p+a+1$ as a total power respectively. Evidently, the image of the first case does not cancel the other cases image, and the same for the other cases, therefore; these cases are disjoint. Consequently, we exploit this property to deal with these cases individually, moreover $M_n(3)$ is written as a direct sum from the kernel of these cases.

Case 1: Total power $= a$, we will consider two separated cases in this case according to either $a \neq p-1$ or $a = p-1$. In both, the general formula of an arbitrary polynomial is given by

$$\theta = \sum_{k=0}^{a}\sum_{m=0}^{k}\sum_{i=0}^{b}\sum_{j=0}^{i} \alpha_{i,j}^{k,m} x_1^m y_1^{k-m} z_1^{a-k} x_p^j y_p^{i-j} z_p^{b-i} \quad \text{for } \alpha_{i,j}^{k,m} \in \mathbb{F}_p \tag{5.1}$$

Now, when $a < p-1$ applying $\mathcal{P}_1$ implies

$$\begin{aligned}
\mathcal{P}^1(\theta) &= \sum_{k=0}^{a}\sum_{m=0}^{k}\sum_{i=0}^{b}\sum_{j=0}^{i} (b-i)\alpha_{i,j}^{k,m} x_1^m y_1^{k-m} z_1^{a+1-k} x_p^j y_p^{i-j} z_p^{b-i-1} \\
&+ \sum_{k=0}^{a}\sum_{m=0}^{k}\sum_{i=0}^{b}\sum_{j=0}^{i} (i-j)\alpha_{i,j}^{k,m} x_1^m y_1^{k+1-m} z_1^{a-k} x_p^j y_p^{i-j-1} z_p^{b-i} \\
&+ \sum_{k=0}^{a}\sum_{m=0}^{k}\sum_{i=0}^{b}\sum_{j=0}^{i} j\alpha_{i,j}^{k,m} x_1^{m+1} y_1^{k-m} z_1^{a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i}
\end{aligned}$$

Assuming θ belongs to $M_n(3)$ gives $\mathcal{P}_1\theta = 0$, and substituting $x_1^p = y_1^p = z_1^p = 0$ in previous expression and rewriting it produces

$$\sum_{i=1}^{b}\sum_{j=1}^{i}(b+1-i)\alpha_{i-1,j-1}^{0,0}z_1^{a+1}x_p^{j-1}y_p^{i-j}z_p^{b-i}$$
$$+\sum_{i=1}^{b}\sum_{j=1}^{i}(i+1-j)\alpha_{i,j-1}^{a,0}y_1^{a+1}x_p^{j-1}y_p^{i-j}z_p^{b-i}$$
$$+\sum_{i=1}^{b}\sum_{j=1}^{i}j\alpha_{i,j}^{a,a}x_1^{a+1}x_p^{j-1}y_p^{i-j}z_p^{b-i}$$
$$+\sum_{k=0}^{a-1}\sum_{i=1}^{b}\sum_{j=1}^{i}\left((b+1-i)\alpha_{i-1,j-1}^{k+1,k+1}+j\alpha_{i,j}^{k,k}\right)x_1^{k+1}z_1^{a-k}x_p^{j-1}y_p^{i-j}z_p^{b-i}$$
$$+\sum_{m=0}^{a-1}\sum_{i=1}^{b}\sum_{j=1}^{i}\left((i+1-j)\alpha_{i,j-1}^{a,m+1}+j\alpha_{i,j}^{a,m}\right)x_1^{m+1}y_1^{a-m}x_p^{j-1}y_p^{i-j}z_p^{b-i}$$

$$+\sum_{k=0}^{a-1}\sum_{i=1}^{b}\sum_{j=1}^{i}\{(b+1-i)\alpha_{i-1,j-1}^{k+1,0}+(i+1-j)\alpha_{i,j-1}^{k,0}\}y_1^{k+1}z_1^{a-k}x_p^{j-1}y_p^{i-j}z_p^{b-i}$$
$$+\sum_{k=1}^{a-1}\sum_{m=0}^{k-1}\sum_{i=1}^{b}\sum_{j=1}^{i}\left((b+1-i)\alpha_{i-1,j-1}^{k+1,m+1}+(i+1-j)\alpha_{i,j-1}^{k,m+1}+j\alpha_{i,j}^{k,m}\right)$$
$$x_1^{m+1}y_1^{k-m}z_1^{a-k}x_p^{j-1}y_p^{i-j}z_p^{b-i}=0$$

On examining the previous expression we find that the terms are independent and this implies each one of them is equal to zero. Likewise, it is very noticeable that the monomials of each term also linearly independent. Hence, we get, if $a \neq p-1$, the following relations:

1) $\alpha_{i-1,j-1}^{0,0} = 0$ for $1 \le i \le b$ and $1 \le j \le i$,

2) $\alpha_{i,j-1}^{a,0} = 0$ for $1 \le i \le b$ and $1 \le j \le i$,

3) $\alpha_{i,j}^{a,a} = 0$ for $1 \le i \le b$ and $1 \le j \le i$,

4) $j\alpha_{i,j}^{k,k} = -(b+1-i)\alpha_{i-1,j-1}^{k+1,k+1}$ for $1 \le i \le b$ and $1 \le j \le i$ where $0 \le k \le a-1$,

5) $j\alpha_{i,j}^{a,m} = -(i+1-j)\alpha_{i,j-1}^{a,m+1}$ for $1 \le i \le b$ and $1 \le j \le i$ where $0 \le m \le a-1$,

6) $(i+1-j)\alpha_{i,j-1}^{k,0} = -(b+1-i)\alpha_{i-1,j-1}^{k+1,0}$ for $1 \le i \le b$ and $1 \le j \le i$ where $0 \le k \le a-1$,

7) $j\alpha_{i,j}^{k,m} = -((b+1-i)\alpha_{i-1,j-1}^{k+1,m+1} + (i+1-j)\alpha_{i,j-1}^{k,m+1})$ for $1 \le i \le b$ and $1 \le j \le i$ where $1 \le k \le a-1$ and $0 \le m \le k-1$.

According to the above system of linear equations we have $\frac{b(b+1)}{2}$ linear equations from relation (1). Examining the subscript indices of these equations shows they are independent because each value of i or j describes different variable. Obviously, similar thing could be seen when one considers the equations in relations (2) and (3).

On the other hand, the superscript indices reveals that these equations together are independent since $a \neq 0$ (if $a = 0$, then the relations from (4) to (7) will be finished and the equations in relations (1) to (3) will be given by $\alpha_{i,j}^{0,0} = 0$ for $0 \leq i \leq b$ and $0 \leq j \leq i$, that means $\theta = 0$ and this contradict with the assumption since $p \leq d < p^2$).

Turning to relation (4) that involves $\frac{ab(b+1)}{2}$ linear equations which are also independent, because of; for a fixed $k = c$ the equations $j\alpha_{i,j}^{c,c} = -(b+1-j)\alpha_{i-1,j-1}^{c+1,c+1}$ involve new variable $\alpha_{i,j}^{c,c}$ for each one such that $1 \leq i \leq b$ and $1 \leq j \leq i$, so they are independent,likewise; for any value of k such that $0 \leq k \leq a-1$.

In addition, these new variables could not seen in (1), (2) and (3) except in two cases. The first one, if $k = 0$, then (4) is given by $j\alpha_{i,j}^{0,0} = -(b+1-i)\alpha_{i,j}^{1,1}$, but $b+1-i \neq 0$ for $1 \leq i \leq b$ implies these equations are independent of the equations in relations (1). The second one, when $k = a-1$, so (4) becomes $j\alpha_{i,j}^{a-1,a-1} = -(b+1-i)\alpha_{i-1,j-1}^{a,a}$, similarly; since $j \neq 0$ for $1 \leq j \leq i$ illustrates why (4) independent of (3). Consequently, the equations in (1), (2), (3) and (4) are independent.

The same arguments can be used to shows that the equations in (5) are independent and they are independent of what are in (1), (2) and (3). To check the independence of equations (4) and (5), we need to consider only the case when $k = a-1$ and $m = a-1$, so we get respectively from (4) and (5) the following

$$j\alpha_{i,j}^{a-1,a-1} = -(b+1-i)\alpha_{i-1,j-1}^{a,a},$$

and

$$j\alpha_{i,j}^{a,a-1} = -(i+1-j)\alpha_{i-1,j-1}^{a,a}.$$

Clearly, the equations in the above two systems are independent. Hence, the equation of (5) are independent of (1), (2) ,(3) and (4).

By the same way, we can show that the equations of relation (6) are independent and independent of the equations in previous relations. Finally, in (7) the following equations

$$(b+1-j)\alpha_{i-1,j-1}^{k+1,m+1} = -j\alpha_{i,j}^{k,m} - (i+1-j)\alpha_{i,j+1}^{k,m+1}$$

for $1 \leq i \leq b$ and $1 \leq j \leq i$ such that $1 \leq k \leq a-1$ and $1 \leq m \leq k-1$, introduce for each value of k or m a new variable(the left side of each equation), that is to say; these equations are independent. For $1 \leq i \leq b$ and $1 \leq j \leq i$ where $1 \leq k \leq a-2$ and $1 \leq m \leq k-1$ these new variables do not appear in any equation of previous relations, so the equations with these value of i, j, k and m are independent of what are in previous relations.

Whilst, if $k = a-1$ we get

$$(b+1-j)\alpha^{a,m+1}_{i-1,j-1} = -j\alpha^{a-1,m}_{i,j} - (i+1-j)\alpha^{a-1,m+1}_{i,j+1},$$

where $1 \leq i \leq b$, $1 \leq j \leq i$ and $0 \leq m \leq a-2$. The equations in this case may be give a sense they are dependent on some equations in relation (5), but we will see this is not the case when we look at the left superscript index of the right variables in both formulas. Moreover, in (7) if the one of right variables dose not free variables, then it depends on variables in relation (7) and so on until we stop at the free one. Therefore, the equations of relation (7) are independent of the equation in (1) to (6). Hence, all the equations in that system are independent.

Thus, we have $\frac{b(b+1)}{2}$ linearly independent equations from relation (1), (2) and (3), so adding these we get $\frac{3b(b+1)}{2}$ equations. Now relation (4), (5) and (6) gives $\frac{ab(b+1)}{2}$ linearly independent equations, this time adding gives $\frac{3ab(b+1)}{2}$. Finally, the number of linearly independent equations in relation (7) is $\frac{ab(a-1)(b+1)}{4}$. Hence, the total number of linearly independent equations we get is $\frac{b(b+1)(a+3)(a+2)}{4}$.

On the other hand, the number of variables $\alpha^{k,m}_{i,j}$ of θ is $\frac{(a+1)(a+2)(b+1)(b+2)}{4}$. Consequently, the dimension in this case is given by:

$$\begin{aligned} Dim\ C_1 &= \frac{(a+1)(a+2)(b+1)(b+2)}{4} - \frac{b(b+1)(a+3)(a+2)}{4} \\ &= \frac{(b+1)(a+2)(a+1-b)}{2} \end{aligned} \tag{5.2}$$

If $a = p-1$, then similar previous argument gives the equations below:

1) $j\alpha^{k,k}_{i,j} = -(b+1-i)\alpha^{k+1,k+1}_{i-1,j-1}$ for $1 \leq i \leq b$ and $1 \leq j \leq i$ where $0 \leq k \leq p-2$.

2) $j\alpha^{a,m}_{i,j} = -(i+1-j)\alpha^{a,m+1}_{i,j-1}$ for $1 \leq i \leq b$ and $1 \leq j \leq i$ where $0 \leq m \leq p-2$.

3) $(i+1-j)\alpha^{k,0}_{i,j-1} = -(b+1-i)\alpha^{k+1,0}_{i-1,j-1}$ for $1 \leq i \leq b$ and $1 \leq j \leq i$ where $0 \leq k \leq p-2$.

4) $j\alpha^{k,m}_{i,j} = -((b+1-i)\alpha^{k+1,m+1}_{i-1,j-1} + (i+1-j)\alpha^{k,m+1}_{i,j-1})$ for $1 \leq i \leq b$ and $1 \leq j \leq i$ where $1 \leq k \leq p-2$ and $0 \leq m \leq k-1$.

The independence of the equations of the above system can be deduced from the case where $a < p-1$, so the last relations from (1) to (4) give $\frac{b(b+1)(p+4)(p-1)}{4}$ linearly independent equations, whilst; there are $\frac{p(p+1)(b+1)(b+2)}{4}$ variables in the formula (5.1) when $a = p-1$. Hence, we have

$$Dim\ C_1 = \frac{(b+1)}{2}(p(p+1) - b(p-2)) \tag{5.3}$$

Case 2: Total power $= a+p$. In this case we will deal with two separate cases according to a, the first one when $a<p-1$ and the second one is if $a=p-1$. For both we will use the same technique that has been done to proof case (1) to find the dimension. Now, if $a<p-1$, then an arbitrary polynomial should be written by

$$\theta = \sum_{k=a+1}^{p-1}\sum_{m=0}^{k}\sum_{i=0}^{b-1}\sum_{j=0}^{i}\beta_{i,j}^{k,m}x_1^m y_1^{k-m}z_1^{p+a-k}x_p^j y_p^{i-j}z_p^{b-i-1}$$
$$+\sum_{k=0}^{a}\sum_{m=k+1}^{p-1}\sum_{i=0}^{b-1}\sum_{j=0}^{i}\beta_{i,j}^{k,m}x_1^m y_1^{p+k-m}z_1^{a-k}x_p^j y_p^{i-j}z_p^{b-i-1}. \tag{5.4}$$

Applying $\mathcal{P}^1$ implies

$$\begin{aligned}
\mathcal{P}^1\theta &= \sum_{k=a+1}^{p-1}\sum_{m=0}^{k}\sum_{i=0}^{b-2}\sum_{j=0}^{i}(b-i-1)\beta_{i,j}^{k,m}x_1^m y_1^{k-m}z_1^{p+a+1-k}x_p^j y_p^{i-j}z_p^{b-i-2}\\
&+ \sum_{k=a+1}^{p-1}\sum_{m=0}^{k}\sum_{i=1}^{b-1}\sum_{j=0}^{i-1}(i-j)\beta_{i,j}^{k,m}x_1^m y_1^{k+1-m}z_1^{p+a-k}x_p^j y_p^{i-j-1}z_p^{b-i-1}\\
&+ \sum_{k=a+1}^{p-1}\sum_{m=0}^{k}\sum_{i=1}^{b-1}\sum_{j=1}^{i}j\beta_{i,j}^{k,m}x_1^{m+1}y_1^{k-m}z_1^{p+a-k}x_p^{j-1}y_p^{i-j}z_p^{b-i-1}\\
&+ \sum_{k=0}^{a}\sum_{m=k+1}^{p-1}\sum_{i=0}^{b-2}\sum_{j=0}^{i}(b-i-1)\beta_{i,j}^{k,m}x_1^m y_1^{p+k-m}z_1^{a+1-k}x_p^j y_p^{i-j}z_p^{b-i-2}\\
&+ \sum_{k=0}^{a}\sum_{m=k+1}^{p-1}\sum_{i=1}^{b-1}\sum_{j=0}^{i-1}(i-j)\beta_{i,j}^{k,m}x_1^m y_1^{p+k+1-m}z_1^{a-k}x_p^j y_p^{i-j-1}z_p^{b-i-1}\\
&+ \sum_{k=0}^{a}\sum_{m=k+1}^{p-1}\sum_{i=1}^{b-1}\sum_{j=1}^{i}j\beta_{i,j}^{k,m}x_1^{m+1}y_1^{p+k-m}z_1^{a-k}x_p^{j-1}y_p^{i-j}z_p^{b-i-1},
\end{aligned}$$

rewriting the previous equation subject to the relations $x_1^p = y_1^p = z_1^p = 0$ gives,

$$\begin{aligned}
\mathcal{P}^1\theta = &\sum_{k=a+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i}j\beta_{i,j}^{k,k}x_1^{k+1}z_1^{p+a-k}x_p^{j-1}y_p^{i-j}z_p^{b-i-1}\\
&+\sum_{k=a+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i}(b-i)\beta_{i-1,j-1}^{k+1,k+1}x_1^{k+1}z_1^{p+a-k}x_p^{j-1}y_p^{i-j}z_p^{b-i-1}\\
&+\sum_{k=a+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=0}^{i-1}(i-j)\beta_{i,j}^{k,0}y_1^{k+1}z_1^{p+a-k}x_p^j y_p^{i-j-1}z_p^{b-i-1}\\
&+\sum_{k=a+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=0}^{i-1}(b-i)\beta_{i-1,j}^{k+1,0}y_1^{k+1}z_1^{p+a-k}x_p^j y_p^{i-j-1}z_p^{b-i-1}
\end{aligned}$$

$$+\sum_{m=a+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i} j\beta_{i,j}^{a,m} x_1^{m+1} y_1^{p+a-m} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{m=a+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i} (i+1-j)\beta_{i,j-1}^{a,m+1} x_1^{m+1} y_1^{p+a-m} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{k=a+1}^{p-1}\sum_{m=0}^{k-1}\sum_{i=1}^{b-1}\sum_{j=1}^{i} j\beta_{i,j}^{k,m} x_1^{m+1} y_1^{k-m} z_1^{p+a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{k=a+1}^{p-1}\sum_{m=0}^{k-1}\sum_{i=1}^{b-1}\sum_{j=1}^{i} (i+1-j)\beta_{i,j-1}^{k,m+1} x_1^{m+1} y_1^{k-m} z_1^{p+a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{k=a+1}^{p-1}\sum_{m=0}^{k-1}\sum_{i=1}^{b-1}\sum_{j=1}^{i} (b-i)\beta_{i-1,j-1}^{k+1,m+1} x_1^{m+1} y_1^{k-m} z_1^{p+a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{k=0}^{a-1}\sum_{m=k+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i} j\beta_{i,j}^{k,m} x_1^{m+1} y_1^{p+k-m} z_1^{a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{k=0}^{a-1}\sum_{m=k+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i} (i+1-j)\beta_{i.j-1}^{k,m+1} x_1^{m+1} y_1^{p+k-m} z_1^{a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{k=0}^{a-1}\sum_{m=k+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i} (b-i)\beta_{i-1,j-1}^{k+1,m+1} x_1^{m+1} y_1^{p+k-m} z_1^{a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

If $\theta \in M_*(3)$ that is, $\theta \in Ker\mathcal{P}_1$,

$$\mathcal{P}^1\theta = \sum_{k=a+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i} \{j\beta_{i,j}^{k,k} + (b-i)\beta_{i-1,j-1}^{k+1,k+1}\} x_1^{k+1} z_1^{p+a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{k=a+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i} \{(i+1-j)\beta_{i,j-1}^{k,0} + (b-i)\beta_{i-1,j-1}^{k+1,0}\} y_1^{k+1} z_1^{p+a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{m=a+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i} \{j\beta_{i,j}^{a,m} + (i+1-j)\beta_{i,j-1}^{a,m+1}\} x_1^{m+1} y_1^{p+a-m} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{k=a+1}^{p-1}\sum_{m=0}^{k-1}\sum_{i=1}^{b-1}\sum_{j=1}^{i} \{j\beta_{i,j}^{k,m} + (i+1-j)\beta_{i,j-1}^{k,m+1} + (b-i)\beta_{i-1,j-1}^{k+1,m+1}\}$$
$$x_1^{m+1} y_1^{k-m} z_1^{p+a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-1}$$

$$+\sum_{k=0}^{a-1}\sum_{m=k+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i} \{j\beta_{i,j}^{k,m} + (i+1-j)\beta_{i,j-1}^{k,m+1} + (b-i)\beta_{i-1,j-1}^{k+1,m+1}\}$$
$$x_1^{m+1} y_1^{p+k-m} z_1^{a-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-1} = 0$$

Looking at the last expression we see that each constitute summand is independent, like; the monomials in these summands. For these reasons,the following relations are follow

1) $j\beta_{i,j}^{k,k} = -(b-i)\beta_{i-1,j-1}^{k+1,k+1}$ for $1 \leq i \leq b-1$ and $1 \leq j \leq i$ where $a+1 \leq k \leq p-2$.

2) $j\beta_{i,j}^{a,m} = -(i+1-j)\beta_{i,j-1}^{a,m+1}$ for $1 \leq i \leq b-1$ and $1 \leq j \leq i$ where $a+1 \leq m \leq p-2$.

3) $(i+1-j)\beta_{i,j-1}^{k,0} = -(b-i)\beta_{i-1,j-1}^{k+1,0}$ for $1 \leq i \leq b-1$ and $1 \leq j \leq i$ where $a+1 \leq k \leq p-2$.

4) $j\beta_{i,j}^{k,m} = -((i+1-j)\beta_{i,j-1}^{k,m+1} + (b-i)\beta_{i-1,j-1}^{k+1,m+1})$ for $1 \leq i \leq b-1$ and $1 \leq j \leq i$ where $a+1 \leq k \leq p-1$ and $0 \leq m \leq k-1$.

5) $j\beta_{i,j}^{k,m} = -((i+1-j)\beta_{i,j-1}^{k,m+1} + (b-i)\beta_{i-1,j-1}^{k+1,m+1})$ for $1 \leq i \leq b-1$ and $1 \leq j \leq i$ where $0 \leq k \leq a-1$ and $k+1 \leq m \leq p-2$.

Note that in relation (4) $\beta_{i-1,j-1}^{p,m+1} = \beta_{i-1,j-1}^{0,m+1}$ for $1 \leq i \leq b-1$ and $1 \leq j \leq i$ where $0 \leq m \leq p-2$.

The equations in relation (1) are independent since each value for i, j and k gives new variable. Similarly, for relations (2) and (3). Moreover, the equations in each relation are independent of the others because the variables in equations of relation (1) are different on the variables in equations of (2) and (3). Likewise, the variables of relation (2) can not seen in (3)(we need to looking at the superscript to see that easily).

On the other hand, the right side of the equations of relation (5) introduces new variables for each value of i, j, k and m in that range. On examining the equations in relations from (1) to (3) we can not see these new variables since the left superscript index run through the value 0 to $a-1$, while; in (1) and (3) are taken the values $a+1 \leq k \leq p-2$, and in (2) is a, so that the equations in (5) are independent of the equations in these relations.

Finally, the equations of the relation (4) are independent, and they are independent of the equations in relation (5) for the same reason why equations (5) are independent of equations (1) to (3). In the same way, they are independent of the equations in (1) because $m \leq k-1$, that is; it is impossible to find superscript with equating indices. Because of, in (4) $a+1 \leq k \leq p-1$, so we can not see a variable with left superscript equal to a, and since if $m = 0$ the right side of each equation can not involves variable such that the right superscript of this variable could be zero. For these reasons the equations in (4) independent of the equations in (2) and (3). Thus, the equations of the relations (1) to (5) are linearly independent.

Now, according to $\theta's$ formula, it is clear to see that the first summation contains $\left((p-a-1)p - \frac{(p-a-1)(p-a-2)}{2}\right)\frac{b(b+1)}{2}$ variables, however; the total number of variables in the second one are $\left((a+1)(p-1) - \frac{a(a+1)}{2}\right)\frac{b(b+1)}{2}$. While, the total number of the equations in the first three relations (1),(2) and (3) is $3(p-a-2)\frac{b(b-1)}{2}$, whereas; relation (4) gives $\left((p-a-1)(p-1)-\frac{(p-a-1)(p-a-2)}{2}\right)\frac{b(b-1)}{2}$ linearly equations, and from (5) we have $\left(a(p-2)-\frac{a(a-1)}{2}\right)\frac{b(b-1)}{2}$ equations. Hence, the degree of freedom is given by

$$\begin{aligned}
Dim\ C_2 &= \left((p-a-1)p+(a+1)(p-1)-\frac{(p-a-1)(p-a-2)}{2}-\frac{a(a+1)}{2}\right)\frac{b(b+1)}{2}\\
&- \left(3(p-a-2)+(p-a-1)(p-1)-\frac{(p-a-1)(p-a-2)}{2}\right)\frac{b(b-1)}{2}\\
&- \left(a(p-2)-\frac{a(a-1)}{2}\right)\frac{b(b-1)}{2},\\
&= \frac{b}{2}(p-a-1)(p+b+a+1)+\frac{b}{2}(p+bp+2ap-a^2-3a-b-1)\\
&- \frac{b}{2}(3p+6b+3ab-3bp-3a-6)\\
&= \frac{bp(p-b)}{2}+b(a+2)(p+b-a-2)
\end{aligned} \tag{5.5}$$

Let $a=p-1$, for this case an arbitrary polynomial is given by the form below

$$\theta=\sum_{k=0}^{p-2}\sum_{m=k+1}^{p-1}\sum_{i=0}^{b-1}\sum_{j=0}^{i}\beta_{i,j}^{k,m}x_1^m y_1^{p+k-m}z_1^{p-k-1}x_p^j y_p^{i-j}z_p^{b-i-1} \tag{5.6}$$

such that $\beta_{i,j}^{k,m}\in\mathbb{F}_p$. If $b=1$, then 5.6 becomes

$$\theta=\sum_{k=0}^{p-2}\sum_{m=k+1}^{p-1}\beta_{k,m}x_1^m y_1^{p+k-m}z_1^{p-k-1},$$

where $\beta_{k,m}\in\mathbb{F}_p$. Apparently, θ which is given in previous formula belongs to $Ker\mathcal{P}_1$, so each constituent monomial represents a basis element, hence; we get

$$Dim\ C_2=\frac{p(p-1)}{2}. \tag{5.7}$$

Returning to equation 5.6, now we will deal with the case when $b\geq 2$, so applying the operation $\mathcal{P}_1$ yields

$$\begin{aligned}
\mathcal{P}_1\theta =&\sum_{k=0}^{p-3}\sum_{m=k+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i}(b-i)\beta_{i-1,j-1}^{k+1,m+1}x_1^{m+1}y_1^{p+k-m}z_1^{p-k-1}x_p^{j-1}y_p^{i-j}z_p^{b-i-2}\\
&+\sum_{k=0}^{p-3}\sum_{m=k+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i}(i+1-j)\beta_{i,j-1}^{k,m+1}x_1^{m+1}y_1^{p+k-m}z_1^{p-k-1}x_p^{j-1}y_p^{i-j}z_p^{b-i-2}\\
&+\sum_{k=0}^{p-3}\sum_{m=k+1}^{p-2}\sum_{i=1}^{b-1}\sum_{j=1}^{i}j\beta_{i,j}^{k,m}x_1^{m+1}y_1^{p+k-m}z_1^{p-k-1}x_p^{j-1}y_p^{i-j}z_p^{b-i-2}
\end{aligned}$$

so, equating the image of θ under $\mathcal{P}_1$ to zero, and the independence of the monomials $x_1^{m+1}y_1^{p+k-m}z_1^{p-k-1}x_p^{j-1}y_p^{i-j}z_p^{b-i-2}$ where $0 \leq k \leq p-3$ and $k+1 \leq m \leq p-2$ for $1 \leq i \leq b-1$ and $1 \leq j \leq i$ provides

$$j\beta_{i,j}^{k,m} = -(i+1-j)\beta_{i,j-1}^{k,m+1} - (b-i)\beta_{i-1,j-1}^{k+1,m+1} \tag{5.8}$$

such that i, j, k and m in those given ranges.

Obviously, the number of the linearly independent equations in 5.8 is $\frac{(p-1)(p-2)}{2} \cdot \frac{b(b-1)}{2}$, whilst; formula 5.6 includes $\frac{p(p-1)}{2} \cdot \frac{b(b+1)}{2}$ variables, so that;

$$\begin{aligned} Dim\ C_2 &= \frac{p(p-1)}{2}\frac{b(b+1)}{2} - \frac{(p-1)(p-2)}{2}\frac{b(b-1)}{2} \\ &= \frac{b(p-1)(p+b-1)}{2} \end{aligned} \tag{5.9}$$

Case 3: Total power $= a+2p$. The most striking feature in this case is $0 \leq a \leq p-3$, because the greatest total power of x_1, y_1 and z_1 is $3p-3 = 2p+(p-3)$, when the power of each variable be $p-1$, that automatically forces $a \leq p-3$. An example of this is, when $p=3$, then a have to be taken the value zero. Hence, any polynomial in this case will be given by

$$\theta = \sum_{i=0}^{b-2}\sum_{j=0}^{i} \lambda_{i,j} x_1^2 y_1^2 z_1^2 x_p^j y_p^{i-j} z_p^{b-2-i} \tag{5.10}$$

where $\lambda_{i,j} \in \mathbb{F}_p$, but $b=2$ because we deal with polynomial of degree less than p^2(notice that if $b<2$, then formula 5.10 will be zero), then

$$\theta = \lambda x_1^2 y_1^2 z_1^2,$$

such that $\lambda \in \mathbb{F}_p$, and without any effort we can see that $\mathcal{P}_1(\theta) = 0$,hence; when $p=3$ the dimension is one, and the basis of this case is $x_1^2y_1^2z_1^2$.

Now, in general any arbitrary polynomial satisfy the condition of case (3) is given by

$$\theta = \sum_{k=a+2}^{p-1}\sum_{m=0}^{p-1-k}\sum_{i=0}^{b-2}\sum_{j=0}^{i} \lambda_{i,j}^{k,m} x_1^{m+k} y_1^{p-1-m} z_1^{p+a+1-k} x_p^j y_p^{i-j} z_p^{b-i-2}, \tag{5.11}$$

and

$$\begin{aligned} \mathcal{P}_1\theta = &\sum_{k=a+2}^{p-1}\sum_{m=0}^{p-1-k}\sum_{i=0}^{b-2}\sum_{j=0}^{i} (b-i-2)\lambda_{i,j}^{k,m} x_1^{m+k} y_1^{p-1-m} z_1^{p+a+2-k} x_p^j y_p^{i-j} z_p^{b-i-3} \\ &+ \sum_{k=a+2}^{p-1}\sum_{m=0}^{p-1-k}\sum_{i=0}^{b-2}\sum_{j=0}^{i} (i-j)\lambda_{i,j}^{k,m} x_1^{m+k} y_1^{p-m} z_1^{p+a+1-k} x_p^j y_p^{i-j-1} z_p^{b-i-2} \\ &+ \sum_{k=a+2}^{p-1}\sum_{m=0}^{p-1-k}\sum_{i=0}^{b-2}\sum_{j=0}^{i} j\lambda_{i,j}^{k,m} x_1^{m+k+1} y_1^{p-1-m} z_1^{p+a+1-k} x_p^{j-1} y_p^{i-j} z_p^{b-i-2} \end{aligned}$$

If $\mathcal{P}_1\theta = 0$, that means

$$\sum_{k=a+2}^{p-2}\sum_{m=0}^{p-k-2}\sum_{i=1}^{b-2}\sum_{j=1}^{i}\{(b-i-1)\lambda_{i-1,j-1}^{k+1,m} + (i+1-j)\lambda_{i,j-1}^{k,m+1} + j\lambda_{i,j}^{k,m}\}$$
$$x_1^{m+k+1}y_1^{p-1-m}z_1^{p+a+1-k}x_p^{j-1}y_p^{i-j}z_p^{b-i-2} = 0$$

So, the linearity independence of the monomials of the previous expression and since $\mathcal{P}_1(\theta) = 0$, we infer

$$j\lambda_{i,j}^{k,m} = -(b-i-1)\lambda_{i-1,j-1}^{k+1,m} - (i+1-j)\lambda_{i,j-1}^{k,m+1} \tag{5.12}$$

for $1 \le i \le b-2$ and $1 \le j \le i$ where $a+2 \le k \le p-2$ and $0 \le m \le p-k-2$.

The relation 5.12 shows that there are $\frac{(p-a-3)(p-a-2)}{2}\frac{(b-2)(b-1)}{2}$ linearly independent equations. On the other hand, the number of variables in 5.11 is $\frac{(p-a-2)(p-a-1)}{2}\frac{b(b-1)}{2}$. Therefore, we have

$$\begin{aligned} Dim\ C_3 &= \frac{b(b-1)(p-a-1)(p-a-2)}{4} - \frac{(b-1)(b-2)(p-a-2)(p-a-3)}{4} \\ &= \frac{(b-1)(p-a-2)}{2}(p+b-a-3) \end{aligned} \tag{5.13}$$

According to the previous cases and degree form $n = a + bp$ such that $0 \le a \le p-1$ and $1 \le b \le p-1$, we should discuss the following possibilities. Firstly, If $b = 1$, then for degree reason we can not get an elements satisfy case (3) condition because if $b = 1$, then $p \le n \le 2p-1$, whilst the elements in case (3) have to be in degrees n such that $n \ge 2p$. Thus, we infer the dimension of this case from the dimension of case (1) and (2) according as $a < p-1$ or $a = p-1$. For $a < p-1$, substituting $b = 1$ in both 5.2 and 5.5, and adding the result gives the dimension in this case as

$$Dim\ M_n(3) = (a+2)(p-1) + \frac{p(p-1)}{2}.$$

In the same way, when $a = p-1$ we substitute $b = 1$ in 5.3, and add this to 5.7 to get

$$Dim\ M_n(3) = p^2 + 2 + \frac{p(p-1)}{2}.$$

Secondly, when $b \ge 2$, if $a < b$ then automatically $a \ne p-1$ and we calculate the dimension in this case from 5.5 and 5.13 which is given by

$$Dim\ M_n(3) = bp(p-1) + \frac{b(b-a)(a+2) - (p-a-2)(p-a-3)}{2}.$$

If $a \ge b$ and $a < p-1$, then we should add equation 5.2 to previous case and this yields

$$Dim\ M_n(3) = bp(p-1) + \frac{(a+2)(a+1) - (p-a-2)(p-a-3)}{2}.$$

Finally, when $b \geq 2$ and $a = p-1$ as we have shown in case (3) a has to be restricted between 0 and $p-3$, hence; there are no elements from case (3) and we need only to consider 5.3 and 5.9 to deduce the dimension in this case which is

$$Dim\ M_n(3) = bp(p-1) + \frac{p(p+1) + b(b+3)}{2}.$$

□

The rest of this section is devoted to determining the basis elements of a given degree in theorem 5.1.1. We need the following notations $C_{xy} = (x_1 y_p - y_1 x_p)$, $C_{xz} = (x_1 z_p - z_1 x_p)$ and $C_{yz} = (y_1 z_p - z_1 y_p)$, we call these elements *Crossley* brackets according to the first appearance of these elements in [6] and [7]. In fact, the *Crossley* bracket C_{xy} and its powers played the essential role in describing the basis of $M_n(2)$ where $p^s - 1 \leq n \leq p^{s+2} + p^{s+1} - 2$. Similarly, these brackets describe the basis of $M_n(3)$ where $n \leq p^2 + (p-1)p - 3$, according to our calculation.

Theorem 5.1.2. *For the degrees n such that $n \leq 2p-1$, the basis elements of $M_n(3)$ are given by*

Table 5.2: *Basis of $M_n(3)$*

Degree, n	Basis of $M_n(3)$
$1 \leq n \leq p-1$	$\{x_1^i y_1^j z_1^k \mid i+j+k=n\}$,
$n = a+p$, $0 \leq a < p-1$	$\{y_1^k z_1^{a-k-1} C_{yz} \mid 0 \leq k \leq a-1\} \cup$ $\{x_1^m y_1^{k-m} z_1^{a-k-1} C_{xz} \mid 0 \leq k \leq a-1, 0 \leq m \leq k\} \cup$ $\{x_1^m y_1^{k-m} z_1^{a-k-1} C_{xy} \mid 0 \leq k \leq a-1, 0 \leq m \leq k\} \cup$ $\{x_1^m y_1^{k-m} z_1^{p+a-k} \mid a+1 \leq k \leq p-1, 0 \leq m \leq k\} \cup$ $\{x_1^m y_1^{p+k-m} z_1^{a-k} \mid 0 \leq k \leq a, k+1 \leq m \leq p-1\}$,
$n = a+p$, $a = p-1$,	$\{x_1^{p-1} x_p\} \cup \{y_1^{p-1} y_p\} \cup \{z_1^{p-1} z_p\} \cup$ $\{y_1^k z_1^{p-2-k} C_{yz} \mid 0 \leq k \leq p-2\} \cup$ $\{x_1^m y_1^{k-m} z_1^{p-2-k} C_{xz} \mid 1 \leq k \leq p-1, 0 \leq m \leq k-1\} \cup$ $\{x_1^m y_1^{k-m-1} z_1^{p-1-k} C_{xy} \mid 1 \leq k \leq p-1, 0 \leq m \leq k-1\} \cup$ $\{x_1^m y_1^{p+k-m} z_1^{p-1-k} \mid 0 \leq k \leq p-2, k+1 \leq m \leq p-1\}$.

Proof. **Case 1:** When $1 \leq n \leq p-1$. We have mentioned at the beginning of proof of theorem 5.1.1 that each element in this range of n is written as a linear combination of monomials in the form $x_1^m y_1^{l-m} z_1^{n-l}$ where $0 \leq l \leq n$ and $0 \leq m \leq l$. That is to say, if $\theta \in H_n(3)$, then $\theta = \sum_{l=0}^{n} \sum_{m=0}^{l} \xi_{l,m} x_1^m y_1^{l-m} z_1^{n-l} = \sum_{i+j+k=n} \xi_{i,j,k} x_1^i y_1^j z_1^k$, where $\xi_{l,m}, \xi_{i,j,k} \in \mathbb{F}_p$. Obviously, from the degree consideration there is no condition to be $\theta \in M_n(3)$, thus the basis is given as in the first row of the above table.

Case 2: If $n = a + p$ and $0 \leq a < p - 1$. First, if the total exponent=a, then from equation 5.1 we have

$$\theta = \sum_{k=0}^{a}\sum_{m=0}^{k}\sum_{i=0}^{1}\sum_{j=0}^{i} \alpha_{i,j}^{k,m} x_1^m y_1^{k-m} z_1^{a-k} x_p^j y_p^{i-j} z_p^{1-i},$$

where $\alpha_{i,j}^{k,m} \in \mathbb{F}_p$, but if $\theta \in M_n(3)$, then the coefficients $\alpha_{i,j}^{k,m}$ have to be satisfy the relations from 1 to 7 (the proof of 5.1.1 first case where $0 \leq a < p-1$). Starting with the equations 1, 2 and 3, we get $\alpha_{0,0}^{0,0} = \alpha_{1,0}^{a,0} = \alpha_{1,1}^{a,a} = 0$, so

$$\begin{aligned}\theta =& \sum_{k=0}^{a-1} \alpha_{1,1}^{k,k} x_1^k z_1^{a-k} x_p + \sum_{m=0}^{a-1} \alpha_{1,1}^{a,m} x_1^m y_1^{a-m} x_p + \sum_{k=1}^{a-1}\sum_{m=0}^{k-1} \alpha_{1,1}^{k,m} x_1^m y_1^{k-m} z_1^{a-k} x_p \\ &+ \sum_{m=0}^{a-1} \alpha_{1,0}^{a,m+1} x_1^{m+1} y_1^{k-m-1} y_p + \sum_{k=0}^{a-1} \alpha_{1,0}^{k,0} y_1^k z_1^{a-k} y_p + \sum_{k=1}^{a-1}\sum_{m=0}^{k-1} \alpha_{1,0}^{k,m+1} x_1^{m+1} y_1^{k-m-1} z_1^{a-k} y_p \\ &+ \sum_{k=0}^{a-1} \alpha_{0,0}^{k+1,k+1} x_1^{k+1} z_1^{a-k-1} z_p + \sum_{k=0}^{a-1} \alpha_{0,0}^{k+1,0} y_1^{k+1} z_1^{a-k-1} z_p + \sum_{k=1}^{a-1}\sum_{m=0}^{k-1} \alpha_{0,0}^{k+1,m+1} x_1^{m+1} y_1^{k-m} z_1^{a-k-1} z_p.\end{aligned}$$

Moving to the substitutions of the relations 4, 5, 6 and 7, that implies

$$\begin{aligned}\theta =& \sum_{k=0}^{a-1} \alpha_{0,0}^{k+1,k+1} x_1^k z_1^{a-k-1}(x_1 z_p - z_1 x_p) + \sum_{m=0}^{a-1} \alpha_{1,0}^{a,m+1} x_1^m y_1^{a-m-1}(x_1 y_p - y_1 x_p) \\ &+ \sum_{k=0}^{a-1} \alpha_{0,0}^{k+1,0} y_1^k z_1^{a-k-1}(y_1 z_p - z_1 y_p) + \sum_{k=1}^{a-1}\sum_{m=0}^{k-1} \alpha_{1,0}^{k,m+1} x_1^m y_1^{k-m-1} z_1^{a-k}(x_1 y_p - y_1 x_p) \\ &+ \sum_{k=1}^{a-1}\sum_{m=0}^{k-1} \alpha_{0,0}^{k+1,m+1} x_1^m y_1^{k-m} z_1^{a-k-1}(x_1 z_p - z_1 x_p).\end{aligned}$$

Therefore,

$$\begin{aligned}\theta =& \sum_{k=0}^{a-1} \alpha_{0,0}^{k+1,0} y_1^k z_1^{a-k-1}(y_1 z_p - z_1 y_p) + \sum_{k=0}^{a-1}\sum_{m=0}^{k} \alpha_{0,0}^{k+1,m+1} x_1^m y_1^{k-m} z_1^{a-k-1}(x_1 z_p - z_1 x_p) \\ &+ \sum_{k=0}^{a-1}\sum_{m=0}^{k} \alpha_{1,0}^{k,m+1} x_1^m y_1^{k-m} z_1^{a-k-1}(x_1 y_p - y_1 x_p),\end{aligned}$$

and that gives the basis elements in the third, fourth and fifth row in previous table.

Second, when the total exponent$= a + p$, then θ will given by,

$$\begin{aligned}\theta =& \sum_{k=a+1}^{p-1}\sum_{m=0}^{k}\sum_{i=0}^{b-1}\sum_{j=0}^{i} \lambda_{i,j}^{k,m} x_1^m y_1^{k-m} z_1^{p+a-k} x_p^j y_p^{i-j} z_p^{b-i-1} \\ &+ \sum_{k=0}^{a}\sum_{m=k+1}^{p-1}\sum_{i=0}^{b-1}\sum_{j=0}^{i} \lambda_{i,j}^{k,m} x_1^m y_1^{p+k-m} z_1^{a-k} x_p^j y_p^{i-j} z_p^{b-i-1},\end{aligned}$$

such that $\lambda_{i,j}^{k,m}$ for all i, j, k and m in that range are elements in $\mathbb{F}_p$, since $b = 1$ then

$$\theta = \sum_{k=a+1}^{p-1} \sum_{m=0}^{k} \lambda_{0,0}^{k,m} x_1^m y_1^{k-m} z_1^{p+a-k} + \sum_{k=0}^{a} \sum_{m=k+1}^{p-1} \lambda_{0,0}^{k,m} x_1^m y_1^{p+k-m} z_1^{a-k}.$$

Hence, the basis elements are

$$\begin{aligned} &\{x_1^m y_1^{k-m} z_1^{p+a-k} | a+1 \leq k \leq p-1, 0 \leq m \leq k\} \cup \\ &\{x_1^m y_1^{p+k-m} z_1^{a-k} | 0 \leq k \leq a, k+1 \leq m \leq p-1\} \\ &= \{x_1^i y_1^j z_1^k | i+j+k = a+p \text{ such that } i, j, k < p\}, \end{aligned}$$

which are corresponding to the sixth and seventh rows in that table.

Case 3: If $n = a + p$ and $a = p - 1$, then from relation 5.1

$$\begin{aligned} \theta =& \sum_{k=0}^{p-1} \sum_{m=0}^{k} \alpha_{0,0}^{k,m} x_1^m y_1^{k-m} z_1^{a-k} z_p + \sum_{k=0}^{p-1} \sum_{m=0}^{k} \alpha_{1,0}^{k,m} x_1^m y_1^{k-m} z_1^{a-k} y_p + \\ & \sum_{k=0}^{p-1} \sum_{m=0}^{k} \alpha_{1,1}^{k,m} x_1^m y_1^{k-m} z_1^{a-k} x_p, \end{aligned}$$

using the same techniques that are used in case 2. Substituting the relations from 1 to 4 (the relations in the proof of theorem 5.1.1 case 1 where $a = p - 1$) in previous expression and rearranging it implies,

$$\begin{aligned} \theta =& \alpha_{0,0}^{0,0} z_1^{p-1} z_p + \alpha_{1,0}^{p-1,0} y_1^{p-1} y_p + \alpha_{1,1}^{p-1,p-1} x_1^{p-1} x_p + \sum_{k=0}^{p-2} \alpha_{0,0}^{k+1,0} y_1^k z_1^{p-2-k} (y_1 z_p - z_1 y_p) + \\ & \sum_{k=1}^{p-1} \sum_{m=0}^{k-1} \alpha_{0,0}^{k+1,m+1} x_1^m y_1^{k-m} z_1^{p-2-k} (x_1 z_p - z_1 x_p) + \sum_{k=1}^{p-1} \sum_{m=0}^{k-1} \alpha_{1,0}^{k,m+1} x_1^m y_1^{k-m-1} z_1^{p-1-k} (x_1 y_p - y_1 x_p). \end{aligned}$$

Hence, any θ in this case can be written as a linear combination from the basis in table 5.2 from first till the fourth row from the third group.

The final case, immediately from 5.4 we have

$$\sum_{k=0}^{p-1} \sum_{m=k+1}^{p-1} \beta_{i,j}^{k,m} x_1^m y_1^{p+k-m} z_1^{p-1-k} = \sum_{k=0}^{p-2} \sum_{m=k+1}^{p-1} \beta_{i,j}^{k,m} x_1^m y_1^{p+k-m} z_1^{p-1-k},$$

then we get the last row in the table of basis. □

5.2 Some properties of $M_*(3)$

In this section we will introduce some properties and facts on $M_*(3)$ for a specific case where $p = 3$. We will give a description of the formula of the elements of $M_d(3)$ of higher degrees, precisely for $n \geq p^2$. From one hand, these properties enable us to extend the results of theorem 5.1.1 in case the odd prime $p = 3$. On the other hand, it may help to calculate whole $M_*(3)$ for this prime in a future work.

Before stating these properties, we will make use of the following preliminaries which can be found in [6]. We define the iterated operator e as an algebra homomorphism acting on the generators by $e(x_{p^n}) = x_{p^{n+1}}$, similarly for $e(y_{p^n}) = y_{p^{n+1}}$ and $e(z_{p^n}) = z_{p^{n+1}}$. While, the action of the linear map f on an element $\theta \in H_n(3)$ is given by $f(\theta) = x_1^{p-1}y_1^{p-1}z_1^{p-1}e\theta$.

The following lemmas and the corollary are a special case for three variables from the general one of k-variables, which are stated.

Lemma 5.2.1 (Crossley). *For any arbitrary $\theta \in H_*(\mathbb{C}P^\infty \times \mathbb{C}P^\infty \times \mathbb{C}P^\infty; \mathbb{F}_p)$, and a non-negative integer q,*

$$x_1^{p-1}y_1^{p-1}z_1^{p-1}\mathcal{P}_q(e\theta) = \begin{cases} f\mathcal{P}_t(\theta), & \textit{if } q = tp; \\ 0, & \textit{Otherwise.} \end{cases}$$

Corollary 5.2.2 (Crossley).

$$f(\theta) \in M_{(n+3)p-3}(3) \Longleftrightarrow \theta \in M_n(3)$$

Lemma 5.2.3 (Crossley). *For any polynomial $\theta \in H_*(3)$, then*

$$\mathcal{P}_1(e\theta) = x_1 e\phi + y_1 e\psi + z_1 e\omega,$$

for some $\phi, \psi, \omega \in H_*(3)$.

Corollary 5.2.4. *For any polynomial $\theta \in H_*(3)$ such that $deg(\theta) > 0$. θ does not involve a factor of x, a factor of y or z-factor if and only if $\phi = 0$, $\psi = 0$, or $\omega = 0$ respectively, where ϕ, ψ and ω are those given in lemma 5.2.3.*

Proof. Let θ to be an arbitrary polynomial in $H_*(3)$, then we have to consider the following cases:

Case 1: If θ contains only the z- factor, that is $e\theta$ consists of monomials in the form $z_{p^{n_1}}^{\alpha_1} \cdots z_{p^{n_k}}^{\alpha_k}$, where α_i, n_i are integers for $1 \leq i \leq k$ satisfy $1 \leq \alpha_1 \leq p-1$, $n_1 \neq 0$, for $i = 2, \cdots, k$ $0 \leq \alpha_i \leq p-1$ and $n_1 < \cdots < n_r$. But,

$$\mathcal{P}_1(z_{p^{n_1}}^{\alpha_1} \cdots z_{p^{n_k}}^{\alpha_k}) = (-1)^{n_1-1}\alpha_1 z_1 z_p^{p-1} \cdots z_{p^{n_1}}^{\alpha_1-1} \cdots z_{p^{n_k}}^{\alpha_k}.$$

Extending the action of $\mathcal{P}_1$ linearly on each monomial in $e\theta$, we get

$$\mathcal{P}_1(e\theta) = z_1 e\omega. \tag{5.14}$$

Notice that $e\omega \neq 0$ this is implied by, first; for each monomial $n_1 \neq 0$ so when we apply $\mathcal{P}_1$ the monomial does not vanished, the second reason; there is no cancellations between the image of $\mathcal{P}_1$.

Comparing the relation in lemma 5.2.3 with relation 5.14 we get $x_1 e\phi + y_1 e\psi = 0$, thus from the independence of $x_1 e\phi$ and $y_1 e\psi$, then $e\phi = e\psi = 0$. Hence, $\phi = \psi = 0$. Precisely, by the same way we can show that $\psi = \omega = 0$ and that $\phi = \omega = 0$ if θ involves only x-factor or only y-factor respectively.

Case 2: If θ involves a factor of y, z and it does not contain an x-factor. Then, there is at least one of the constituent monomials is given by the form $y_{p^{n_1}}^{\alpha_1} \cdots y_{p^{n_k}}^{\alpha_k} z_{p^{m_1}}^{\beta_1} \cdots z_{p^{m_s}}^{\beta_s}$, such that the integers n_i, m_j, α_i and β_j where $1 \leq i \leq k$ and $1 \leq j \leq s$ satisfy $n_1 \neq m_1 \neq 0$, $1 \leq \alpha_1, \beta_1 \leq p-1$ $n_1 < \cdots < n_r$, $m_1 < \cdots < m_r$ and $0 \leq \alpha_i, \beta_j \leq p-1$ where $2 \leq i \leq k$ and $2 \leq j \leq s$.

Acting by $\mathcal{P}_1$ on such monomial, and applying *Cartan* formula gives

$$\begin{aligned}\mathcal{P}_1(y_{p^{n_1}}^{\alpha_1} \cdots y_{p^{n_k}}^{\alpha_k} z_{p^{m_1}}^{\beta_1} \cdots z_{p^{m_s}}^{\beta_s}) =& (-1)^{n_1-1}\alpha_1 y_1 y_p^{p-1} \cdots y_{p^{n_1}}^{\alpha_1-1} \cdots y_{p^{n_k}}^{\alpha_k} z_{p^{m_1}}^{\beta_1} \cdots z_{p^{m_s}}^{\beta_s} + \\ & (-1)^{m_1-1}\beta_1 y_{p^{n_1}}^{\alpha_1} \cdots y_{p^{n_k}}^{\alpha_k} z_1 z_p^{p-1} \cdots z_{p^{m_1}}^{\beta_1-1} \cdots z_{p^{m_s}}^{\beta_s}\end{aligned}$$

extending the action of $\mathcal{P}_1$ linearly on each monomial in $e\theta$ and grouping the terms which contain y_1 and the terms involve z_1 individually, implies

$$\mathcal{P}_1(e\theta) = y_1 e\psi + z_1 e\omega, \tag{5.15}$$

for some $\psi, \omega \in H_*(3)$ such that $\psi \neq \omega \neq 0$ for the same reasons that have been stated in the previous case. According to relation 5.15 and the relation in lemma 5.2.3, we have that $x_1 e\phi = 0$, thus $\phi = 0$. By the same way one can show if θ does not involve only y-factor, then $\psi = 0$ and $\phi \neq \omega \neq 0$, or if it is not involving only z-factor, then $\omega = 0$ and $\phi \neq \psi \neq 0$.

In fact there is a possible case to write the polynomial $e\theta$ without the monomial $y_{p^{n_1}}^{\alpha_1} \cdots y_{p^{n_k}}^{\alpha_k} z_{p^{m_1}}^{\beta_1} \cdots z_{p^{m_s}}^{\beta_s}$, when $e\theta = e\theta_1 + e\theta_2$, where θ_1 and θ_2 as same as θ that is considered in the first case, such that θ_1 is a polynomial only contains y-factor and the other only for z. Obviously, the argument in that case implies the result here.

Case 3: If x, y and z are all appear in θ, then θ is given by one of the following case. First $e\theta = e\theta_1 + e\theta_2 + e\theta_3$ such that $e\theta_1, e\theta_2$ and $e\theta_3$ as in the case 1, but each one for a one factor. Then, immediately, from case 1 we get

$$\mathcal{P}_1(e\theta) = x_1 e\phi + y_1 e\psi + z_1 e\omega \tag{5.16}$$

such that $\phi \neq \psi \neq \omega \neq 0$. Second, $e\theta = e\theta_1 + e\theta_2$ such that $e\theta_1$ as in the case 1 for a factor and $e\theta_2$ as in the case 2 for the other factors. Hence, from case 1 and case 2 we get the same result as we have gotten in the first case (of case 3).

Finally, if $e\theta$ contains a monomial in the form $x_{p^{n_1}}^{\alpha_1}\cdots x_{p^{n_k}}^{\alpha_k}y_{p^{m_1}}^{\beta_1}\cdots y_{p^{m_s}}^{\beta_s}z_{p^{l_1}}^{\gamma_1}\cdots z_{p^{l_t}}^{\gamma_t}$ where the integers $\alpha_i, \beta_i, \gamma_i, n_i, m_i$ and γ_i for appropriate i in that range, satisfy some conditions can be deduced from the previous cases. The same techniques that used in previous cases implies the same result as above (first and second case of case 3).

Conversely, suppose that $\theta \in H_*(3)$ such that $\phi = \psi = 0$, if θ contains a factor of y (if it does not contain any factor of x), then from 5.15 we have $\mathcal{P}_1(e\theta) = y_1e\psi + z_1e\omega$, where $\psi \neq \omega \neq 0$, and this is contradiction with our assumption $\psi = 0$, thus θ must not involve any y-factor. Similarly, if it contains a factor of x and there is no y-factor, we will get contradiction, so that; θ is written by z only. By using same argument we can show if $\phi = \omega = 0$ or $\psi = \omega = 0$, then θ consists of only y or only x-factor respectively.

Regarding the case when $\phi = 0$. If θ contains any factor of x, then from 5.16 we have $\mathcal{P}_1(e\theta) = x_1e\phi + y_1e\psi + z_1e\omega$ such that $\phi \neq \psi \neq \omega \neq 0$, contrary to hypothesis that $\phi = 0$, thus θ does not involve any factor of x. Similarly, one can show that if $\psi = 0$ or $\omega = 0$ then θ does not contain y-factor or a factor of z respectively. Hence, the corollary is proven. □

Lemma 5.2.5. *For any polynomial $\theta \in H_*(3)$, then*

$$\mathcal{P}_1(e^2\theta) = x_1x_p^{p-1}e^2\phi + y_1y_p^{p-1}e^2\psi + z_1z_p^{p-1}e^2\omega$$

for some $\phi, \psi, \omega \in H_*(3)$.

Proof. Assume that $\theta \in H_*(3)$, acting twice by the homomorphism e on θ, we get a polynomial such that each constituent monomial have to be given by the form $x_{p^{n_1}}^{\alpha_1}x_{p^{n_2}}^{\alpha_2}\cdots x_{p^{n_r}}^{\alpha_r}y_{p^{m_1}}^{\beta_1}y_{p^{m_2}}^{\beta_2}\cdots y_{p^{m_s}}^{\beta_s}z_{p^{k_1}}^{\gamma_1}z_{p^{k_2}}^{\gamma_2}\cdots z_{p^{k_t}}^{\gamma_t}$ such that $n_1 < \cdots < n_r$, $m_1 < \cdots < m_s$, $k_1 < \cdots < k_t$ and $n_1, m_1, k_1 \geq 2$. Recall that $\mathcal{P}_1(x_{p^r}^n) = (-1)^{r-1}nx_1x_p^{p-1}x_{p^2}^{p-1}\cdots x_{p^r}^{n-1}$, and similarly; for $y_{p^r}^n$ and $z_{p^r}^n$.

The linearity of $\mathcal{P}_1$ and *Cartan* argument implies that, applying $\mathcal{P}_1$ on $e^2\theta$ produces sum of monomials of the form $x_1x_p^{p-1}e^2\Lambda_1$ or $y_1y_p^{p-1}e^2\Lambda_2$ or $z_1z_p^{p-1}e^2\Lambda_3$ i.e. each one contains precisely one and only one factor of $x_1x_p^{p-1}$ or $y_1y_p^{p-1}$ or $z_1z_p^{p-1}$. For instance, $e^2\Lambda_1 = (-1)^{n_1-1}x_{p^2}^{p-1}\cdots x_{p^{n_1}}^{\alpha_1-1}x_{p^{n_2}}^{\alpha_2}\cdots x_{p^{n_r}}^{\alpha_r}y_{p^{m_1}}^{\beta_1}y_{p^{m_2}}^{\beta_2}\cdots y_{p^{m_s}}^{\beta_s}z_{p^{k_1}}^{\gamma_1}z_{p^{k_2}}^{\gamma_2}\cdots z_{p^{k_t}}^{\gamma_t}$.

Now, just gathering the terms that contain the same factor we obtain the result. □

Corollary 5.2.6. *In previous lemma $\phi = 0$ if and only if θ does not involve x-factor. Similarly, the necessary and sufficient condition for $\psi = 0$ or $\omega = 0$, is θ does not contain y-factor or z-factor respectively.*

Proof. By the same argument that has been used in the proof of 5.2.4, we can prove this corollary. □

The following lemmas describe the elements of $M_n(3)$ where $p = 3$ in higher degrees.

Lemma 5.2.7. *When $p = 3$, if $\theta \in M_n(3)$, such that $n \geq p^2$ and $n \equiv 1 \bmod p$, then θ is given by*

$$\theta = \sum_{\substack{i+j+k=p+1 \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k}$$

for some $\theta_{i,j,k} \in M_m(3)$, such that $m = \frac{n-1}{p} - 1$.

Proof. Assume that $\theta \in H_n(3)$ and $n \equiv 1 \bmod p$, this implies

$$\theta = x_1 e\theta_1 + y_1 e\theta_2 + z_1 e\theta_3 + \sum_{\substack{i+j+k=p+1 \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k}$$

for arbitrary polynomials $\theta_1, \theta_2, \theta_3$ and $\theta_{i,j,k}$. Now, since $\theta \in M_n(3)$, then $\theta \in Ker\mathcal{P}_1$. Recall from lemma 5.2.1 that $\mathcal{P}_1(e\theta_i) = x_1 e\phi_i + y_1 e\psi_i + z_1 ew_i$, where $i = 1, 2, 3$, and that; $\mathcal{P}_1(e\theta_{i,j,k}) = x_1 e\phi_{i,j,k} + y_1 e\psi_{i,j,k} + z_1 ew_{i,j,k}$ thus

$$\begin{aligned}\mathcal{P}_1(\theta) =& x_1^2 e\phi_1 + y_1^2 e\psi_2 + z_1^2 ew_3 + x_1 y_1(e\psi_1 + e\phi_2) + x_1 z_1(ew_1 + e\phi_3) + \\ & y_1 z_1(ew_2 + e\psi_3) + \sum_{\substack{i+j+k=p+1 \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k (x_1 e\phi_{i,j,k} + y_1 e\psi_{i,j,k} + z_1 ew_{i,j,k}) = 0.\end{aligned}$$

From the independence of the previous linear terms we get the following. Firstly, $e\phi_1 = 0$, so $\phi_1 = 0$, and that means θ_1 does not contain a factor of x, this implied by corollary 5.2.4. Similarly, there is no y factor and z factor in θ_2 and θ_3 respectively.

Secondly, the relation $e\psi_1 = -e\phi_2$ reveals that $e\theta_1 = y_p.eg(z)$, and $e\theta_2 = x_p.eg(z)$ where $g(z)$ is a polynomial for z, because if we suppose $e\theta_1 = eg^*(yz)$ which is not in the form $y_p \cdot eg(z)$, then applying $\mathcal{P}_1$ produces $y_1 e\psi_1 + z_1 ew_1$ such that $e\psi_1$ have to be involve a factor of y, but θ_2 does not contain a factor of y, so ϕ_2 also does not involve a y-factor and since $e\psi_1 = -e\phi_2$ we get contradiction, thus; $e\theta_1 = y_p.eg(z)$.

The same argument can be applied to show that from relation $ew_1 = -e\phi_3$ we have $e\theta_1 = z_p eh(y)$. These two relations suggest that $e\theta_1 = \lambda y_p z_p$. If $\lambda \neq 0$, then $deg(e\theta_1) = 2p \Rightarrow deg(\theta) = 2p+1$, contrary to hypothesis that $deg(\theta) \geq p^2$. Hence, $\lambda = 0$, i.e. $\theta_1 = 0$. By the same way we can show $\theta_2 = \theta_3 = 0$.

According to the previous argument we get that

$$\theta = \sum_{\substack{i+j+k=p+1 \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k}.$$

Now, $x_1^{p-1-i} y_1^{p-1-j} z_1^{p-1-k}\theta = x_1^{p-1} y_1^{p-1} z_1^{p-1} e\theta_{i,j,k} \in M_m(3)$ where $0 \leq i, j, k \leq p-1$ because in the left hand side $\theta \in M_n(3)$ and $\mathcal{P}_q(x_1^{p-1-i} y_1^{p-1-j} z_1^{p-1-k}) = 0$ for all $q > 0$ so we see that $\theta_{i,j,k} \in M_{\frac{n-1}{p}-1}(3)$ from 5.2.2. □

Lemma 5.2.8. *When $p = 3$, if $\theta \in M_n(3)$, where $n \geq p^2$ and $n \equiv 0 \bmod p$, then θ is given by one of the following forms:*

$$a)\quad \theta = \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k},$$

$$b)\quad \theta = x_1^2 y_1^2 z_1^2 e(\theta^*)$$

$$c)\quad \theta = \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k} + x_1^2 y_1^2 z_1^2 e(\theta^{**})$$

for some $\theta_{i,j,k} \in M_{\frac{n}{p}-1}(3)$, $\theta^* \in M_{\frac{n}{p}-2}(3)$, and $\theta^{**} \notin M_{\frac{n}{p}-2}(3)$.

Proof. Suppose $\theta \in M_n(3)$ such that $n \equiv 0 \bmod p$, so by degree consideration we have

$$\theta = e\theta_1 + \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k} + x_1^2 y_1^2 z_1^2 e(\theta^*)$$

for arbitrary polynomials $\theta_1, \theta_{i,j,k}$ and θ^* in $H_*(3)$. According to our assumption $\theta \in M_n(3)$, so

$$\mathcal{P}_1(\theta) = x_1 e\phi_1 + y_1 e\psi_2 + z_1 e w_3 + \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k (x_1 e\phi_{i,j,k} + y_1 e\psi_{i,j,k} + z_1 e w_{i,j,k}) = 0.$$

Since the terms in previous expression are linearly independent, immediately we see that $\phi_1 = \psi_1 = w_1 = 0$. That is, θ_1 does not involve any x, y, z factors, in other word $\theta_1 = 0$. Thus, θ should be given by the following form, if it belongs to $M_n(3)$

$$\theta = \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k} + x_1^2 y_1^2 z_1^2 e(\theta^*).$$

Now, if $\theta^* \in M_{\frac{n}{p}-2}(3)$, then according to 5.2.2; the second term $\Lambda_2 = x_1^2 y_1^2 z_1^2 e(\theta^*) = f(\theta^*)$ is an element of $M_n(3)$, so $\mathcal{P}_{p^r}(\Lambda_2) = 0$ for $r \geq 0$. Consequently, the first expression $\Lambda_1 = \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k}$ must be an element in $M_n(3)$ since θ belongs to it. Multiplying Λ_1 by $x_1^{p-1-i} y_1^{p-1-j} z_1^{p-1-k}$ illustrates why $\theta_{i,j,k}$ has to be an element in $M_{\frac{n}{p}-2}(3)$. In this case θ is given to be a sum of two elements each one of them in $M_n(3)$ i.e. $\theta = \Lambda_1 + \Lambda_2$. Hence, (a) and (b) from the lemma are proven.

Turning to the case when $\theta^* \notin M_{\frac{n}{p}-2}$, since $\theta \in M_n(3)$ then $x_1^{p-1-i} y_1^{p-1-j} z_1^{p-1-k}\theta = x_1^2 y_1^2 z_1^2 e\theta_{i,j,k} = f(\theta_{i,j,k})$ is an element of $M_{n+2p-(i+j+k)}(3)$, thus $\theta_{i,j,k} \in M_{\frac{n}{p}-1}(3)$ for $0 \leq i, j, k \leq p-1$. □

We have not been able to establish formulas for $\theta \in M_n(3)$ such that $|\theta| \geq p^2$ and $n \equiv 2 \bmod p$.

According to the definition of f we can deduce that if $\theta \in H_n(3)$ such that $n = ap^{\alpha} + \cdots + lp^{\lambda} - 3$, then $m_s = ap^{\alpha+s} + \cdots + lp^{\lambda+s} - 3$ will be the degree for $f^s(\theta)$. The following theorem serves to determine the dimension and the basis elements of $M_{m_s}(3)$, if they are known for $M_n(3)$ for $s \geq 1$.

Theorem 5.2.9. *Let $p = 3$ and $n > 3$ be an integer such that $n \equiv 0 \bmod p$, then the linear injection $f : M_n(3) \longrightarrow M_{(n+2)p}$ is an isomorphism.*

Proof. In the following proof we will applying the lemma 5.2.5 without comment. According to the definition of f and $\theta \in M_n(3) \Longleftrightarrow f(\theta) \in M_{(n+2)p}(3)$, we deduce that f is injective homomorphism. That is, we need to show that if $n \equiv 0 \bmod p$, and $M_{(n+2)p}(3) \neq 0$, then there is no element $\theta \in M_{(n+2)p}$ such that $\theta = \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k}$ or $\theta = \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k} + x_1^2 y_1^2 z_1^2 e(\theta^{**})$ for some $\theta_{i,j,k} \in M_{\frac{n}{p}-1}(3)$, and $\theta^{**} \notin M_{\frac{n}{p}-2}(3)$.

Assume that f in these degrees is not one-to-one correspondence, that means; there is an element $\theta \in M_{(n+2)p}(3)$ such that $\theta \neq f(\Lambda^*)$ where $\Lambda^* \in M_n(3)$, then lemma 5.2.8 implies that

$$\theta = \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k} + x_1^2 y_1^2 z_1^2 e(\theta^{**}),$$

for some $\theta_{i,j,k} \in M_{n+1}(3)$ where $0 \leq i,j,k \leq p-1$ and $\theta^{**} \notin M_n(3)$. Applying 5.2.1 gives $\mathcal{P}_1(x_1^2 y_1^2 z_1^2 e(\theta^{**})) = 0$, then $\Lambda = \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k}$ belongs to $Ker\mathcal{P}_1$, and it is clear that $deg(\theta_{i,j,k}) \equiv 1 \bmod p$ for all i,j,k in that range because $deg(e\theta_{i,j,k}) = (n+1)p$. Therefore, from lemma 5.2.7 $\theta_{i,j,k} = \sum_{\substack{l+m+n=p+1 \\ 0\leq l,m,n\leq p-1}} x_1^l y_1^m z_1^n e\theta_{l,m,n}$ such that $\theta_{l,m,n} \in M(3)$.

Avoiding the same notations, we write $\theta_{i,j,k}$ by the following way

$$\theta_{i,j,k} = y_1^2 z_1^2 e\Lambda_1^{i,j,k} + x_1^2 z_1^2 e\Lambda_2^{i,j,k} + x_1 y_1 z_1^2 e\Lambda_3^{i,j,k} + x_1^2 y_1^2 e\Lambda_4^{i,j,k} + x_1 y_1^2 z_1 e\Lambda_5^{i,j,k} + x_1^2 y_1 z_1 e\Lambda_6^{i,j,k},$$

and hence;

$$\begin{aligned} e\theta_{i,j,k} =& y_p^2 z_p^2 e^2 \Lambda_1^{i,j,k} + x_p^2 z_p^2 e^2 \Lambda_2^{i,j,k} + x_p y_p z_p^2 e^2 \Lambda_3^{i,j,k} + x_p^2 y_p^2 e^2 \Lambda_4^{i,j,k} + x_p y_p^2 z_p e^2 \Lambda_5^{i,j,k} + \\ & x_p^2 y_p z_p e^2 \Lambda_6^{i,j,k}. \end{aligned}$$

Recall that $\mathcal{P}_1(\Lambda) = \mathcal{P}_1\left(\sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k}\right) = 0$ and *Cartan* formula, implies that $\mathcal{P}_1(x_1^2\Lambda) = 0$, and since $x_1^2\Lambda = x_1^2 y_1^2 z_1 e\theta_{0,2,1} + x_1^2 y_1 z_1^2 e\theta_{0,1,2}$, so

$$\begin{aligned} \mathcal{P}_1(x_1^2\Lambda) =& x_1^2 y_1^2 z_1^2 (2 y_p^2 z_p e^2 \Lambda_1^{0,2,1} + 2 x_p^2 z_p e^2 \Lambda_2^{0,2,1} + 2 x_p y_p z_p e^2 \Lambda_3^{0,2,1} + x_p^2 y_p^2 z_p^2 e^2 \omega_4^{0,2,1} + \\ & x_p y_p^2 e^2 \Lambda_5^{0,2,1} + x_p^2 y_p e^2 \Lambda_6^{0,2,1}) + x_1^2 y_1^2 z_1^2 (2 y_p z_p^2 e^2 \Lambda_1^{0,1,2} + x_p^2 y_p^2 z_p^2 e^2 \psi_2^{0,1,2} + \\ & x_p z_p^2 e^2 \Lambda_3^{0,1,2} + 2 x_p^2 y_p e^2 \Lambda_4^{0,1,2} + 2 x_p y_p z_p e^2 \Lambda_5^{0,1,2} + x_p^2 z_p e^2 \Lambda_6^{0,1,2}) = 0. \end{aligned}$$

By the linear independence of the terms of the previous expression we infer (and if one considers $\mathcal{P}_1(y_1^2\Lambda) = 0$ and $\mathcal{P}_1(z_1^2\Lambda) = 0$)

1) $\Lambda_1^{0,2,1}=\Lambda_5^{0,2,1}=0,$ 7) $\Lambda_2^{1,0,2}=\Lambda_3^{1,0,2}=0,$ 13) $\Lambda_4^{1,2,0}=\Lambda_5^{1,2,0}=0,$

2) $\Lambda_1^{0,1,2}=\Lambda_3^{0,1,2}=0,$ 8) $\Lambda_2^{2,0,1}=\Lambda_6^{2,0,1}=0,$ 14) $\Lambda_4^{2,1,0}=\Lambda_6^{2,1,0}=0,$

3) $\Lambda_2^{0,2,1}=\Lambda_6^{0,1,2},$ 9) $\phi_1^{1,0,2}=-\omega_4^{2,0,1},$ 15) $\phi_1^{1,2,0}=-\psi_2^{2,1,0},$

4) $\Lambda_3^{0,2,1}=-\Lambda_5^{0,1,2},$ 10) $\Lambda_4^{1,0,2}=\Lambda_5^{2,0,1},$ 16) $\Lambda_3^{1,2,0}=\Lambda_1^{2,1,0},$

5) $\Lambda_6^{0,2,1}=\Lambda_4^{0,1,2},$ 11) $\Lambda_5^{1,0,2}=\Lambda_1^{2,0,1},$ 17) $\Lambda_2^{1,2,0}=\Lambda_3^{2,1,0},$

6) $\omega_4^{0,2,1}=-\psi_2^{0,1,2},$ 12) $\Lambda_6^{1,0,2}=-\Lambda_3^{2,0,1},$ 18) $\Lambda_6^{1,2,0}=-\Lambda_5^{2,1,0},$

Now, substituting the zero's components in Λ, and considering $x_1y_1\Lambda=x_1^2y_1z_1^2e\theta_{1,0,2}+x_1^2y_1^2z_1e\theta_{1,1,1}+x_1y_1^2z_1^2e\theta_{0,1,2}$ which has $\mathcal{P}_1(x_1y_1\Lambda)=0$, gives

$$\begin{aligned}\mathcal{P}_1(x_1y_1\Lambda)=&x_1^2y_1^2z_1^2(2y_pz_p^2e^2\Lambda_1^{1,0,2}+2x_p^2y_pe^2\Lambda_4^{1,0,2}+2x_py_pz_pe^2\Lambda_5^{1,0,2}+x_p^2z_pe^2\Lambda_6^{1,0,2})+\\&x_1^2y_1^2z_1^2(2y_p^2z_pe^2\Lambda_1^{1,1,1}+2x_p^2z_pe^2\Lambda_2^{1,1,1}+2x_py_pz_pe^2\Lambda_3^{1,1,1}+x_p^2y_p^2z_p^2e^2\omega_4^{1,1,1}+\\&x_py_p^2e^2\Lambda_5^{1,1,1}+x_p^2y_pe^2\Lambda_6^{1,1,1})+x_1^2y_1^2z_1^2(2x_pz_p^2e^2\Lambda_2^{0,1,2}+2x_py_p^2e^2\Lambda_4^{0,1,2}+\\&y_p^2z_pe^2\Lambda_5^{0,1,2}+2x_py_pz_pe^2\Lambda_6^{0,1,2})\\=&2x_1^2y_1^2z_1^2y_pz_p^2e^2\Lambda_1^{1,0,2}+x_1^2y_1^2z_1^2x_p^2y_p^2z_p^2e^2\omega_4^{1,1,1}+2x_1^2y_1^2z_1^2x_pz_p^2e^2\Lambda_2^{0,1,2}+\\&x_1^2y_1^2z_1^2x_p^2y_p(2\Lambda_4^{1,0,2}+\Lambda_6^{1,1,1})+x_1^2y_1^2z_1^2x_p^2z_p(e^2\Lambda_6^{1,0,2}+2e^2\Lambda_2^{1,1,1})+\\&x_1^2y_1^2z_1^2y_p^2z_p(\Lambda_5^{0,1,2}+\Lambda_1^{1,1,1})+x_1^2y_1^2z_1^2x_py_p^2(e^2\Lambda_4^{0,1,2}+2e^2\Lambda_5^{1,1,1})+\\&2x_1^2y_1^2z_1^2x_py_pz_p(\Lambda_5^{1,0,2}+\Lambda_3^{1,1,1}+\Lambda_6^{0,1,2})=0\end{aligned}$$

so the linearity and the independece of the terms of $\mathcal{P}_1(x_1y_1\Lambda)$, implies the following

1) $\Lambda_1^{1,0,2}=\Lambda_2^{0,1,2}=\omega_4^{1,1,1}=0,$

2) $\Lambda_4^{1,0,2}=\Lambda_6^{1,1,1},$

3) $\Lambda_6^{1,0,2}=\Lambda_2^{1,1,1},$

4) $\Lambda_5^{0,1,2}=\Lambda_1^{1,1,1},$

5) $\Lambda_4^{0,1,2}=\Lambda_5^{1,1,1},$

6) $\Lambda_5^{1,0,2}+\Lambda_3^{1,1,1}+\Lambda_6^{0,1,2}=0.$

By the same argument if we consider $x_1z_1\Lambda$ and $y_1z_1\Lambda$ we get

1) $\Lambda_1^{1,2,0}=\Lambda_4^{0,2,1}=\psi_2^{1,1,1}=0,$ 7) $\Lambda_2^{2,1,0}=\Lambda_4^{2,0,1}=\phi_1^{1,1,1}=0,$

2) $\Lambda_2^{1,2,0}=\Lambda_6^{1,1,1},$ 8) $\Lambda_1^{2,1,0}=\Lambda_5^{1,1,1},$

3) $\Lambda_6^{1,2,0}=\Lambda_4^{1,1,1},$ 9) $\Lambda_5^{2,1,0}=\Lambda_4^{1,1,1},$

4) $\Lambda_3^{0,2,1}=\Lambda_1^{1,1,1},$ 10) $\Lambda_1^{2,0,1}=\Lambda_3^{1,1,1},$

5) $\Lambda_2^{0,2,1} = \Lambda_3^{1,1,1}$,

6) $\Lambda_3^{1,2,0} + \Lambda_5^{1,1,1} + \Lambda_6^{0,2,1} = 0$,

11) $\Lambda_3^{2,0,1} = \Lambda_2^{1,1,1}$,

12) $\Lambda_3^{2,1,0} + \Lambda_6^{1,1,1} + \Lambda_5^{2,0,1} = 0$,

On the other hand, $\theta_{i,j,k} \in M_*(3)$ for $0 \le i,j,k \le p-1$, that is; $\mathcal{P}_1(\theta_{i,j,k}) = 0$, denote to $\mathcal{P}_1(e\Lambda_i^{i,j,k}) = x_1 e\hat{\phi}_i^{i,j,k} + y_1 e\hat{\psi}_i^{i,j,k} + z_1 e\hat{\omega}_i^{i,j,k}$, so we will deal with two cases of $\theta_{i,j,k}$ and see what they produce, and by using same argument someone can deal with the other cases. Firstly, after substituting the zero's components that we get from the last relations we have

$$\begin{aligned}\mathcal{P}_1(\theta_{0,2,1}) =& \mathcal{P}_1(x_1^2 z_1^2 e\Lambda_2^{0,2,1} + x_1 y_1 z_1^2 e\Lambda_3^{0,2,1} + x_1^2 y_1 z_1 \Lambda_6^{0,2,1}) \\ =& x_1^2 y_1 z_1^2 e\hat{\psi}_2^{0,2,1} + x_1^2 y_1 z_1^2 e\hat{\phi}_3^{0,2,1} + x_1 y_1^2 z_1^2 e\hat{\psi}_3^{0,2,1} + x_1^2 y_1^2 z_1 e\hat{\psi}_6^{0,2,1} + x_1^2 y_1 z_1^2 e\hat{\omega}_6^{0,2,1} \\ =& 0\end{aligned}$$

The independence of the summands of $\mathcal{P}_1(\theta_{0,2,1})$ gives, $\hat{\psi}_3^{0,2,1} = \hat{\psi}_6^{0,2,1} = 0$, and $\hat{\psi}_2^{0,2,1} + \hat{\phi}_3^{0,2,1} + \hat{\omega}_6^{0,2,1} = 0$, so that; neither $\Lambda_3^{0,2,1}$ nor $\Lambda_6^{0,2,1}$ involve y-factor. While; $\phi_1^{1,1,1} = 0$ and $\Lambda_1^{1,1,1} = \Lambda_3^{0,2,1}$ implies that $\Lambda_3^{0,2,1}$ does not contain x-factor. Thus, $\Lambda_3^{0,2,1}$ is a polynomial which involves only z-factor, and because of $\Lambda_3^{0,2,1} \in M_*(3)$ see lemma 5.2.7, $\Lambda_3^{0,2,1} = \xi z_1^{p-1} z_p^{p-1} \cdots z_{p^r}^i$ for appropriate i, r see chapter 4, theorem 4.2.2.

Secondly,

$$\begin{aligned}\mathcal{P}_1(\theta_{0,1,2}) =& \mathcal{P}_1(x_1^2 y_1^2 e\Lambda_4^{0,1,2} + x_1 y_1^2 z_1 e\Lambda_5^{0,1,2} + x_1^2 y_1 z_1 \Lambda_6^{0,1,2}) \\ =& x_1^2 y_1^2 z_1 e\hat{\omega}_4^{0,1,2} + x_1^2 y_1^2 z_1 e\hat{\phi}_5^{0,1,2} + x_1 y_1^2 z_1^2 e\hat{\omega}_5^{0,1,2} + x_1^2 y_1^2 z_1 e\hat{\psi}_6^{0,1,2} + x_1^2 y_1 z_1^2 e\hat{\omega}_6^{0,1,2} \\ =& x_1^2 y_1 z_1^2 e\hat{\omega}_6^{0,1,2} + x_1 y_1^2 z_1^2 e\hat{\omega}_5^{0,1,2} + x_1^2 y_1^2 z_1 (e\hat{\omega}_4^{0,1,2} + e\hat{\phi}_5^{0,1,2} + e\hat{\psi}_6^{0,1,2}) = 0\end{aligned}$$

Similarly, from the independence of the terms of the previous expression we get the following relations $\hat{\omega}_6^{0,1,2} = \hat{\omega}_5^{0,1,2} = 0$, and $\hat{\omega}_4^{0,1,2} + \hat{\phi}_5^{0,1,2} + \hat{\psi}_6^{0,1,2} = 0$. The first relation shows that there is no z-factor in $\Lambda_5^{0,1,2}$, but that contrast $\Lambda_5^{0,1,2} = -\Lambda_3^{0,2,1} = -\xi z_1^{p-1} z_p^{p-1} \cdots z_{p^r}^i$, unless $\xi = 0$ and if it is; then we get $\Lambda_5^{0,1,2} = \Lambda_3^{0,2,1} = \Lambda_1^{1,1,1} = 0$ (from $\Lambda_5^{0,1,2} = \Lambda_1^{1,1,1}$).

Therefore, the second relation is given alternatively by $\hat{\omega}_4^{0,1,2} = -\hat{\psi}_6^{0,1,2}$, likewise; $\hat{\psi}_2^{0,2,1} = -\hat{\omega}_6^{0,2,1}$. Now, since $\Lambda_6^{0,2,1}$ does not contain y-factor, so that $\hat{\omega}_6^{0,2,1}$ and $\hat{\psi}_2^{0,2,1}$ do not involve y-factor, that is; either $\Lambda_2^{0,2,1} = 0$, or $\Lambda_2^{0,2,1} = y_1 \cdot g(x,z)$ where $g(x,z)$ an arbitrary polynomial in x and z. On the other hand, $\Lambda_2^{0,2,1} = \Lambda_6^{0,1,2}$, and $\Lambda_6^{0,1,2}$ does not involve z-factor implies that $\Lambda_2^{0,2,1} = y_1 \cdot h(x)$, and since $\Lambda_2^{0,2,1} \in M_*(3)$, then $\Lambda_2^{0,2,1} = \Lambda_6^{0,1,2} = y_1 x_1^{p-1} x_p^{p-1} \cdots x_{p^r}^i$. By same argument we get $\Lambda_4^{0,1,2} = \Lambda_6^{0,2,1} = -z_1 x_1^{p-1} x_p^{p-1} \cdots x_{p^r}^i$.

Using same techniques show that from $\theta_{1,2,0}$ and $\theta_{2,1,0}$ we get the following $\Lambda_6^{1,2,0} = \Lambda_5^{2,1,0} = \Lambda_4^{1,1,1} = 0$ ($\Lambda_5^{2,1,0} = \Lambda_4^{1,1,1}$), $\Lambda_2^{1,2,0} = \Lambda_3^{2,1,0} = -y_1 z_1^{p-1} z_p^{p-1} \cdots z_{p^r}^i$, and $\Lambda_3^{1,2,0} = \Lambda_1^{2,1,0} = x_1 z_1^{p-1} z_p^{p-1} \cdots z_{p^r}^i$. Whereas, $\theta_{1,0,2}$ and $\theta_{2,0,1}$ gives $\Lambda_6^{1,0,2} = \Lambda_3^{2,0,1} = \Lambda_2^{1,1,1} = 0$ ($\Lambda_3^{2,0,1} = \Lambda_2^{1,1,1}$), $\Lambda_4^{1,0,2} = \Lambda_5^{2,0,1} = z_1 y_1^{p-1} y_p^{p-1} \cdots y_{p^r}^i$, and $\Lambda_5^{1,0,2} = \Lambda_1^{2,0,1} = -x_1 y_1^{p-1} y_p^{p-1} \cdots y_{p^r}^i$.

First, $\Lambda_4^{0,1,2} = \Lambda_5^{1,1,1}$ and $\Lambda_1^{2,1,0} = \Lambda_5^{1,1,1}$, but this is contradiction unless $\Lambda_4^{0,1,2} = \Lambda_1^{2,1,0} = \Lambda_5^{1,1,1} = 0$, and this implies $\Lambda_6^{0,2,1} = \Lambda_3^{1,2,0} = 0$. Furthermore, $\Lambda_2^{0,2,1} = \Lambda_3^{1,1,1}$ and $\Lambda_1^{2,0,1} =$

$\Lambda_3^{1,1,1}$ gives $\Lambda_2^{0,2,1} = \Lambda_1^{2,0,1} = \Lambda_3^{1,1,1} = 0$, so that; $\Lambda_6^{0,1,2} = \Lambda_5^{1,0,2} = 0$. Finally, $\Lambda_2^{1,2,0} = \Lambda_6^{1,1,1}$ and $\Lambda_4^{1,0,2} = \Lambda_6^{1,1,1}$ provides $\Lambda_2^{1,2,0} = \Lambda_4^{1,0,2} = \Lambda_6^{1,1,1} = 0$ and $\Lambda_3^{2,1,0} = \Lambda_5^{2,0,1} = 0$. Thus, $\theta_{i,j,k} = 0$ for all i, j and k such that $0 \leq i, j, k \leq p-1$ since all their components are vanished. Hence, $\Lambda = \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k} = 0$, that is

$$\theta = x_1^2 y_1^2 z_1^2 e(\theta^{**})$$

Precisely, by the same argument we can show there is no element $\theta \in M_{(n+2)p}(3)$ such that $\theta = \sum_{\substack{i+j+k=p \\ 0\leq i,j,k\leq p-1}} x_1^i y_1^j z_1^k e\theta_{i,j,k}$. Hence, the proof is completed. □

Chapter 6

The subring of lines $L_*(k)$.

6.1 Comments and the construction of $g^{tr}_{r,i}(\alpha_1, \ldots, \alpha_k)$.

Let us consider the right action of $GL(k, \mathbb{F}_p) \cong GL(V)$ on *Hopf* algebra $\mathbb{F}_p[x_1, \cdots x_k] \cong H^*((\mathbb{C}P^\infty)^k, \mathbb{F}_p)$ where $|x_i| = 2$ for $i = 1, \cdots, k$, using *linear substitutions*, that means: if $g = (g_{i,j}) \in GL(V)$ and $x_i \in \mathbb{F}_p[x_1, \cdots, x_k]$, then

$$x_i \triangleleft g = g(x_i) = \sum_{j=1}^{k} g_{i,j} x_j,$$

for $1 \leq i \leq k$, which is extended to all $\theta \in \mathbb{F}_p[x_1, \cdots, x_k]$ by the action,

$$(\theta \triangleleft g)(x_1, x_2, \cdots, x_n) = \theta(x_1 \triangleleft g, \cdots, x_k \triangleleft g).$$

So that, we can view $\mathbb{F}_p[x_1, \ldots, x_k]$ as a right $GL(k, \mathbb{F}_p)$-module.

In fact, this action has been derived from the action of $GL(V)$ on V via a linear transformation, this reveals that each $g \in GL(V)$ induces a *Hopf* algebra homomorphism on $H^*(BV)/H^1(BV)$. Thus, if one thinks of g as a matrix and $H^*(BV)/H^1(BV) \cong \mathbb{F}_p[x_1, \cdots, x_n]$, then

$$g(x_1) = \sum_{j=1}^{k} g_{1,j} x_j, \cdots \text{ and } g(x_k) = \sum_{j=1}^{k} g_{k,j} x_j.$$

Since g is an algebra homomorphism,

$$g(x_1^{\alpha_1} \cdots x_k^{\alpha_k}) = g(x_1)^{\alpha_1} \cdots g(x_k)^{\alpha_k}, \quad \text{for } \alpha_i \in \mathbb{N}_0, i \in \{1, \cdots, k\},$$

and using the linearity of g gives the action of $GL(n, \mathbb{F}_p)$ on any polynomial $\theta \in \mathbb{F}_p[x_1, \cdots, x_k]$.

Motivated by the definition of total *Steenrod* square Sq in [28], and see also [22] we define the total *Steenrod* mod p as follows.

Definition 6.1.1 (Total Steenrod mod p). The algebra map $\mathcal{P} : P(k) \longrightarrow P(k)$ that is defined by $\mathcal{P}(1) = 1$ and $\mathcal{P}(x_n) = x_n + x_n^p$, is called *total Steenrod mod p*, where p is an odd prime, and $P(k)$ is the graded polynomial algebra in k variables over $\mathbb{F}_p$.

Proposition 6.1.2. *The right $GL(k, \mathbb{F}_p)$ action on $P(k)$ commutes with the action of $\mathcal{P}$ on $P(k)$, i.e. $\mathcal{P}(\theta \lhd g) = \mathcal{P}(\theta) \lhd g$, where $\theta \in P(k)$ and $g \in GL(k, \mathbb{F}_p)$.*

Proof. Using the fact that both $\mathcal{P}$ and g are maps of algebra implies that we need to consider θ as a variable. Thus,

$$\begin{aligned}\mathcal{P}(\theta \lhd g) =& \mathcal{P}(x_n \lhd g),\\ =&\mathcal{P}(\sum_{j=1}^{k} g_{n,j}x_j),\\ =&\sum_{j=1}^{k} g_{n,j}\mathcal{P}(x_j),\\ =&\sum_{j=1}^{k} g_{n,j}x_j + \sum_{j=1}^{k} g_{n,j}x_j^p.\end{aligned}$$

On the other hand,

$$x_n^p \lhd g = (g_{n,1}x_1 + \cdots + g_{n,k}x_k)^p = \sum_{t_1+t_2+\cdots+t_k=p} \frac{p!}{t_1! \cdots t_k!} g_{n,1}^{t_1} x_1^{t_1} \cdots g_{n,k}^{t_k} x_k^{t_k},$$

but each summand in the right previous expression is zero since $\frac{p!}{t_1!\cdots t_k!} \equiv 0 \bmod p$, unless $t_i = p$ for $i = 1, \cdots k$ and when this happen, we get $g_{n,i}^p = g_{n,i}$ because $g_{n,i} \in \mathbb{F}_p$ and $g_{n,i}^{p-1} = 1$, so $(g_{n,1}x_1 + \cdots + g_{n,k}x_k)^p = \sum_{j=1}^{k} g_{n,j}x_j^p$. Hence,

$$\begin{aligned}\mathcal{P}(\theta \lhd g) =& \sum_{j=1}^{k} g_{n,j}x_j + \sum_{j=1}^{k} g_{n,j}x_j^p,\\ &= x_n \lhd g + x_n^p \lhd g,\\ &= (x_n + x_n^p) \lhd g,\\ &= \mathcal{P}(x_n) \lhd g.\end{aligned}$$

□

Turning to the dual case $H_*((\mathbb{C}P^\infty)^k, \mathbb{F}_p) \cong H_*(k)$, where $H_*(k)$ is a *Divided Power Algebra* of k variables over $\mathbb{F}_p$ (the product of divided power algebra has been induced from the coproduct of $H^*(BV)$ which is $\Delta(x) = x \otimes 1 + 1 \otimes x$, as we have seen in chapter 3.2). Similarly, for each $g \in GL(k, \mathbb{F}_p)$, g^{tr} acts on the right of $H_*(BV)/H_1(BV)$ by linear substitutions and this action commutes with the dual *Steenrod* operations. In other word,

$$y_i \lhd g^{tr} = g^{tr}(y_i) = \sum_{j=1}^{k} g_{j,i}y_j = \sum_{j=1}^{k} g_{i,j}^{tr}y_j,$$

$$\theta(y_1,\cdots,y_n)\lhd g^{tr}=\theta(y_1\lhd g^{tr},\cdots,y_n\lhd g^{tr})$$

and

$$\mathcal{P}_q(\theta\lhd g^{tr})=\mathcal{P}_q(\theta)\lhd g^{tr},$$

where $\theta\in H_*(k)$. The last property shows that

$$g^{tr}:M_*(1)\longrightarrow M_*(k).$$

The main idea here is finding the image of the spike $x_1^{p-1}x_p^{p-1}\cdots x_{p^{r-1}}^{p-1}x_{p^r}^i\in M_{(i+1)p^r-1}(1)$ under g^{tr} where $g^{tr}\in GL(k,\mathbb{F}_p)$. We denoted to $g^{tr}(x_1^{p-1}x_p^{p-1}\cdots x_{p^r}^i)$ by $g^{tr}_{r,i}(\alpha_1,\cdots,\alpha_k)$ where $\alpha_i\in\mathbb{F}_p$ for $i=1,\cdots,k$ are the entries of the first column in g^{tr}, and $L_*(k)$ for the graded ring that is generated by $\{g^{tr}_{r,i}(\alpha_1,\cdots,\alpha_k)|(\alpha_1,\cdots,\alpha_k)\in\mathbb{F}_p^k,\text{ and } i,r\geq 0\}$. $L_*(k)$ is said to be the **subring of lines**.

Assuming that $(x_1)_{p^i},(x_2)_{p^i},\cdots,(x_k)_{p^i}$ are generators of $H_*(k)$ which are dual to the $x_1^{p^i},x_2^{p^i},\cdots,x_k^{p^i}$ in $P(k)$ respectively for $i\geq 0$. According to $(x_i)_n\cdot(x_i)_m=\binom{n+m}{m}(x_i)_{n+m}$, those generators are the indecomposable elements in $H_*(k)$. Then $<\theta\lhd g^{tr},\Lambda>=<\theta,\Lambda\lhd g>$, where $\theta\in H_*(k)$ and $\Lambda\in P(k)$. Therefore,

.

$$\begin{aligned}\langle(x_1)_n\lhd g^{tr},x_1^{t_1}\cdots x_k^{t_k}\rangle &=\langle(x_1)_n,(\alpha_1x_1+\cdots\kappa_1x_k)^{t_1}\cdots(\alpha_kx_1+\cdots\kappa_kx_k)^{t_k}\rangle\\ &=\begin{cases}\alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_k^{t_k}, & \text{if } t_1+t_2+\cdots+t_k=n;\\ 0, & \text{if } t_1+t_2+\cdots+t_k\neq n.\end{cases}\end{aligned}$$

where $t_1,\cdots,t_k\in\mathbb{N}_0$. Consequently,

$$g^{tr}\left((x_1)_n\right)=\sum_{t_1+t_2+\cdots+t_k=n}\alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_k^{t_k}(x_1)_{t_1}(x_2)_{t_2}\cdots(x_k)_{t_k}\tag{6.1}$$

Since g^{tr} is a homomorphism as we have seen, thus finding $g^{tr}(x_1^{p-1}x_p^{p-1}\cdots x_{p^r}^i)$ will be required to calculate $g^{tr}(x_{p^s})$ such that $0\leq s\leq r$ that we denoted by u_{p^s}, so by 6.1

$$u_{p^s}=\sum_{t_1+t_2+\cdots+t_k=p^s}\alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_k^{t_k}(x_1)_{t_1}(x_2)_{t_2}\cdots(x_k)_{t_k}.\tag{6.2}$$

From the first glance and basing on the results in [6, 7], we may be expect that $u_{p^s}=e^su_1=(\alpha_1(x_1)_{p^s}+\alpha_2(x_2)_{p^s}+\cdots+\alpha_k(x_k)_{p^s})$, but the following discussion shows otherwise.

Now, assume $p\geq k$, and take the p-adic expansion of t_i for $i=1,\cdots,k$ to be
$t_1=t_{1,0}+t_{1,1}p+\cdots+t_{1,s}p^s$,
$t_2=t_{2,0}+t_{2,1}p+\cdots+t_{2,s}p^s$,
.
.
.
$t_k=t_{k,0}+t_{k,1}p+\cdots+t_{k,s}p^s$,

where $0 \le t_{i,j} \le p-1$ for $1 \le i \le k$ and $0 \le j \le s$. Set $b_0 = \sum_{j=1}^{k} t_{j,0}, \cdots, b_k = \sum_{j=1}^{k} t_{j,k}$. Hence, $p^s = b_0 + b_1 p + \cdots + b_s p^s$ such that $0 \le b_i \le k(p-1)$ for $i = 0, 1, \cdots, s-2$, whilst $0 \le b_{s-1} \le p$, and $b_s = 0, 1$. In fact we can find b_i by the following. Since p/p^s, so $b_0 = n_0 p$ such that $n_0 = 0, 1, \cdots k-1$(because $(k-1)p \le k(p-1)$ iff $p \ge k$). While, $b_1 = n_1 p$ if $b_0 = 0$, otherwise; $b_1 = n_1 p - n_0$, so that

$$b_1 = \begin{cases} n_1 p, & \text{if } n_0 = 0; \\ n_1 p - n_0, & \text{if } n_0 \ne 0. \end{cases}$$

such that $0 \le n_1 \le k-1$. likewise;

$$b_i = \begin{cases} n_i p, & \text{if } n_{i-1} = 0; \\ n_i p - n_{i-1}, & \text{otherwise.} \end{cases}$$

where $0 \le n_i \le k-1$ for $2 \le i \le s-2$. In the case of b_{s-1} there is slightly different from the other, like b_s because $b_{s-1} = p - n_{s-2}$, and

$$b_s = \begin{cases} 1, & \text{if } b_{s-1} = 0; \\ 0, & \text{if } b_{s-1} \ne 0. \end{cases}$$

Note if $b_i = 0$, then $b_j = 0$ for $0 \le j < i$ otherwise we get a contradiction. In contrast, when $b_s = 0$ it has to be at least $b_{s-1} \ne 0$, and if $b_s = 1$, then $b_0 = \cdots = b_{s-1} = 0$.

Definition 6.1.3. For each value of $b_0, b_1, \cdots, b_s$ which are defined as above, the string

$$p^s = b_0 + b_1 p + \cdots + b_s p^s,$$

is called a **type of** p^s.

Proposition 6.1.4. *If $k \le p$, then the number of all types of p^s is given by*

$$1 + \sum_{i=0}^{s-1} (k-1)^i$$

Proof. The proof will be achieved by induction on s. The first step when $s = 0$, so it is clearly that $b_0 = 1$, and we have not other cases, so the number of type is 1. Assume if $s = m-1$, then the number of types of p^{m-1} is given by $1 + 1 + (k-1) + \cdots + (k-1)^{m-2}$. Now, when $s = m$, then each type of $p^{m-1} = b_0 + b_1 p + \cdots + b_{m-1} p^{m-1}$ can be regarded as a type of p^m by multiplying this type by p. Therefore, a large chunk of types of p^m have been already known, and we need only to account the types such that $b_0 \ne 0$.

But, if $b_0 \ne 0$, then $b_1 = n_1 p - n_0 \ne 0$, and so on until $b_{m-2} = n_{m-2} p - n_{m-3} \ne 0$, and $b_{m-1} = p - n_{m-2} \ne 0, p$. On the other hand, we have $k-1$ choice for b_0 since $b_0 = n_0 p$, and $n_0 = 1, \cdots k-1$, and for each one of these choices also we have $k-1$ choice for b_1, so we get $(k-1)^2$ types from b_0 and b_1, thus up to b_{m-2} there are $(k-1)^{m-1}$ types.finally,

b_{m-1} is determined totally by n_{m-2}, so we still have $(k-1)^{m-1}$ types, and in this case $b_m = 0$.

Hence, from induction step and this case we conclude there are $1 + \sum_{i=0}^{m-1} (k-1)^i$ types of p^m. Thus, the proposition is proven. □

Returning to our task which is the calculation of u_{p^s} for $s \geq 0$ in relation 6.2. If $s = 0$, then according to previous proposition we have one type for this value of s, and from 6.2 we get

$$u_1 = \alpha_1(x_1)_1 + \alpha_2(x_2)_1 + \cdots + \alpha_k(x_k)_1.$$

We need to consider u_1 as an element belongs to $\mathbb{Z}[(x_1)_1, \cdots, (x_k)_1]/[(x_1)_1^p, \cdots, (x_k)_1^p]$, so $u_1^p = (\alpha_1(x_1)_1 + \alpha_2(x_2)_1 + \cdots + \alpha_k(x_k)_1)^p$ is divisible by p. Let w_1 be the unique with $pw_1 = (\alpha_1(x_1)_1 + \alpha_2(x_2)_1 + \cdots + \alpha_k(x_k)_1)^p$. In fact $w_1 \in \mathbb{F}_p[(x_1)_1, \cdots, (x_k)_1]/[(x_1)_1^p, \cdots, (x_k)_1^p]$, precisely

$$w_1 = \sum_{\substack{i_1+\cdots+i_k=p \\ i_1,\cdots i_k<p}} \frac{(p-1)!}{i_1!\cdots i_k!} \alpha_1^{i_1} \cdots \alpha_k^{i_k} (x_1)_1^{i_1} \cdots (x_k)_1^{i_k}$$

According to the previous construction of w_1, we conclude the following lemma which will be useful in the next theorem.

Lemma 6.1.5. *Let k, n are a positive integers such that $2 \leq k \leq p$, then*

a) $w_1^n = 0$, if $n \geq k$,

b) $u_1^{p-(n-1)} \cdot w_1^{k-1} = 0$, when $2 \leq n \leq k$.

Proof. Both parts of the lemma can be proven by the same idea which is if $\theta \in \mathbb{F}_p[(x_1)_1, \cdots, (x_k)_1]/[(x_1)_1^p, \cdots, (x_k)_1^p]$, then $0 \leq deg(\theta) \leq k(p-1)$ (see the proof of theorem 5.1.1 case 3[1]). Otherwise, i.e. when $deg(\theta) > k(p-1)$, implies $\theta = 0$ because the truncation property.

Immediately, from the construction of w_1 we have $deg(w_1) = p$, thus $deg(w_1^n) = np$, so when $n \geq k$ we get $w_1^n = 0$. By the same way, $deg(u_1^{p-(n-1)} \cdot w_1^{k-1}) = kp + 1 - n$, but for any value of $2 \leq n \leq k$ we see $kp + 1 - n > kp - k$, so $u_1^{p-(n-1)} \cdot w_1^{k-1} = 0$. □

Theorem 6.1.6. *If $k \leq p$, then u_{p^s} can be written in terms of u_1, w_1 and e. In fact,*

$$u_{p^s} = \sum \prod_{n=0}^{s} e^n \left(\frac{(-1)^{c_n} u_1^{d_n} w_1^{c_n}}{c_n! d_n!} \right)$$

summands over all $b_0, b_1, \cdots, b_s$ where $p^s = b_0 + b_1 p + \cdots + b_s p^s$ is a type of p^s, such that $b_n = c_n p + d_n$ and $0 \leq c_n, d_n \leq p-1$, for $0 \leq n \leq s$.

[1]In that case we have dealt with three variables, but one can easily generalise this fact for any k variables.

Proof. For a fixed type of $p^s = b_0 + b_1 p + \cdots + b_s p^s$, relation 6.2 shows

$$\begin{aligned} u_{p^s} &= \sum_{t_1+\cdots+t_k=p^s} \alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_k^{t_k}(x_1)_{t_1}(x_2)_{t_2}\cdots(x_k)_{t_k}, \\ &= \sum_{\substack{t_1+\cdots+t_k=p^s \\ t_{1,0}+\cdots+t_{k,0}=b_0 \\ t_{1,1}+\cdots+t_{k,1}=b_1 \\ \cdots \\ t_{1,s}+\cdots+t_{k,s}=b_s}} \alpha_1^{t_1}\alpha_2^{t_2}\cdots\alpha_k^{t_k}(x_1)_{t_1}(x_2)_{t_2}\cdots(x_k)_{t_k} \end{aligned}$$

and the right summation can be factorized as

$$\begin{aligned} u_{p^s} = &\sum_{t_{1,0}+\cdots+t_{k,0}=b_0} \alpha_1^{t_{1,0}}\cdots\alpha_k^{t_{k,0}}(x_1)_{t_{1,0}}\cdots(x_k)_{t_{k,0}} \sum_{t_{1,1}+\cdots+t_{k,1}=b_1} \alpha_1^{t_{1,1}}\cdots\alpha_k^{t_{k,1}}(x_1)_{t_{1,1}p}\cdots(x_k)_{t_{k,1}p} \\ &\cdots \sum_{t_{1,s}+\cdots+t_{k,s}=b_s} \alpha_1^{t_{1,s}}\cdots\alpha_k^{t_{k,s}}(x_1)_{t_{1,s}p^s}\cdots(x_k)_{t_{k,s}p^s}, \end{aligned}$$

$$\begin{aligned} = &\sum_{t_{1.0}+\cdots+t_{k.0}=b_0} \alpha_1^{t_{1.0}}\cdots\alpha_k^{t_{k,0}}(x_1)_{t_{1.0}}\cdots(x_k)_{t_{k,0}} e\left(\sum_{t_{1,1}+\cdots+t_{k,1}=b_1} \alpha_1^{t_{1.1}}\cdots\alpha_k^{t_{k,1}}(x_1)_{t_{1,1}}\cdots(x_k)_{t_{k,1}}\right) \\ &\cdots e^s\left(\sum_{t_{1,s}+\cdots+t_{k,s}=b_s} \alpha_1^{t_{1,s}}\cdots\alpha_k^{t_{k,s}}(x_1)_{t_{1,s}}\cdots(x_k)_{t_{k,s}}\right), \\ = &\prod_{n=0}^{s} e^n \left(\sum_{\sum_{j=1}^k t_{j,n}=b_n} \alpha_1^{t_{j,n}}\cdots\alpha_k^{t_{j,n}}(x_1)_{t_{j,n}}\cdots(x_k)_{t_{j,n}}\right). \end{aligned}$$

For all types of p^s we get

$$u_{p^s} = \sum_{b_0,b_1,\cdots,b_s} \prod_{n=0}^{s} e^n \left(\sum_{\sum_{j=1}^k t_{j,n}=b_n} \alpha_1^{t_{j,n}}\cdots\alpha_k^{t_{j,n}}(x_1)_{t_{j,n}}\cdots(x_k)_{t_{j,n}}\right).$$

So, we just need to show that for a fixed n, let $n = m$ the following holds:

$$\frac{(-1)^{c_m}u_1^{d_m}w_1^{c_m}}{c_m!d_m!} = \sum_{\sum_{j=1}^k t_{j,m}=b_m} \alpha_1^{t_{j,m}}\cdots\alpha_k^{t_{j,m}}(x_1)_{t_{j,m}}\cdots(x_k)_{t_{j,m}}.$$

Now consider the right hand side of previous relation

$$\sum_{t_{1,m}+\cdots+t_{k,m}=b_m} \alpha_1^{t_{j,m}}\cdots\alpha_k^{t_{j,m}}(x_1)_{t_{j,m}}\cdots(x_k)_{t_{j,m}} = \frac{(\alpha_1(x_1)_1+\alpha_2(x_2)_1+\cdots+\alpha_k(x_k)_1)^{b_m}}{b_m!}.$$

We need to work in $\mathbb{Z}[(x_1)_1, \cdots, (x_k)_1]/[(x_1)_1^p, \cdots, (x_k)_1^p]$, and since $0 \leq b_m \leq k(p-1)$ for $0 \leq m \leq s$, recall that $k \leq p$, so $b_m = c_m p + d_m$ this implies

$$\frac{(\alpha_1(x_1)_1 + \alpha_2(x_2)_1 + \cdots + \alpha_k(x_k)_1)^{b_m}}{b_m!} = \frac{u_1^{c_m p + d_m}}{(c_m p + d_m)!} = \frac{p^{c_m} w_1^{c_m} u_1^{d_m}}{(c_m p + d_m)!}.$$

Finally, we have to show that $(c_m p + d_m)!$ is divisible by p^{c_m} and $\frac{(c_m p + d_m)!}{p^{c_m}} \bmod p = (-1)^{c_m} c_m! d_m!$

$$\begin{aligned}(c_m p + d_m)! =& 1 \cdot 2 \cdots (p-1) \cdot p(p+1) \cdots (p + (p-1)) \cdot 2p \cdot (2p+1) \cdots (2p + (p-1)) \\ & ((c_m - 1)p + 1) \cdots ((c_m - 1)p + (p-1)) \cdot c_m p \cdot (c_m p + 1) \cdots (c_m p + d_m), \\ =& c_m! p^{c_m} (p-1)! \cdot \{(p+1)(p+2) \cdots (p + (p-1))\} \cdots \{((c_m - 1)p + 1) \cdots \\ & ((c_m - 1)p + (p-1))\} \cdot (c_m p + 1) \cdots (c_m p + d_m),\end{aligned}$$

and so

$$\left[\frac{(c_m p + d_m)!}{p^{c_m}}\right]_p = c_m!((p-1)!)^{c_m} d_m! = (-1)^{c_m} c_m! d_m!$$

as required. □

Theorem 6.1.7. *For some integer $2 \leq k \leq p$ If $r \geq 0$ and $1 \leq i \leq p-1$,*

$$\begin{aligned}u_1^{p-1} u_p^{p-1} \cdots u_{p^r}^i =& u_1^{p-1} (eu_1 - w_1)^{p-1} \cdots e^{r-1} (eu_1 - w_1)^i, \\ =& u_1^{p-1} (eu_1^{p-1} + u_1^{p-2} w_1 + \cdots + eu_1^{p-(k-1)} w_1^{k-2}) \cdots e^{r-1} (eu_1 - w_1)^i\end{aligned}$$

We will argue by induction to prove this theorem, and the induction begins when $r = 1$, because the case $r = 0$ is an trivial case as we have already seen.

Proof. If $r = 1$, then $p = b_0 + b_1 p$ so we have two types. The first one $b_0 = 0$ and $b_1 = 1$, that is; $c_0 = 0, d_0 = 0, c_1 = 0, d_1 = 1$, where $b_0 = c_0 p + d_0$ and $b_1 = c_1 p + d_1$. The second one is $b_0 = p$, while $b_1 = 0$, so $c_0 = 1, d_0 = 0, c_1 = 0, d_1 = 0$, applying theorem 6.1.6 gives

$$u_p = eu_1 - w_1,$$

so

$$u_1^{p-1} u_p^i = u_1^{p-1} (eu_1 - w_1)^i,$$

when $i = p-1$, so $u_p^{p-1} = \sum_{j=0}^{p-1} (-1)^{p-1-j} (-1)^j e u_1^{p-1-j} w_1^j$, but lemma 6.1.5 shows $w_1^j = 0$, for $k \leq j \leq p-1$, thus $u_p^{p-1} = \sum_{j=0}^{k-1} (-1)^{p-1} e u_1^{p-1-j} w_1^j$, and because $u_1^{p-1} w_1^{k-1} = 0$ (the second part of the same lemma substitute $n = 2$), we conclude

$$u_1^{p-1} u_p^{p-1} = u_1^{p-1} (eu_1^{p-1} + eu_1^{p-2} w_1 + \cdots + eu_1^{p-(k-1)} w_1^{k-2})$$

Now, assume that the statement is true when $r = t-1$ for $1 \leq i \leq p-1$, that is to say;

$$\begin{aligned}u_1^{p-1} u_p^{p-1} \cdots u_{p^{t-1}}^i =& u_1^{p-1} (eu_1 - w_1)^{p-1} \cdots e^{t-2} (eu_1 - w_1)^i, \\ =& u_1^{p-1} (eu_1^{p-1} + u_1^{p-2} w_1 + \cdots + eu_1^{p-(k-1)} w_1^{k-2}) \cdots e^{t-2} (eu_1 - w_1)^i.\end{aligned}$$

If $r = t$ we need to show for $1 \leq i \leq p-1$

$$\begin{aligned} u_1^{p-1}u_p^{p-1}\cdots u_{p^t}^i =& u_1^{p-1}(eu_1 - w_1)^{p-1}\cdots e^{t-2}(eu_1-w_1)^i, \\ =& u_1^{p-1}(eu_1^{p-1} + u_1^{p-2}w_1 + \cdots + eu_1^{p-(k-1)}w_1^{k-2})\cdots e^{t-1}(eu_1-w_1)^i. \end{aligned}$$

Firstly, from the induction assumption we have

$$\begin{aligned} u_1^{p-1}u_p^{p-1}\cdots u_{p^{t-1}}^{p-1} =& u_1^{p-1}(eu_1 - w_1)^{p-1}\cdots e^{t-2}(eu_1-w_1)^{p-1}, \\ =& u_1^{p-1}(eu_1^{p-1} + u_1^{p-2}w_1 + \cdots + eu_1^{p-(k-1)}w_1^{k-2})\cdots e^{t-3}(eu_1^{p-1} + u_1^{p-2}w_1 + \\ & \cdots + eu_1^{p-(k-1)}w_1^{k-2}).e^{t-2}\sum_{j=0}^{p-1}(-1)^{p-1-j}(-1)^j eu_1^{p-1-j}w_1^j \end{aligned}$$

the same reason in the first induction step implies that the last summation is cut up to $k-1$. whilst, $e^{t-3}(eu_1^{p-1} + u_1^{p-2}w_1 + \cdots + eu_1^{p-(k-1)}w_1^{k-2})e^{t-2}(eu_1^{pk}w_1^{k-1}) = 0$ since

$$\begin{aligned} & e^{t-3}(eu_1^{p-1} + u_1^{p-2}w_1 + \cdots + eu_1^{p-(k-1)}w_1^{k-2})e^{t-2}(eu_1^{p-k}w_1^{k-1}) \\ =& e^{t-1}(u_1^{p-k})e^{t-3}\left(e(u_1^{p-1}w_1^{k-1}) + e(u_1^{p-2}w_1^{k-1})w_1 + \cdots + e(u_1^{p-(k-1)}w_1^{k-1})w_1^{k-1}\right) \end{aligned}$$

and from 6.1.5.b and e is an ring homomorphism so the last expression will be finished. Hence,

$$\begin{aligned} u_1^{p-1}u_p^{p-1}\cdots u_{p^{t-1}}^{p-1} =& u_1^{p-1}(eu_1^{p-1} + u_1^{p-2}w_1 + \cdots + eu_1^{p-(k-1)}w_1^{k-2})\cdots e^{t-3}(eu_1^{p-1} + u_1^{p-2}w_1 + \\ & \cdots + eu_1^{p-(k-1)}w_1^{k-2}).e^{t-2}(eu_1^{p-1} + u_1^{p-2}w_1 + \cdots + eu_1^{p-(k-1)}w_1^{k-2}) \end{aligned}$$

Secondly, to complete this proof is enough to show

$$u_1^{p-1}u_p^{p-1}\cdots u_{p^{t-1}}^{p-1}u_{p^t} = u_1^{p-1}u_p^{p-1}\cdots u_{p^{t-1}}^{p-1}e^{t-1}(eu_1 - w_1),$$

that means the only surviving terms from expression $u_{p^t} = \sum_{b_0,b_1,\cdots,b_t}\prod_{n=0}^t e^n\left(\frac{(-1)^{c_n}u_1^{d_n}w_1^{c_n}}{c_n!d_n!}\right)$ after multiplying it by $u_1^{p-1}u_p^{p-1}\cdots u_{p^{t-1}}^{p-1}$ are just the cases when we substitute $b_t = 1, b_{t-1} = \cdots = b_0 = 0$ and $b_t = 0, b_{t-1} = p, b_{t-2} = \cdots = b_0 = 0$ as will be shown.

Starting with the types such that $b_0 \neq 0$, then $b_0 = n_0 p$ where $n_0 = 1, \cdots, k-1$, while $b_0 = c_0 p + d_0$ (theorem 6.1.6), so $c_0 = n_0$ and $d_0 = 0$ for each c_0. But, $b_1 = c_1 p + d_1 = n_1 p - c_0 = (n_1 - 1)p + p - c_0$, this gives that $c_1 = n_1 - 1$ where $c_1 = 0, 1, \cdots, k-2$ and that $d_1 = p - c_0$. Applying theorem 6.1.6 we get

$$P_0 u_{p^t} = \sum_{c_0=1}^{k-1}\sum_{c_1=0}^{k-2} N(u_1, w_1, e)\cdot e(u_1^{p-c_0}w_1^{c_1})\cdot w_1^{c_0}$$

We mean by $P_0 u_{p^t}$ the parts of u_{p^t} such that $b_0 \neq 0$, and $N(u_1, w_1, e) = \prod_{n=2}^t e^n\left(\frac{(-1)^{c_n}u_1^{d_n}w_1^{c_n}}{c_n!d_n!}\right)$. Hence,

$$P_0 u_{p^t} = \sum_{c_0=1}^{k-1} M(u_1, w_1, e)\cdot eu_1^{p-c_0}w_1^{c_0},$$

where $M(u_1, w_1, e) = \sum_{c_1=0}^{k-2} N(u_1, w_1, e)ew_1^{c_1}$.

On the other hand,

$$\begin{aligned} u_p^{p-1} P_0 u_{p^t} &= \sum_{j=1}^{k-1} eu_1^{p-j} w_1^j \sum_{c_0=1}^{k-1} M(u_1, w_1, e) eu_1^{p-c_0} w_1^{c_0} \\ &= \sum_{j=1}^{k-1} \sum_{c_0=1}^{k-1} M(u_1, w_1, e) eu_1^{2p-(j+c_0)} w_1^{j+c_0} \\ &= \sum_{t=2}^{2k-2} M(u_1, w_1, e) eu_1^{2p-t} w_1^t \end{aligned}$$

according to lemma 6.1.5 the last expression equal to zero. Thus, $u_p^{p-1} P_0 u_{p^t} = 0$.

Hence, for the set of all types such that $b_0 \neq 0$ we get the corresponding part of u_{p^t}, when multiplied by $u_1^{p-1} u_p^{p-1} \cdots u_{p^{t-1}}^{p-1}$ the result will be zero. By the same way we can prove there is no remaining if $b_0 = 0$ and $b_1 \neq 0$, similarly; for the other types until $b_0 = b_1 = \cdots b_{t-2} \neq 0$. Consequently, we remaining with the only two types which are $b_t = 1, b_{t-1} = \cdots = b_0 = 0$ and $b_t = 0, b_{t-1} = p, b_{t-2} = \cdots = b_0 = 0$.

Hence, from theorem 6.1.6 we get

$$u_1^{p-1} u_p^{p-1} \cdots u_{p^{t-1}}^{p-1} u_{p^t} = u_1^{p-1} u_p^{p-1} \cdots u_{p^{t-1}}^{p-1} e^{t-1}(eu_1 - w_1),$$

and

$$u_1^{p-1} u_p^{p-1} \cdots u_{p^{t-1}}^{p-1} u_{p^t}^i = u_1^{p-1} u_p^{p-1} \cdots u_{p^{t-1}}^{p-1} e^{t-1}(eu_1 - w_1)^i$$

□

Now, if we consider $k = 3$, then k satisfies $k \leq p$ for any odd prime number p, and this implies the following

Corollary 6.1.8. *If $k = 3$ and p any odd prime number, then*

$$\begin{aligned} u_1^{p-1} u_p^{p-1} \cdots u_{p^r}^i &= u_1^{p-1}(eu_1 - w_1)^{p-1} \cdots e^{r-1}(eu_1 - w_1)^i, \\ &= u_1^{p-1}(eu_1^{p-1} + eu_1^{p-2} w_1) \cdots e^{r-1}(eu_1^i - ieu_1^{i-1} w_1) \end{aligned}$$

Proof. From theorem 6.1.7 substitute $k = 3$. □

6.2 Calculation of $L_*(3)$.

Now we restrict our attention on the case of three variables where corollary 6.1.8 works perfectly. The motivation behind finding $L_*(3)$ is to determined a large part of $M_*(3)$ since $L_*(k) \subseteq M_*(k)$ for $k \geq 1$, this can easily be deduced from the construction of the generators of $L_*(k)$ and *Cartan* formula.

We define the spaces $\mathcal{W}_n^1(3)$, $\mathcal{W}_n^2(3)$ and $\mathcal{W}_n^3(3)$ to be the subspaces from the space $L_n(3)$ which are spanned by $g_{r,i}^{tr}(v_1)$, $g_{r,i}^{tr}(v_1)\cdot g_{s,j}^{tr}(v_2)$ and $g_{r,i}^{tr}(v_1)\cdot g_{s,j}^{tr}(v_2)\cdot g_{t,k}^{tr}(v_3)$ respectively, where $v_1, v_2, v_3 \in \mathbb{F}_p^3$. It turns out we use the $x_{p^i}, y_{p^i}, z_{p^i}$ instead of $(x_1)_{p^i}$, $(x_2)_{p^i}$ and $(x_3)_{p^i}$ for $i \geq 0$ as a generators, and we denote by $\mathbb{F}_p^3$ for the $\mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p$. Before starting our calculation, we need to show the following fact about the generators of $L_*(3)$.

Lemma 6.2.1. *For $v \in \mathbb{F}_p^3$, $\xi \in \mathbb{F}_p$ and $1 \leq i \leq p-1$, $r \geq 0$,*

$$g_{r,i}^{tr}(\xi v) = \xi^i g_{r,i}^{tr}(v).$$

Proof. Let $v = (q_1, q_2, q_3)$, so

$$\begin{aligned} g_{r,i}^{tr}(\xi v) =& (\xi q_1 x_1 + \xi q_2 y_1 + \xi q_3 z_1)^{p-1}\{(\xi q_1 x_p + \xi q_2 y_p + \xi q_3 z_p) + \\ & \sum_{\substack{i_0+j_0+k_0=p \\ i_0,j_0,k_0<p}} \frac{(\xi q_1)^{i_0}(\xi q_2)^{j_0}(\xi q_3)^{k_0}}{i_0!j_0!k_0!} x_1^{i_0} y_1^{j_0} z_1^{k_0}\}^{p-1} \cdots \{(\xi q_1 x_{p^r} + \xi q_2 y_{p^r} + \xi q_3 z_{p^r}) + \\ & \sum_{\substack{i_{r-1}+j_{r-1}+k_{r-1}=p \\ i_{r-1},j_{r-1},k_{r-1}<p}} \frac{(\xi q_1)^{i_{r-1}}(\xi q_2)^{j_{r-1}}(\xi q_3)^{k_{r-1}}}{i_{r-1}!j_{r-1}!k_{r-1}!} x_{p^{r-1}}^{i_r} y_{p^{r-1}}^{j_r} z_{p^{r-1}}^{k_r}\}^i \end{aligned}$$

since, $\xi^{p-1} = 1$, we have $\xi^p = \xi$ and this implies $(\xi q_1)^{i_s}(\xi q_2)^{j_s}(\xi q_3)^{k_s} = \xi q_1^{i_s} q_2^{j_s} q_3^{k_s}$ where $i_s + j_s + k_s = p$, and $0 \leq s \leq r$. Thus,

$$g_{r,i}^{tr}(\xi u) = (\xi^{p-1})^r \xi^i g_{r,i}^{tr}(v) = \xi^i g_{r,i}^{tr}(v),$$

as required. □

Lemma 6.2.2. *If $v_1, v_2, v_3 \in \mathbb{F}_p^3$, then*

$$g_{0,p-1}^{tr}(v_1) g_{0,p-1}^{tr}(v_2) g_{0,p-1}^{tr}(v_3) = \begin{cases} \xi x_1^{p-1} y_1^{p-1} z_1^{p-1}, & \text{if } v_1, v_2, \text{ and } v_3 \text{ are linearly independent;} \\ 0, & \text{otherwise.} \end{cases}$$

where $\xi \in \mathbb{F}_p$.

Proof. Assume that $v_1 = (q_1, q_2, q_3)$, $v_2 = (t_1, t_2, t_3)$ and $v_3 = (l_1, l_2, l_3)$, then

$$\begin{aligned} g_{0,p-1}^{tr}(v_1) g_{0,p-1}^{tr}(v_2) g_{0,p-1}^{tr}(v_3) =& (q_1 x_1 + q_2 y_1 + q_3 z_1)^{p-1}(t_1 x_1 + t_2 y_1 + t_3 z_1)^{p-1} \cdot \\ & (l_1 x_1 + l_2 y_1 + l_3 z_1)^{p-1}. \end{aligned}$$

In fact, each monomial in each bracket has degree $p-1$, so that such multiplication produces a polynomial of degree $3p-3$ which consists only of the factors x_1, y_1 and z_1. However, this is impossible, unless it is a monomial that is given by $\xi x_1^{p-1} y_1^{p-1} z_1^{p-1}$.

Now if v_1 and v_2 are linearly dependent, then there is $c \in \mathbb{F}_p$ such that $v_2 = cv_1$ (or $v_1 = \hat{c}v_2$ where $\hat{c} \in \mathbb{F}_p$) so,

$$\begin{aligned} g^{tr}_{0,p-1}(v_1)g^{tr}_{0,p-1}(v_2) =&(q_1x_1+q_2y_1+q_3z_1)^{p-1}(t_1x_1+t_2y_1+t_3z_1)^{p-1} \\ =&(q_1x_1+q_2y_1+q_3z_1)^{p-1}(cq_1x_1+cq_2y_1+cq_3z_1)^{p-1} \\ =&c^{p-1}(q_1x_1+q_2y_1+q_3z_1)^{p-1}(q_1x_1+q_2y_1+q_3z_1)^{p-1} \\ =&c^{p-1}(q_1x_1+q_2y_1+q_3z_1)^{2p-2}, \end{aligned}$$

but $(q_1x_1+q_2y_1+q_3z_1)^n = 0$ if $n \geq p$. Hence,

$$g^{tr}_{0,p-1}(v_1)g^{tr}_{0,p-1}(v_2) = 0$$

Likewise, when v_1 and v_3 or if v_2 and v_3 are linearly dependent.

If $v_3 = c_1v_1 + c_2v_2$ for $c_1, c_2 \in \mathbb{F}_p$, then

$$\begin{aligned} g^{tr}_{0,p-1}(v_1)g^{tr}_{0,p-1}(v_2)g^{tr}_{0,p-1}(v_3) =&(q_1x_1+q_2y_1+q_3z_1)^{p-1}(t_1x_1+t_2y_1+t_3z_1)^{p-1}\cdot \\ &(l_1x_1+l_2y_1+l_3z_1)^{p-1} \\ =&(q_1x_1+q_2y_1+q_3z_1)^{p-1}(t_1x_1+t_2y_1+t_3z_1)^{p-1} \\ &\{(c_1q_1+c_2t_1)x_1+(c_1q_2+c_2t_2)y_1+(c_1q_3+c_2t_3)z_1\}^{p-1} \\ =&(q_1x_1+q_2y_1+q_3z_1)^{p-1}(t_1x_1+t_2y_1+t_3z_1)^{p-1} \\ &\{(c_1q_1x_1+c_1q_2y_1+c_1q_3z_1)+(c_2t_1x_1+c_2t_2y_1+c_2t_3z_1)\}^{p-1} \\ =&\sum_{i=0}^{p-1}(-1)^i c_1^i c_2^{p-1-i}(q_1x_1+q_2y_1+q_3z_1)^{p+i-1}(t_1x_1+t_2y_1+t_3z_1)^{2p-2-i} \\ =&0 \end{aligned}$$

Similarly, if v_1 or v_2 are written as a linear combinations of v_2 and v_3, or v_1 and v_3 respectively. Consequently, if v_1, v_2 and v_3 are linearly dependent vectors in $\mathbb{F}_p^3$, then $g^{tr}_{0,p-1}(v_1)g^{tr}_{0,p-1}(v_2)g^{tr}_{0,p-1}(v_3) = 0$, otherwise we get $\xi x_1^{p-1}y_1^{p-1}z_1^{p-1}$ such that $\xi \in \mathbb{F}_p$. □

Thus the last lemma illustrates that the product of more than three generators will be zero because the dimension of $\mathbb{F}_p^3$ is 3. Hence, for any four vectors $v_1, v_2, v_3, v_4 \in \mathbb{F}_p^3$ at least one of them have to be written as a linear combination from the others.

Therefore, we need to consider only the case of single generator, the product of two generators and the product of three generators to find $L_*(3)$. In other words, our calculations of $L_n(3)$ will be based on the degree's form n, recall $g^{tr}_{r,i}(v)$ has degree $n = (i+1)p^r - 1$ where $v \in \mathbb{F}_p^3$ where i, r are integers such that $0 \leq i \leq p-1$ and $r \geq 0$.

Proposition 6.2.3. *If $n = (i+1)p^r - 1$, where $1 \leq i \leq p-1$ and $r \geq 1$, then*

$$Dim\ \mathcal{W}^1_n(3) = p^2 + p + 1.$$

and the basis is given by

$$\{g^{tr}_{r,i}(0,0,1) \cup g^{tr}_{r,i}(0,1,q_1) \cup g^{tr}_{r,i}(1,q_2,q_3)\}$$

such that $q_1, q_2, q_3 \in \mathbb{F}_p$.

Proof. From the definition of $\mathcal{W}^1_n(3)$ we have to deal with a single generator, that is; we need to show that in $g^{tr}_{r,i}(\alpha,\beta,\gamma)$ there are only p^2+p+1 linearly independent elements for $\alpha,\beta,\gamma \in \mathbb{F}_p$. In fact, lemma 6.2.1 will reduce the choices of the representative lines (α,β,γ) to the following cases $(0,0,1),(0,1,q_1)$ and $(1,q_2,q_3)$, since any line (α,β,γ) can be written in the form $(1,q_2,q_3)$ such that $q_2 = \beta/\alpha$ and $q_3 = \gamma/\alpha$. Likewise, in the case $(0,\beta,\gamma) = \beta(0,1,q_1)$ where $q_1 = \beta/\gamma$ for $q_1,q_2,q_3 \in \mathbb{F}_p$.

According to this discussion, we infer that $\mathcal{W}^1_n(3)$ is spanned by elements

$$\{g^{tr}_{r,i}(0,0,1) \cup g^{tr}_{r,i}(0,1,q) \cup g^{tr}_{r,i}(1,q_1,q_2)\}$$

and we need just to check the independency of these elements.

Case 1: $g^{tr}_{r,i}(1,q_2,q_3)$ Consider

$$\begin{aligned} g^{tr}_{r,i}(1,q_2,q_3) =&(x_1+q_2y_1+q_3z_1)^{p-1}\{(x_p+q_2y_p+q_3z_p)+\sum_{\substack{i_0+j_0+k_0=p\\ i_0,j_0,k_0<p}}\frac{q_2^{j_0}q_3^{k_0}}{i_0!j_0!k_0!}x_1^{i_0}y_1^{j_0}z_1^{k_0}\}^{p-1}\\ &\cdots\{(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})+\sum_{\substack{i_{r-1}+j_{r-1}+k_{r-1}=p\\ i_{r-1},j_{r-1},k_{r-1}<p}}\frac{q_2^{j_{r-1}}q_3^{k_{r-1}}}{i_{r-1}!j_{r-1}!k_{r-1}!}x_{p^{r-1}}^{i_{r-1}}y_{p^{r-1}}^{j_{r-1}}z_{p^{r-1}}^{k_{r-1}}\}^i\\ =&(x_1+q_2y_1+q_3z_1)^{p-1}x_p^{p-1}\cdots x_{p^r}^i\\ &+(x_1+q_2y_1+q_3z_1)^{p-1}\sum_{\substack{i_0+j_0+k_0=p\\ i_0,j_0,k_0<p}}\frac{q_2^{j_0}q_3^{k_0}}{i_0!j_0!k_0!}x_1^{i_0}y_1^{j_0}z_1^{k_0}x_p^{p-2}\cdots x_{p^r}^i\\ &+R(x,y,z), \end{aligned}$$

such that $R(x,y,z)$ is sum of terms which are not divisible by neither $x_p^{p-1}\cdots x_{p^r}^i$ nor $x_p^{p-2}\cdots x_{p^r}^i$.

Firstly, let

$$R_1 = (x_1+q_2y_1+q_3z_1)^{p-1}x_p^{p-1}\cdots x_{p^r}^i = \sum_{j=0}^{p-1}(-1)^j q_2^j y^j (x_1+q_3z_1)^{p-1-j}x_p^{p-1}\cdots x_{p^r}^i.$$

There are $\frac{p(p+1)}{2}$ linearly independent elements in R_1, to show that it is enough to show for each j such that $0 \le j \le p-1$ there are $p-j$ linearly independent elements, and those linearly independent sets are disjoint, because each of them involves the factor y_1^j.

Let $j = k$ and $R_k(q_2, q_3) = q_2^k y^k (x_1 + q_3 z_1)^{p-1-k} x_p^{p-1} \cdots x_{p^r}^i$ for $0 \leq q_2, q_3 \leq p-1$. Then

$$R_k(q_2, q_3) = (-1)^k q_2^k y_1^k \sum_{n=0}^{p-1-k} \binom{p-1-k}{n} q_3^n x_1^{p-1-k-n} z_1^n x_p^{p-1} \cdots x_{p^r}^i$$

Now, put $\phi_n = (-1)^k \binom{p-1-k}{n} x_1^{p-1-k-n} y_1^k z_1^n x_p^{p-1} \cdots x_{p^r}^i$, so $R_k(q_1, q_2) = \sum_{n=0}^{p-1-k} q_1^k q_2^n \phi_n$. It is clear that the $R_k(q_1, q_2)$ is spanned by ϕ_n to find the dimension, let

$$\sum_{q_1=0}^{p-1} \sum_{q_2=0}^{p-1} \xi_{q_1,q_2} \sum_{n=0}^{p-1-k} q_1^k q_2^n \phi_n = \sum_{n=0}^{p-1-k} \phi_n \sum_{q_1=0}^{p-1} \sum_{q_2=0}^{p-1} \xi_{q_1,q_2} q_1^k q_2^n = \sum_{n=0}^{p-1-k} \sum_{q_1=0}^{p-1} \sum_{q_2=0}^{p-1} \xi_{q_1,q_2} q_1^k q_2^n = 0$$

the last relation is exposed a homogeneous system of equations multiply by q_1^k, so it can be reduced to the following system $\sum_{q_2=0}^{p-1} \sum_{n=0}^{p-1-k} q_2^n \xi_{q_1,q_2} = 0$.

Therefore,

$$\begin{pmatrix} 1 & 1 & 1 & \cdot & \cdot & \cdot & (p-1)^0 \\ 0 & 1 & 2 & \cdot & \cdot & \cdot & (p-1)^1 \\ 0 & 1^2 & 2^2 & \cdot & \cdot & \cdot & (p-1)^2 \\ \cdot & \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & \cdot & & & & \cdot \\ 0 & 1^m & 2^m & \cdot & \cdot & \cdot & (p-1)^m \end{pmatrix} \begin{pmatrix} \xi_{q_1,0} \\ \xi_{q_1,1} \\ \xi_{q_1,2} \\ \cdot \\ \cdot \\ \cdot \\ \xi_{q_1,p-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}$$

such that $m = p-1-k$. The largest $(m+1, m+1)$ submatrix contains the top left entry of the coefficient matrix is a *Vandermonde* matrix which reveals it is an invertible matrix, so the only solution of that system is the zero solution, and this implies that there are $m+1 = p-k$ linearly independent elements.

We conclude that, for each j such that $0 \leq j \leq p-1$ there are $p-j$ linearly independent elements and for any two different values of j, they give distinct sets of linearly independent elements, thus we have

$$Dim\ R_1 = \sum_{s=1}^{p} s = \frac{p(p+1)}{2}.$$

Secondly, we consider

$$R_2 = (x_1 + q_1 y_1 + q_2 z_1)^{p-1} \sum_{\substack{i+j+k=p \\ i,j,k<p}} \frac{q_1^j q_2^k}{i!j!k!} x_1^i y_1^j z_1^k x_p^{p-2} \cdots x_{p^r}^i$$

that will show, It is a subspace of dimension $p(p-1)/2$. Simplify of R_2 yields

$$R_2 = (x_1 + q_1 y_1 + q_2 z_1)^{p-1} \sum_{\substack{j+k=p \\ j,k<p}} \frac{q_1^j q_2^k}{j!k!} y_1^j z_1^k x_p^{p-2} \cdots x_{p^r}^i \qquad (*)$$

relation (*) exposes if either $q_1 = 0$ or $q_2 = 0$, then $R_2 = 0$; so in this case $1 \leq q_1, q_2 \leq p-1$, and such multiplication produces monomials each of them of degree $(2p-1)$.

That means we can rewrite R_2 by the following form

$$R_2 = \sum_{j=1}^{p-1} \sum_{k=p-j}^{p-1} \frac{q_1^j q_2^k}{(2p-j-k-1)!j!k!} x_1^{2p-j-k-1} y_1^j z_1^k x_p^{p-2} \cdots x_{p^r}^i,$$

put $j = n(1 \leq n \leq p-1)$ and

$$\begin{aligned} R_n(q_1,q_2) &= q_1^n \sum_{k=p-n}^{p-1} \frac{q_2^k}{(2p-n-k-1)!n!k!} x_1^{2p-n-k-1} y_1^n z_1^k x_p^{p-2} \cdots x_{p^r}^i \\ &= \sum_{k=1}^{n} \frac{q_1^n q_2^{p+k-n-1}}{(p-k)!n!(p+k-n-1)!} x_1^{p-k} y_1^n z_1^{p+k-n-1} x_p^{p-2} \cdots x_{p^r}^i \end{aligned}$$

Let $\hat{\phi}_k = \frac{1}{(p-k)!n!(p+k-n-1)!} x_1^{p-k} y_1^n z_1^{p+k-n-1} x_p^{p-2} \cdots x_{p^r}^i$, so $R_n(q_1,q_2) = \sum_{k=1}^n q_1^n q_2^{p+k-n-1} \hat{\phi}_k$. Obviously, $\hat{\phi}_k{}'s$ span the subspace $R_n(q_1,q_2)$ of the space R_2, to find the dimension of this subspace, let

$$\sum_{q_1=1}^{p-1} \sum_{q_2=1}^{p-1} \sum_{k=1}^{n} \lambda_{q_1,q_2} q_1^n q_2^{p+k-n-1} \hat{\phi}_k = \sum_{q_1=1}^{p-1} \sum_{q_2=1}^{p-1} q_1^n q_2^{p-n} \sum_{k=1}^{n} \lambda_{q_1,q_2} q_2^{k-1} \hat{\phi}_k = \sum_{q_2=1}^{p-1} \sum_{k=1}^{n} \lambda_{q_1,q_2} q_2^{k-1} = 0$$

so we have from the last system the following coefficient matrix

$$\begin{pmatrix} 1 & 2 & . & . & . & (p-1)^1 \\ 1^2 & 2^2 & . & . & . & (p-1)^2 \\ . & . & & & & . \\ . & . & & & & . \\ . & . & & & & . \\ 1^n & 2^n & . & . & . & (p-1)^n \end{pmatrix}$$

The matrix which involves the first n columns admits it is an *Vandermonde* matrix, and its determinant not zero. Hence, there are n linearly independent rows in that matrix. Consequently, we have n linearly independent elements forming a basis for $R_n(q_1,q_2)$. So that, for a fixed $j = n$ is gotten a subspace of dimension n and these subspaces are disjoint, and since $1 \leq j \leq p-1$, implies

$$Dim\ R_2 = \sum_{s=1}^{p-1} s = \frac{p(p-1)}{2}$$

On examining the elements of R_1 we see that they are divisible by $x_p^{p-1} \cdots x_{p^r}^i$. By contrast , an element in R_2 is multiplied by $x_p^{p-2} \cdots x_{p^r}^i$. Thus, these subspaces from the space $g_{r,i}^{tr}(1,q_2,q_3)$ are disjoint, and hence $g_{r,i}^{tr}(1,q_2,q_3)$ involves p^2 linearly independent elements where $q_2, q_3 \in \mathbb{F}_p$.

Case 2: $g^{tr}_{r,i}(0,0,1) \cup g^{tr}_{r,i}(0,1,q_1)$
We have from [6] that the dimension of $v_{r,i}(0,1) \cup v_{r,i}(1,q)$ is $p+1$ if the degree is given by $n = (i+1)p^r - 1$ such that $1 \leq i \leq p-1$ and $r \geq 1$, where $q \in \mathbb{F}_p$ which is corresponding to this case, that means;

$$v_{r,i}(0,1) \cup v_{r,i}(1,q) \simeq g^{tr}_{r,i}(0,0,1) \cup g^{tr}_{r,i}(0,1,q_1),$$

where $q_1 \in \mathbb{F}_p$. Moreover, there is no x factor in this case because $\alpha = 0$ in $g^{tr}_{r,i}(\alpha,\beta,\gamma)$. Therefore, the basis elements of **Case 1** and **Case 2** are distinct, so we get

$$Dim\{g^{tr}_{r,i}(0,0,1) \cup g^{tr}_{r,i}(0,1,q_1) \cup g^{tr}_{r,i}(1,q_2,q_3)\} = p^2+p+1.$$

and the basis is given by

$$g^{tr}_{r,i}(0,0,1) \cup g^{tr}_{r,i}(0,1,q_1) \cup g^{tr}_{r,i}(1,q_2,q_3)$$

□

Proposition 6.2.4. *If $n = (i+1)p^r + (j+1)p^s - 2$, where $1 \leq i,j \leq p-1$, $r \geq 1$, $s \geq 0$ and $r \geq s$, then*

$$Dim\ \mathcal{W}^2_n(3) = \begin{cases} (j+1)(p^2+p+1), & \text{if } s = 0 \text{ and } r \geq 2; \\ (p+1)(p^2+p+1), & \text{if } s \geq 1 \text{ and } r \geq s+2. \end{cases}$$

In the following proof We have eight essential cases. we calculate the dimension of the cases from (1) to (7) for all possibilities of r, s, i and j, but unfortunately we cannot find that for case (8) unless in two cases which are stated in the context of above proposition.

Proof. According to definition of $\mathcal{W}^2_n(3)$ (the space that is spanned by $g^{tr}_{r,i}(v_1) \cdot g^{tr}_{s,j}(v_2)$ where $v_1, v_2 \in \mathbb{F}^3_p$), the degree n of space $\mathcal{W}^2_n(3)$ is given by $n = (i+1)p^r + (j+1)p^s - 2$, where $(a+1)p^\alpha - 1$ for each generator. Avoiding to the repetition and misconception we will take $r \geq s$ and when $r = s$ then $i \geq j$ where $1 \leq i,j \leq p-1$ and $r \geq s \geq 1$.

Assume that $v_1 = (q_1,q_2,q_3)$ and $v_2 = (t_1,t_2,t_3)$ such that $q_i, t_i \in \mathbb{F}_p$ for $i = 1,2,3$, then $\mathcal{W}^2_n(3)$ is spanned by

$$g^{tr}_{r,i}(q_1,q_2,q_3) \cdot g^{tr}_{s,j}(t_1,t_2,t_3),$$

and because of,

$$g^{tr}_{r,i}(q_1,q_2,q_3) = g^{tr}_{r,i}(0,0,\bar{q}_3) \cup g^{tr}_{r,i}(0,\bar{q}_2,q_3) \cup g^{tr}_{r,i}(\bar{q}_1,q_2,q_3),$$

where $1 \leq \bar{q}_1, \bar{q}_1, \bar{q}_3 \leq p-1$ and $0 \leq q_1,q_2,q_3 \leq p-1$. Likewise, when one considers $g^{tr}_{s,j}(t_1,t_2,t_3)$. Therefore, the following sets span the space $\mathcal{W}^2_n(3)$.

1) $g^{tr}_{r,i}(0,0,\bar{q}_3) \cdot g^{tr}_{s,j}(0,0,\bar{t}_3) = g^{tr}_{r,i}(0,0,1) \cdot g^{tr}_{s,j}(0,0,1)$,

2) $g^{tr}_{r,i}(0,0,\bar{q_3}) \cdot g^{tr}_{s,j}(0,\bar{t_2},t_3) = g^{tr}_{r,i}(0,0,1) \cdot g^{tr}_{s,j}(0,1,t_3)$,

3) $g^{tr}_{r,i}(0,0,\bar{q_3}) \cdot g^{tr}_{s,j}(\bar{t_1},t_2,t_3) = g^{tr}_{r,i}(0,0,1) \cdot g^{tr}_{s,j}(1,t_2,t_3)$,

4) $g^{tr}_{r,i}(0,\bar{q_2},q_3) \cdot g^{tr}_{s,j}(0,0,\bar{t_3}) = g^{tr}_{r,i}(0,1,q_3) \cdot g^{tr}_{s,j}(0,0,1)$,

5) $g^{tr}_{r,i}(0,\bar{q_2},q_3) \cdot g^{tr}_{s,j}(0,\bar{t_2},t_3) = g^{tr}_{r,i}(0,1,q_3) \cdot g^{tr}_{s,j}(0,1,t_3)$,

6) $g^{tr}_{r,i}(0,\bar{q_2},q_3) \cdot g^{tr}_{s,j}(\bar{t_1},t_2,t_3) = g^{tr}_{r,i}(0,1,q_3) \cdot g^{tr}_{s,j}(1,t_2,t_3)$,

7) $g^{tr}_{r,i}(\bar{q_1},q_2,q_3) \cdot g^{tr}_{s,j}(0,0,\bar{t_3}) = g^{tr}_{r,i}(1,q_2,q_3) \cdot g^{tr}_{s,j}(0,0,1)$,

8) $g^{tr}_{r,i}(\bar{q_1},q_2,q_3) \cdot g^{tr}_{s,j}(0,\bar{t_2},t_3) = g^{tr}_{r,i}(1,q_2,q_3) \cdot g^{tr}_{s,j}(0,1,t_3)$,

9) $g^{tr}_{r,i}(\bar{q_1},q_2,q_3) \cdot g^{tr}_{s,j}(\bar{t_1},t_2,t_3) = g^{tr}_{r,i}(1,q_2,q_3) \cdot g^{tr}_{s,j}(1,t_2,t_3)$.

The next step will be the investigation of the independency of these sets and consider whether there exists any overlapping among them in order to sum up the dimension of $\mathcal{W}^2_n(3)$.

Case 1: $g^{tr}_{r,i}(0,0,1) \cdot g^{tr}_{s,j}(0,0,1)$.
This is the trivial case, since

$$C_1 = z_1^{p-1} \cdots z_{p^r}^{i} \cdot z_1^{p-1} \cdots z_p^{s^j} = 0.$$

Case 2: $g^{tr}_{r,i}(0,0,1) \cdot g^{tr}_{s,j}(0,1,t_3)$.

$$\begin{aligned}
C_2 =& z_1^{p-1} \cdots z_{p^r}^{i} \cdot (y_1 + t_3 z_1)^{p-1} \cdots (y_{p^s} + t_3 z_{p^s})^j \\
=& \begin{cases} y_1^{p-1} \cdots y_{p^s}^{j} \cdot z_1^{p-1} \cdots z_{p^r}^{i}, & \text{if } r > s; \\ y_1^{p-1} \cdots y_{p^s-1}^{p-1} \cdot z_1^{p-1} \cdots z_{p^s-1}^{p-1} z_{p^s}^{i} (y_{p^s} + t_3 z_{p^s})^j, & \text{if } r = s. \end{cases} \\
=& \begin{cases} f_y^s(y_1^{p-1}) f_z^r(z_1^{p-1}), & \text{if } r > s; \\ f_{yz}^{s-1}(y_1^{p-1} z_1^{p-1}) z_{p^s}^{i} (y_{p^s} + t_3 z_{p^s})^j, & \text{if } r = s. \end{cases}
\end{aligned}$$

From to the above relation if $r > s$, then the dimension will be one. If $r = s$, then we need to look at $z_{p^r}^i (y_{p^r} + t_3 z_{p^r})^j$, where $t_3 \in \mathbb{F}_p$. According to [6], we have two separated cases, the first one if $i + j \le p - 1$, then $z_{p^r}^i (y_{p^r} + t_3 z_{p^r})^j = \sum_{k=0}^{j} \binom{j}{k} t_3^k z_{p^r}^{i+k} y_{p^r}^{j-k}$ and hence each summand in the last expression represents a basis element since they are independent, so in this case there are $j + 1$ linearly independent elements. While, the second case when $i + j > p - 1$, then $z_{p^r}^i (y_{p^r} + t_3 z_{p^r})^j = \sum_{k=0}^{p-i-1} \binom{j}{k} t_3^k z_{p^r}^{i+k} y_{p^r}^{j-k}$ and for the same reason as in the first case, we have $p - i$ independent elements see [6] for more details about the proof. Hence,

$$Dim\ C_2 = \begin{cases} j + 1, & \text{if } i + j \le p - 1, \text{ and } r = s; \\ p - i, & \text{if } i + j \ge p, \text{ and } r = s; \\ 1, & \text{if } r > s. \end{cases}$$

Case 3: $g^{tr}_{r,i}(0,0,1)\cdot g^{tr}_{s,j}(1,t_2,t_3)$. (we have to investigate $s=0$)

$$C_3 = z_1^{p-1}\cdots z_{p^r}^{i}(x_1+t_2y_1+t_3z_1)^{p-1}\{(x_p+t_2y_p+t_3z_p)^{p-1}+(p-1)(x_p+t_2y_p+t_3z_p)^{p-2} \sum_{\substack{i_0+j_0+k_0=p\\ i_0,j_0,k_0<p}} \frac{t_2^{j_0}t_3^{k_0}}{i_0!j_0!k_0!}x_1^{i_0}y_1^{j_0}z_1^{k_0}\}\cdots\{(x_{p^s}+t_2y_{p^s}+t_3z_{p^s})^j+j(x_{p^s}+t_2y_{p^s}+t_3z_{p^s})^{j-1} \cdot \sum_{\substack{i_{s-1}+j_{s-1}+k_{s-1}=p\\ i_{s-1},j_{s-1},k_{s-1}<p}} \frac{t_2^{j_{s-1}}t_3^{k_{s-1}}}{i_{s-1}!j_{s-1}!k_{s-1}!}x_{p^{s-1}}^{i_{s-1}}y_{p^{s-1}}^{j_{s-1}}z_{p^{s-1}}^{k_{s-1}}\}.$$

To simplify C_3 we need to consider the following part and by induction we can deduced the simple form of C_3, so for $0\le n\le s-1$ such that $s\ge 1$ and for $1\le i,j\le p-1$ we have

$$Q = z_{p^n}^{p-1}z_{p^{n+1}}^{i}\{(x_{p^n}+t_2y_{p^n}+t_3z_{p^n})^{p-1}+(p-1)(x_{p^n}+t_2y_{p^n}+t_3z_{p^n})^{p-2} \cdot \sum_{\substack{i_{n-1}+j_{n-1}+k_{n-1}=p\\ i_{n-1},j_{n-1},k_{n-1}<p}} \frac{t_2^{j_{n-1}}t_3^{k_{n-1}}}{i_{n-1}!j_{n-1}!k_{n-1}!}x_{p^{n-1}}^{i_{n-1}}y_{p^{n-1}}^{j_{n-1}}z_{p^{n-1}}^{k_{n-1}}\}\{(x_{p^{n+1}}+t_2y_{p^{n+1}}+t_3z_{p^{n+1}})^j + j(x_{p^{n+1}}+t_2y_{p^{n+1}}+t_3z_{p^{n+1}})^{j-1}\cdot \sum_{\substack{i_n+j_n+k_n=p\\ i_n,j_n,k_n<p}} \frac{t_2^{j_n}t_3^{k_n}}{i_n!j_n!k_n!}x_{p^n}^{i_n}y_{p^n}^{j_n}z_{p^n}^{k_n}\}$$

$$= z_{p^n}^{p-1}z_{p^{n+1}}^{i}(x_{p^n}+t_2y_{p^n})^{p-1}(x_{p^{n+1}}+t_2y_{p^{n+1}}+t_3z_{p^{n+1}})^j + jz_{p^n}^{p-1}z_{p^{n+1}}^{i}(x_{p^n}+t_2y_{p^n})^{p-1}\cdot (x_{p^{n+1}}+t_2y_{p^{n+1}}+t_3z_{p^{n+1}})^{j-1}\cdot \sum_{\substack{i_n+j_n+k_n=p\\ i_n,j_n,k_n<p}} \frac{t_2^{j_n}t_3^{k_n}}{i_n!j_n!k_n!}x_{p^n}^{i_n}y_{p^n}^{j_n}z_{p^n}^{k_n}$$
$$+z_{p^n}^{p-1}z_{p^{n+1}}^{i}(x_{p^n}+t_2y_{p^n}+t_3z_{p^n})^{p-2}\cdot(x_{p^{n+1}}+t_2y_{p^{n+1}}+t_3z_{p^{n+1}})^j\cdot \sum_{\substack{i_{n-1}+j_{n-1}+k_{n-1}=p\\ i_{n-1},j_{n-1},k_{n-1}<p}} \frac{t_2^{j_{n-1}}t_3^{k_{n-1}}}{i_{n-1}!j_{n-1}!k_{n-1}!}x_{p^{n-1}}^{i_{n-1}}y_{p^{n-1}}^{j_{n-1}}z_{p^{n-1}}^{k_{n-1}}$$
$$+jz_{p^n}^{p-1}z_{p^{n+1}}^{i}(x_{p^n}+t_2y_{p^n}+t_3z_{p^n})^{p-2}\cdot(x_{p^{n+1}}+t_2y_{p^{n+1}}+t_3z_{p^{n+1}})^{j-1}\cdot \sum_{\substack{i_{n-1}+j_{n-1}+k_{n-1}=p\\ i_{n-1},j_{n-1},k_{n-1}<p}} \frac{t_2^{j_{n-1}}t_3^{k_{n-1}}}{i_{n-1}!j_{n-1}!k_{n-1}!}x_{p^{n-1}}^{i_{n-1}}y_{p^{n-1}}^{j_{n-1}}z_{p^{n-1}}^{k_{n-1}} \sum_{\substack{i_n+j_n+k_n=p\\ i_n,j_n,k_n<p}} \frac{t_2^{j_n}t_3^{k_n}}{i_n!j_n!k_n!}x_{p^n}^{i_n}y_{p^n}^{j_n}z_{p^n}^{k_n},$$

clearly, $z_{p^n}^{p-1}(\bar{t}_1x_{p^n}+t_2y_{p^n})^{p-1}(x_{p^{n+1}}+t_2y_{p^{n+1}}+t_3z_{p^{n+1}})^j\sum_{\substack{i_n+j_n+k_n=p\\ i_n,j_n,k_n<p}}\frac{t_2^{j_n}t_3^{k_n}}{i_n!j_n!k_n!}x_{p^n}^{i_n}y_{p^n}^{j_n}z_{p^n}^{k_n}=0$.

While, from induction steps we have each term in C_3 involves $z_{p^{n-1}}^{p-1}(x_{p^{n-1}}+t_2y_{p^{n-1}})^{p-1}$, so the third and the fourth terms in the previous expression will be vanished. Consequently, if $r=s$; then

$$C_3 = z_1^{p-1}\cdots z_{p^s}^{i}(x_1+t_2y_1)^{p-1}\cdots(x_{p^{s-1}}+t_2y_{p^{s-1}})^{p-1}(x_{p^s}+t_2y_{p^s}+t_3z_{p^s})^j,$$

and if $r > s$; then

$$C_3 = z_1^{p-1} \cdots z_{p^r}^i \cdot (x_1 + t_2y_1)^{p-1} \cdots (x_{p^{s-1}} + t_2y_{p^{s-1}})^{p-1}(x_{p^s} + t_2y_{p^s})^j.$$

Now, when $r = s$, we get

$$\begin{aligned} C_3 =& z_1^{p-1} \cdots z_{p^s}^i (x_1 + t_2y_1)^{p-1} \cdots (x_{p^{s-1}} + t_2y_{p^{s-1}})^{p-1}(x_{p^s} + t_2y_{p^s} + t_3z_{p^s})^j, \\ =& \sum_{n=0}^{j} t_3^n \binom{j}{n} z_1^{p-1} \cdots z_{p^s}^{i+n}(x_1 + t_2y_1)^{p-1} \cdots (x_{p^{s-1}} + t_2y_{p^{s-1}})^{p-1}(x_{p^s} + t_2y_{p^s})^{j-n}, \end{aligned}$$

but for a fixed $n = c$ the expression $z_1^{p-1} \cdots z_{p^s}^{i+c}(x_1 + t_2y_1)^{p-1} \cdots (x_{p^{s-1}} + t_2y_{p^{s-1}})^{p-1}(x_{p^s} + t_2y_{p^s})^{j-c}$ contains p linearly independent elements since the last part $(x_1+t_2y_1)^{p-1} \cdots (x_{p^{s-1}}+ t_2y_{p^{s-1}})^{p-1}(x_{p^s} + t_2y_{p^s})^{j-c}$ involves these elements by [6]. On the other hand, C_3 consists of $j + 1$ expression like the above one if $i + j \leq p - 1$ and when $i + j \geq p$ there are $p - i$ expressions since

$$C_3 = \sum_{n=0}^{p-i-1} t_3^n \binom{j}{n} z_1^{p-1} \cdots z_{p^s}^{i+n}(x_1 + t_2y_1)^{p-1} \cdots (x_{p^{s-1}} + t_2y_{p^{s-1}})^{p-1}(x_{p^s} + t_2y_{p^s})^{j-n}.$$

Obviously, those expressions in both cases are distinct because each of them involves z_{p^s} of different power. Hence, we get $(j+1)p$ linearly independent elements when $i+j \leq p-1$, and if $i + j \geq p$ then we have $(p - i)p$ elements.

Turning to the case when $r > s$,

$$C_3 = z_1^{p-1} \cdots z_{p^r}^i \cdot (x_1 + t_2y_1)^{p-1} \cdots (x_{p^{s-1}} + t_2y_{p^{s-1}})^{p-1}(x_{p^s} + t_2y_{p^s})^j,$$

similarly the part $(x_1 + t_2y_1)^{p-1} \cdots (x_{p^{s-1}} + t_2y_{p^{s-1}})^{p-1}(x_{p^s} + t_2y_{p^s})^j$ contains p linearly independent elements, so the dimension of this case p. Therefore,

$$Dim\ C_3 = \begin{cases} (j + 1)p, & \text{if } i + j \leq p - 1, \text{ and } r = s; \\ (p - i)p, & \text{if } i + j \geq p, \text{ and } r = s; \\ p, & \text{if } r > s. \end{cases}$$

Case 4: $g_{r,i}^{tr}(0, 1, q_3) \cdot g_{s,j}^{tr}(0, 0, 1)$.(check the overlapping if $s = 0$ with C_2)

$$\begin{aligned} C_4 =&(y_1 + q_3z_1)^{p-1} \cdots (y_{p^s} + q_3z_{p^s})^{p-1} \cdots (y_{p^r} + q_3z_{p^r})^i \cdot z_1^{p-1} \cdots z_{p^s}^j \\ =& f_{yz}^{s-1}(y_1^{p-1}z_1^{p-1}) \cdot z_{p^s}^j (y_{p^s} + qz_{p^s})^{p-1} \cdots (y_{p^r} + qz_{p^r})^i. \end{aligned}$$

Finding the linearly independent elements in C_4 required only examining the part $z_{p^s}^j (y_{p^s} + qz_{p^s})^{p-1} \cdots (y_{p^r} + qz_{p^r})^i$. As we have mentioned in proof of proposition 6.2.3 that $v_{r,i}(0, 1) \cup v_{r,i}(1, q) \simeq g_{r,i}^{tr}(0, 0, 1) \cup g_{r,i}^{tr}(0, 1, q_1)$, where $q, q_1 \in \mathbb{F}_p$, so from [6] we have to deal with the following cases.

The first case, if $r = s$, then we get $z_{p^s}^j(y_{p^s} + q_3 z_{p^s})^i = \sum_{k=0}^{i}\binom{i}{k} q_3^k y_{p^s}^{i-k} z_{p^s}^{k+j}$. In fact, we have dealt with this in **Case 2**, just we need to swap i and j. Thus, there are $i+1$ basis elements when $i+j \leq p-1$ and if $i+j \geq p$, then the number of basis elements is $p-j$ elements.

The second case, if $r = s+1$, so $z_{p^s}^j(y_{p^s} + q_3 z_{p^s})^{p-1}(y_{p^{s+1}} + q_3 z_{p^{s+1}})^i$ by rearranging this expression and using *Vandermonde*'s determinant someone can infer that if $i \leq j$, then there are $p+i-j$ basis elements, while; we get p independent elements when $i > j$.

The final case, when $r \geq s+2$, then $z_{p^s}^j(y_{p^s} + q z_{p^s})^{p-1} \cdots (y_{p^r} + q z_{p^r})^i$ and hence the same technique that used in the previous case can be used for this case to show that the dimension of C_4 is p, see [6] for complete proof of these cases. Therefore,

$$Dim\ C_4 = \begin{cases} i+1, & \text{if } i+j \leq p-1, \text{ and } r = s; \\ p-j, & \text{if } i+j \geq p, \text{ and } r = s; \\ p+i-j, & \text{if } i \leq j, \text{ and } r = s+1; \\ p, & \text{if } i > j, \text{ and } r = s+1; \\ p, & \text{if } r \geq s+2. \end{cases}$$

Case 5: $g_{r,i}^{tr}(0,1,q_3) \cdot g_{s,j}^{tr}(0,1,t_3)$.

$$C_5 = (y_1 + q_3 z_1)^{p-1} \cdots (y_{p^r} + q_3 z_{p^r})^i \cdot (y_1 + t_3 z_1)^{p-1} \cdots (y_{p^s} + t_3 z_{p^s})^j$$

recall that $v_{r,i}(1,q_3) \cdot v_{s,j}(1,t_3) \simeq g_{r,i}^{tr}(0,1,q_3) \cdot g_{s,j}^{tr}(0,1,t_3)$, where $q_3, t_3 \in \mathbb{F}_p$ via the homomorphism $h(x_{p^n}) = y_{p^n}$, and $h(y_{p^n}) = z_{p^n}$ for $n \geq 0$. Hence, from [6] we have

$$C_5 = \begin{cases} f_{yz}^s(y_1^{p-1} z_1^{p-1})(y_{p^s} + t_3 z_{p^s})^j (y_{p^r} + q_3 z_{p^r})^i, & \text{if } r = s; \\ f_{yz}^s(y_1^{p-1} z_1^{p-1})(y_{p^s} + t_3 z_{p^s})^j (y_{p^s} + q_3 z_{p^s})^{p-1} \cdots (y_{p^r} + q_3 z_{p^r})^i, & \text{if } r > s \text{ and } j < p-1; \\ f_{yz}^{s+1}(y_1^{p-1} z_1^{p-1})(y_{p^{s+1}} + q_3 z_{p^{s+1}})^{p-1} \cdots (y_{p^r} + q_3 z_{p^r})^i, & \text{if } r > s \text{ and } j = p-1. \end{cases}$$

so, we need to investigate these three cases establish how many linearly independent elements appear in this case.

Starting with the case when $r = s$, then we need to consider $(y_{p^s} + t_3 z_{p^s})^j (y_{p^r} + q_3 z_{p^r})^i = \sum_{n=0}^{j}\binom{j}{n} t_3^{j-n} y_{p^s}^{j-n} z_{p^s}^n \sum_{m=0}^{i}\binom{i}{m} q_3^{i-m} y_{p^s}^{i-m} z_{p^s}^m$. Set $k = n+m$, so last expression could be written by $(y_{p^s} + t_3 z_{p^s})^j (y_{p^r} + q_3 z_{p^r})^i = \sum_{k=0}^{i+j} \xi_k y_{p^s}^{i+j-k} z_{p^s}^k$. Now, if $i+j \leq p-1$, then clearly each summand in the previous expression represents a basis element, thus there are $i+j+1$ basis elements. In the case when $i+j \geq p$, recall $y_{p^s}^p = z_{p^s}^p = 0$, this implies $i+j-k \leq p-1$ so $k \geq i+j-(p-1)$. On the other hand, $k \leq p-1$, thus $(y_{p^s} + t_3 z_{p^s})^j (y_{p^r} + q_3 z_{p^r})^i = \sum_{k=i+j-(p-1)}^{p-1} \xi_k y_{p^s}^{i+j-k} z_{p^s}^k$. Similarly, as previous case we can obtain the dimension in this case; which is $2p-1-i-j$.

Turning to the case such that $r > s$ and $j < p-1$

$$(y_{p^s}+t_3z_{p^s})^j(y_{p^s}+q_3z_{p^s})^{p-1} = \sum_{n=0}^{j}\binom{j}{n}t_3^{j-n}y_{p^s}^{n}z_{p^s}^{j-n}\sum_{m=0}^{p-1}(-1)^{p-1-m}q_3^{p-1-m}y_{p^s}^{m}z_{p^s}^{p-1-m}$$
$$=\sum_{m=0}^{p-1}\sum_{n=0}^{j}(-1)^{p-1-m}\binom{j}{n}q_3^{p-1-m}t_3^{j-n}y_{p^s}^{n+m}z_{p^s}^{p+j-n-m-1}.$$

Set $k = m+n$, then $0 \le k \le p+j-1$ and $m = k-n$ so

$$(y_{p^s}+t_3z_{p^s})^j(y_{p^s}+q_3z_{p^s})^{p-1} = \sum_{k=0}^{p+j-1}\sum_{n=0}^{j}(-1)^{p-1-k+n}\binom{j}{n}q_3^{p-1-k+n}t_3^{j-n}y_{p^s}^{k}z_{p^s}^{p+j-k-1}$$
$$=z_{p^s}^{j}\sum_{k=0}^{p-1}(-1)^{p-1-k}q_3^{p-1-k}y_{p^s}^{k}z_{p^s}^{p-1-k}\sum_{n=0}^{j}(-1)^n\binom{j}{n}q_3^{n}t_3^{j-n}$$
$$=(t_3-q_3)^j z_{p^s}^{j}(y_{p^s}+q_3z_{p^s})^{p-1}.$$

Hence, dealing with this case means we deal exactly with C_4 second and third cases, therefore; this case will be disregarded.

Similarly, the last case $f_{yz}^{s+1}(y_1^{p-1}z_1^{p-1})(y_{p^{s+1}}+q_3z_{p^{s+1}})^{p-1}\cdots(y_{p^r}+q_3z_{p^r})^i$ can be viewed as a special case from C_4 when someone taken $j = p-1$ in C_4 , consequently; this case also will be disregarded.

Case 6 : $g_{r,i}^{tr}(0,1,q_3)\cdot g_{s,j}^{tr}(1,t_2,t_3)$.

$$C_6 =(y_1+q_3z_1)^{p-1}\cdots(y_{p^r}+q_3z_{p^r})^i(x_1+t_2y_1+t_3z_1)^{p-1}\{(x_p+t_2y_p+t_3z_p)^{p-1}+$$
$$(p-1)(x_p+t_2y_p+t_3z_p)^{p-2}\sum_{\substack{i_0+j_0+k_0=p\\ i_0,j_0,k_0<p}}\frac{t_2^{j_0}t_3^{k_0}}{i_0!j_0!k_0!}x_1^{i_0}y_1^{j_0}z_1^{k_0}\}\cdots\{(x_{p^s}+t_2y_{p^s}+t_3z_{p^s})^j+$$
$$j(x_{p^s}+t_2y_{p^s}+t_3z_{p^s})^{j-1}\cdot\sum_{\substack{i_{s-1}+j_{s-1}+k_{s-1}=p\\ i_{s-1},j_{s-1},k_{s-1}<p}}\frac{t_2^{j_{s-1}}t_3^{k_{s-1}}}{i_{s-1}!j_{s-1}!k_{s-1}!}x_{p^{s-1}}^{i_{s-1}}y_{p^{s-1}}^{j_{s-1}}z_{p^{s-1}}^{k_{s-1}}\}.$$

But $(y_{p^n}+q_3z_{p^n})^{p-1}(x_{p^n}+t_2y_{p^n}+t_3z_{p^n})^{p-1}\sum_{\substack{i_n+j_n+k_n=p\\ i_n,j_n,k_n<p}}\frac{t_2^{j_n}t_3^{k_n}}{i_n!j_n!k_n!}x_{p^n}^{i_n}y_{p^n}^{j_n}z_{p^n}^{k_n}=0$ for all n such that $0\le n\le s-1$ implies

$$C_6 =(y_1+q_3z_1)^{p-1}\cdots(y_{p^r}+q_3z_{p^r})^i(x_1+t_2y_1+t_3z_1)^{p-1}\cdots(x_{p^s}+t_2y_{p^s}+t_3z_{p^s})^j.$$

Now, consider $Q_l = (x_{p^l} + t_2 y_{p^l} + t_3 z_{p^l})^j (y_{p^l} + q_3 z_{p^l})^{p-1}$, where $0 \le l \le s$ we have

$$\begin{aligned}
Q_l =& \sum_{m=0}^{j} \binom{j}{m} x_{p^l}^{j-m} (t_2 y_{p^l} + t_3 z_{p^l})^m \sum_{n=0}^{p-1} \binom{p-1}{n} q_3^{p-1-n} y_{p^l}^n z_{p^l}^{p-1-n} \\
=& \sum_{m=0}^{j} \binom{j}{m} x_{p^l}^{j-m} \sum_{d=0}^{m} \binom{m}{d} t_2^d t_3^{m-d} y_{p^l}^d z_{p^l}^{m-d} \sum_{n=0}^{p-1} \binom{p-1}{n} q_3^{p-1-n} y_{p^l}^n z_{p^l}^{p-1-n} \\
=& \sum_{m=0}^{j} \binom{j}{m} x_{p^l}^{j-m} \sum_{d=0}^{m} \sum_{n=0}^{p-1} (-1)^n \binom{m}{d} q_3^{p-1-n} t_2^d t_3^{m-d} y_{p^l}^{d+n} z_{p^l}^{p-1+m-d-n},
\end{aligned}$$

put $k = d + n$, so $0 \le k \le p - 1 + m$ and $n = k - d$ thus

$$\begin{aligned}
Q_l =& \sum_{m=0}^{j} \binom{j}{m} x_{p^l}^{j-m} \sum_{d=0}^{m} \sum_{k=0}^{p-1+m} (-1)^{k-d} \binom{m}{d} q_3^{p-1-k+d} t_2^d t_3^{m-d} y_{p^l}^k z_{p^l}^{p-1+m-k} \\
=& \sum_{m=0}^{j} \binom{j}{m} x_{p^l}^{j-m} \sum_{d=0}^{m} (-1)^d \binom{m}{d} t_2^d q_3^d t_3^{m-d} z_{p^l}^m \sum_{k=0}^{p-1} (-1)^k q_3^{p-1-k} y_{p^l}^k z_{p^l}^{p-1-k} \\
=& \sum_{m=0}^{j} \binom{j}{m} x_{p^l}^{j-m} (t_3 - t_2 q)^m z_{p^l}^m \cdot (y_{p^l} + q z_{p^l})^{p-1} \\
=& (x_{p^l} + (t_3 - t_2 q_3) z_{p^l})^j (y_{p^l} + q z_{p^l})^{p-1}
\end{aligned}$$

for fixed q_3. We have $0 \le t_3 - q_3 t_2 \le p - 1$, set $t = t_3 - q_3 t_2$, we get

$$Q_l = (x_{p^l} + t z_{p^l})^j (y_{p^l} + q_3 z_{p^l})^{p-1} \quad \text{where} \quad t, \in \mathbb{F}_p$$

Hence,

$$C_6 = \begin{cases} (y_1 + q_3 z_1)^{p-1} \cdots (y_{p^s} + q_3 z_{p^s})^i \cdot (x_1 + t z_1)^{p-1} \cdots (x_{p^s} + t_2 y_{p^s} + t_3 z_{p^s})^j, & \text{if } r = s; \\ (y_1 + q_3 z_1)^{p-1} \cdots (y_{p^r} + q_3 z_{p^r})^i \cdot (x_1 + t z_1)^{p-1} \cdots (x_{p^s} + t z_{p^s})^j, & \text{if } r > s; \end{cases}$$

When $s = 0$, and $r = 1$ then

$$C_6 = (x_1 + t z_1)^j (y_1 + q z_1)^{p-1} (y_p + q z_p)^i = \sum_{k=0}^{j} \binom{j}{k} t^k x_1^{j-k} z_1^k (y_1 + q z_1)^{p-1} (y_p + q z_p)^i$$

If $i > j$, then consider the following expression $R_n(q) = x_1^{j-n} z_1^k (y_1 + q z_1)^{p-1} (y_p + q z_p)^i$, for $0 \le n \le j - 1$. The case when $n = j$ is excluded because it gives $R_j(q) = z_1^j (y_1 + q z_1)^{p-1} (y_p + q z_p)^i = C_4$ such that $r = 1$ and $s = 0$. It is clear that for all n in that range we still have $i > n$ since $i > j$.

But we have a complete description for the expression $z_1^n (y_1 + q z_1)^{p-1} (y_p + q z_p)^i$, see C_4 second case such that $s = 0$. Thus for $z_1^n (y_1 + q z_1)^{p-1} (y_p + q z_p)^i$ there are p linearly independent elements, and hence $R_n(q) = x_1^{j-n} z_1^k (y_1 + q z_1)^{p-1} (y_p + q z_p)^i$, where $0 \le n \le j - 1$.

Moreover, these sets are linearly independent because each set involves x_1 of different exponent according as n. Therefore, there are jp basis elements.

If $s = 0$, $r = 1$ and $i \leq j$, so we can split to the following forms

$$C_6 = \sum_{k=0}^{i-1} \binom{j}{k} t^k x_1^{j-k} z_1^k (y_1 + qz_1)^{p-1}(y_p + qz_p)^i + \sum_{k=i}^{j} \binom{j}{k} t^k x_1^{j-k} z_1^k (y_1 + qz_1)^{p-1}(y_p + qz_p)^i.$$

Similarly, let $R_n(q) = x_1^{j-n} z_1^n (y_1 + qz_1)^{p-1}(y_p + qz_p)^i$, such that $0 \leq n \leq j-1$. Note that the case where $n = j$ is disregarded for the same reason in previous case. Obviously, for $0 \leq n \leq i-1$, we have $i > n$, so precisely by using the same argument as in previous case we get ip linearly independent elements.

Now, for $i \leq n \leq j-1$, then also C_4 the second case exposes that the expression $z_1^n (y_1 + qz_1)^{p-1}(y_p + qz_p)^i$ involves $p + i - n$ linearly independent elements, and so $R_n(q) = x_1^{j-k} z_1^k (y_1 + qz_1)^{p-1}(y_p + qz_p)^i$. For the same reason these sets of linearly independent elements are distinct. Thus, we have $(j-i)p - \sum_{a=0}^{j-i-1} a = (j-i)p - \frac{(j-i)^2-(j-i)}{2}$.

On the other hand, the basis elements of $R_n(q)$ such that $0 \leq n \leq i-1$ for those where $i \leq n \leq j-1$ are disjoint according as n, hence the total dimension of $R_n(q)$ is $ip + (j-i)p - \frac{(j-i)^2-(j-i)}{2} = jp - \frac{(j-i)^2-(j-i)}{2}$

If $s = 0$ and $r \geq 2$, so

$$C_6 = (x_1 + tz_1)^j (y_1 + qz_1)^{p-1} \cdots (y_{p^r} + qz_{p^r})^i$$

then the same techniques that has been used in previous case where $i > j$ can be used to show that there are jp basis elements.

If $r > s \geq 1$, then

$$C_6 = (y_1 + q_3 z_1)^{p-1} \cdots (y_{p^r} + q_3 z_{p^r})^i (x_1 + tz_1)^{p-1} \cdots (x_{p^s} + tz_{p^s})^j.$$

It is clear according to q_3 and t which are in $\mathbb{F}_p$, then C_6 in this case is spanned by p^2 elements, so we need to check the linearly independent elements. To make the proof easy to follow we will rearrange C_6 by the following

$$\begin{aligned} C_6 =& (x_1 + tz_1)^{p-1} x_p^{p-1} \cdots x_{p^s}^j (y_1 + q_3 z_1)^{p-1} \cdots (y_{p^r} + q_3 z_{p^r})^i + R_{x,z}(t) \cdot (y_1 + q_3 z_1)^{p-1} \cdots \\ & (y_{p^r} + q_3 z_{p^r})^i \end{aligned}$$

where $R_{x,z}(t) = (x_1 + tz_1)^{p-1} \cdots (x_{p^s} + tz_{p^s})^j - (x_1 + tz_1)^{p-1} x_p^{p-1} \cdots x_{p^s}^j = (x_1 + tz_1)^{p-1} \cdots \sum_{a=0}^{p-2} (-1)^{p-1-a} t^{p-1-a} x_{p^m}^a z_{p^m}^{p-1-a} \cdots (x_{p^s} + tz_{p^s})^j$, such that $1 \leq m \leq s-1$. Then, we choose the first summand in C_6 which is denoted by $Q(t, q_3)$ to investigate how many independent elements in C_6, however; there can be little concerned about this choosing.

Apparently, $Q(t,q_3) \notin M_*(3)$ unless $t=0$, so in fact it is not an element in $L_*(3)$, but each element in C_6 which is automatically in $L_*(3) \subseteq M_*(3)$ involves this expression. Thus, there is no problem with this choosing. While the second concern, the number of independent elements in that part does not determine the dimension of C_6, but it exposes how many at least linearly independent elements are there.

Now, let us consider

$$\begin{aligned} Q(t,q_3) =&(x_1+tz_1)^{p-1}x_p^{p-1}\cdots x_{p^s}^j(y_1+q_3z_1)^{p-1}\cdots(y_{p^r}+q_3z_{p^r})^i \\ =&\sum_{k=0}^{p-1}(-1)^k t^k x_1^{p-1-k}x_p^{p-1}\cdots x_{p^s}^j z_1^k(y_1+q_3z_1)^{p-1}\cdots(y_{p^r}+q_3z_{p^r})^i. \end{aligned}$$

Let $R_n(q_3)=x_1^{p-1-n}x_p^{p-1}\cdots x_{p^s}^j z_1^n(y_1+q_3z_1)^{p-1}\cdots(y_{p^r}+q_3z_{p^r})^i$ such that $0\le n\le p-1$. From C_4 we have that $z_1^n(y_1+q_3z_1)^{p-1}\cdots(y_{p^r}+q_3z_{p^r})^i$ involves p linearly independent elements which are determined by q_3, and so $R_n(q_3)$. Moreover, there are p expressions like $R_n(q_3)$ in $Q(t,q_3)$ and those expression are different according as the power on x_1, then Q_{t,q_3} contains p^2 linearly independent elements.

Thus, C_6 is spanned by p^2 elements, furthermore; these elements are independent. Hence,

$$Dim\ C_6=\begin{cases} jp, & \text{if } i>j,\ s=0 \text{ and } r=1;\\ jp-\frac{(j-i)^2-(j-i)}{2}, & \text{if } i\le j,\ s=0 \text{ and } r=1;\\ jp, & \text{if } s=0 \text{ and } r\ge 2;\\ p^2, & \text{if } r>s\ge 1. \end{cases}$$

Case 7 : $g_{r,i}^{tr}(1,q_2,q_3)\cdot g_{s,j}^{tr}(0,0,1)$.

$$\begin{aligned} C_7 =&z_1^{p-1}\cdots z_{p^s}^j\cdot g_{r,i}^{tr}(1,q_2,q_3) \\ =&z_1^{p-1}\cdots z_{p^s}^j(x_1+q_2y_1+q_3z_1)^{p-1}\cdots(x_{p^s}+q_2y_{p^s}+q_3z_{p^s})^{p-1}\cdots\{(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^i+ \\ & i(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^{i-1}\sum_{\substack{i_{r-1}+j_{r-1}+k_{r-1}=p,\\ i_{r-1},j_{r-1},k_{r-1}<p}}\frac{q_2^{j_{r-1}}q_3^{k_{r-1}}}{i_{r-1}!j_{r-1}!k_{r-1}!}x_{p^{r-1}}^{i_{r-1}}y_{p^{r-1}}^{j_{r-1}}z_{p^{r-1}}^{k_{r-1}}\} \\ =&z_1^{p-1}\cdots z_{p^{s-1}}^{p-1}\cdot(x_1+q_2y_1)^{p-1}\cdots(x_{p^{s-1}}+q_2y_{p^{s-1}})^{p-1}\cdot z_{p^s}^j(x_{p^s}+q_2y_{p^s}+q_3z_{p^s})^{p-1} \end{aligned}$$

$$\{(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^{p-1}+(p-1)(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^{p-2}\cdot$$

$$\sum_{\substack{i_s+j_s+k_s=p,\\ i_s,j_s,k_s<p}}\frac{q_2^{j_s}q_3^{k_s}}{i_s!j_s!k_s!}x_{p^s}^{i_s}y_{p^s}^{j_s}z_{p^s}^{k_s}\}\{(x_{p^{s+2}}+q_2y_{p^{s+2}}+q_3z_{p^{s+2}})^{p-1}+$$

$$(p-1)(x_{p^{s+2}}+q_2y_{p^{s+2}}+q_3z_{p^{s+2}})^{p-2}\sum_{\substack{i_{s+1}+j_{s+1}+k_{s+1}=p,\\ i_{s+1},j_{s+1},k_{s+1}<p}}\frac{q_2^{j_{s+1}}q_3^{k_{s+1}}}{i_{s+1}!j_{s+1}!k_{s+1}!}x_{p^{s+1}}^{i_{s+1}}y_{p^{s+1}}^{j_{s+1}}z_{p^{s+1}}^{k_{s+1}}\}\cdots$$

$$\{(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^i+i(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^{i-1}\cdot$$

$$\sum_{\substack{i_{r-1}+j_{r-1}+k_{r-1}=p,\\ i_{r-1},j_{r-1},k_{r-1}<p}}\frac{q_2^{j_{r-1}}q_3^{k_{r-1}}}{i_{r-1}!j_{r-1}!k_{r-1}!}x_{p^{r-1}}^{i_{r-1}}y_{p^{r-1}}^{j_{r-1}}z_{p^{r-1}}^{k_{r-1}}\}.$$

If $r=s$, then

$$C_7=z_1^{p-1}\cdots z_{p^s}^{j}(x_1+q_2y_1)^{p-1}\cdots(x_{p^s}+q_2y_{p^s}+q_3z_{p^s})^i,$$

let $w_{p^n}^k=(x_{p^n}+q_2y_{p^n})^k$, for $0\le n\le s$ and $0\le k\le p-1$, so

$$C_7=w_1^{p-1}z_1^{p-1}\cdots w_{p^{s-1}}^{p-1}z_{p^{s-1}}^{p-1}z_{p^s}^{j}(w_{p^s}+q_3z_{p^s})^i$$

but $C_7=f_{wz}^s\left(z_1^j(w_1+q_3z_1)^i\right)$, where $f_{wz}=w_1^{p-1}z_1^{p-1}e(\theta)$. Thus, we need only to examine the independency of the expression $Q(q_3)=z_{p^s}^j(w_{p^s}+q_3z_{p^s})^i$.

Now, if $i+j\le p-1$, then

$$Q(q_3)=\sum_{n=0}^{i}\binom{i}{n}\xi^nq_3^nw_{p^s}^{i-n}z_{p^s}^{n+j}.$$

Obviously, each monomial in $Q(q_3)$ represents a basis element, so that; there are $i+1$ linearly independent elements, namely; $\{f_{w,z}^{s-1}(w_1^{p-1}z_1^{p-1})w_{p^s}^{i-n}z_{p^s}^{n+j}:0\le n\le i\}$. Taken any one of them which is $B_l=f_{w,z}^{s-1}(w_1^{p-1}z_1^{p-1})w_{p^s}^{i-l}z_{p^s}^{n+l}$, and replacing the part $w_{p^n}^k=(x_{p^n}+q_2y_{p^n})^k$ implies

$$B_l=z_1^{p-1}\cdots z_{p^s}^{n+l}(x_1+q_2y_1)^{p-1}\cdots(x_{p^s}+q_2y_{p^s})^{i-l}$$

but B_l is spanned by p linearly independent elements are determined by q_2 such that $q_2\in\mathbb{F}_p$, and the $B_l's$ are distinct. Consequently, we have $(i+1)p$ basis elements in this case.

If $i+j\ge p$, then using the same techniques as above gives

$$Q(q_3)=\sum_{n=0}^{i}\binom{i}{n}\xi^nq_3^nw_{p^s}^{i-n}z_{p^s}^{n+j}$$

since $n+j \leq p-1$, otherwise; $Q(q_3)=0$, so $n \leq p-1-j$, and that is;

$$Q(q_3) = \sum_{n=0}^{p-1-j} \binom{i}{n} \xi^n q_3^n w_{p^s}^{i-n} z_{p^s}^{n+j}.$$

Then, we infer the dimension in this range of i and j is $(p-j)p$.

Turning to, C_3 in case $r=s$. Precisely, same argument as in case C_7 establishes that the basis is given by $\{z_1^{p-1}\cdots z_{p^s}^{n+i}(x_1+t_2y_1)^{p-1}\cdots(x_{p^s}+t_2y_{p^s})^{j-n}$ such that $0 \leq n \leq j$ where $t_2 \in \mathbb{F}_p\}$, but these elements are subsets from the basis elements of C_7 because in this case $i \geq j$. Therefore, $C_3 \subseteq C_7$. Similarly, if $i+j \geq p$ same reason implies $C_3 \subseteq C_7$, so C_3 will be disregarded when someone considers this case.

If $r = s+1$, then

$$\begin{aligned} C_7 =& z_1^{p-1}\cdots z_{p^{s-1}}^{p-1}\cdot(x_1+q_2y_1)^{p-1}\cdots(x_{p^{s-1}}+q_2y_{p^{s-1}})^{p-1}\cdot \\ & z_{p^s}^j(x_{p^s}+q_2y_{p^s}+q_3z_{p^s})^{p-1}\{(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^i+ \\ & i(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^{i-1}\cdot \sum_{\substack{i_s+j_s+k_s=p,\\ i_s,j_s,k_s<p}} \frac{q_2^{j_s}q_3^{k_s}}{i_s!j_s!k_s!}x_{p^s}^{i_s}y_{p^s}^{j_s}z_{p^s}^{k_s}\} \end{aligned}$$

We need only to consider the expression

$$\begin{aligned} R(q_1,q_2) =& z_{p^s}^j(x_{p^s}+q_2y_{p^s}+q_3z_{p^s})^{p-1}\{(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^i+ \\ & i(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^{i-1}\cdot \sum_{\substack{i_s+j_s+k_s=p,\\ i_s,j_s,k_s<p}} \frac{q_2^{j_s}q_3^{k_s}}{i_s!j_s!k_s!}x_{p^s}^{i_s}y_{p^s}^{j_s}z_{p^s}^{k_s}\} \end{aligned}$$

Now, if $j=p-1$, then

$$\begin{aligned} C_7 =& (x_{p^s}+q_2y_{p^s})^{p-1}z_{p^s}^{p-1}(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^i \\ =& (x_{p^s}+q_2y_{p^s})^{p-1}z_{p^s}^{p-1}\sum_{n=0}^{i}\binom{i}{n}q_3^n(x_{p^{s+1}}+q_2y_{p^{s+1}})^{i-n}z_{p^{s+1}}^n. \end{aligned}$$

Again *Vandermonde* matrix produces $i+1$ basis elements determined by q_3. On the other hand, each of them can be written by p basis elements, so the dimension in this case $(i+1)p$, but when $n=i$ for this value $C_7 = C_3$. Thus, the dimension becomes ip.

If $j \neq p-1$, then; let

$$R_1 = z_{p^s}^j(x_{p^s}+q_2y_{p^s}+q_3z_{p^s})^{p-1}(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^i$$

and

$$R_2 = z_{p^s}^j(x_{p^s}+q_2y_{p^s}+q_3z_{p^s})^{p-1}(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^{i-1}\sum_{\substack{i_s+j_s+k_s=p,\\ i_s,j_s,k_s<p}} \frac{q_2^{j_s}q_3^{k_s}}{i_s!j_s!k_s!}x_{p^s}^{i_s}y_{p^s}^{j_s}z_{p^s}^{k_s}.$$

So,

$$R_1 = \sum_{n=0}^{p-1}\sum_{m=0}^{n}(-1)^n\binom{n}{m}q_2^{n-m}q_3^{p-1-n}x_{p^s}^m y_{p^s}^{n-m}z_{p^s}^{p+j-n-1}\sum_{k=0}^{i}\sum_{l=0}^{k}\binom{i}{k}\binom{k}{l}q_2^{k-l}q_3^{i-k}x_{p^s+1}^l y_{p^s+1}^{k-l}z_{p^s+1}^{i-k}$$

since, $p+j-n-1 \le p-1 \Longrightarrow n \ge j$, thus;

$$\begin{aligned}R_1 = &\sum_{n=0}^{p-j-1}\sum_{m=0}^{n+j}(-1)^{n+j}\binom{n+j}{m}q_2^{n+j-m}q_3^{p-n-j-1}x_{p^s}^m y_{p^s}^{n+j-m}z_{p^s}^{p-n-1}\\ &\sum_{k=0}^{i}\sum_{l=0}^{k}\binom{i}{k}\binom{k}{l}q_2^{k-l}q_3^{i-k}x_{p^s+1}^l y_{p^s+1}^{k-l}z_{p^s+1}^{i-k}\\ = &\sum_{n=0}^{p-j-1}\sum_{k=0}^{i}\sum_{m=0}^{n+j}\sum_{l=0}^{k}(-1)^{n+j}\binom{n+j}{m}\binom{i}{k}\binom{k}{l}q_2^{n+k+j-m-l}q_3^{p+i-j-n-k-1}\\ &x_{p^s}^m y_{p^s}^{n+j-m}z_{p^s}^{p-n-1}x_{p^s+1}^l y_{p^s+1}^{k-l}z_{p^s+1}^{i-k}.\end{aligned}$$

Set $\Phi_{n,m}^{k,l} = (-1)^{n+j}\binom{n+j}{m}\binom{i}{k}\binom{k}{l}x_{p^s}^m y_{p^s}^{n+j-m}z_{p^s}^{p-n-1}x_{p^s+1}^l y_{p^s+1}^{k-l}z_{p^s+1}^{i-k}$, $a = n+k$, and $b = m+l$. Hence,

$$R_1 = \sum_{a=0}^{p+i-j-1}\sum_{b=0}^{a+j}q_2^{a+j-b}q_3^{p+i-j-a-1}\Phi_{a,b}$$

Turning to,

$$R_2 = \sum_{a=0}^{i-1}\sum_{b=0}^{p+a-j-2}q_2^{p+a-b-1}q_3^{p+i-j-a-2}W_{a,b} + \sum_{a=i}^{p+i-j-3}\sum_{b=0}^{p+2(i-1)-j-a-2}q_2^{p+i-2-b}q_3^{p+i-j-a-2}W_{a,b}$$

Now, if $i > j$, then

$$\begin{aligned}R_1 = &\sum_{a=0}^{p+i-j-1}\sum_{b=0}^{a+j}q_2^{a+j-b}q_3^{p+i-j-a-1}\Phi_{a,b}\\ = &\sum_{a=0}^{i-j-1}\sum_{b=0}^{a+j}q_2^{a+j-b}q_3^{p+i-j-a-1}\hat{\Phi}_{a,b} + \sum_{a=i-j}^{p+i-j-1}\sum_{b=0}^{a+j}q_2^{a+j-b}q_3^{p+i-j-a-1}\Phi_{a,b}\\ = &q_3^{p-1}\sum_{a=0}^{i-j-1}\sum_{b=0}^{a+j}q_2^{a+j-b}q_3^{i-j-a}\hat{\Phi}_{a,b} + \sum_{a=i-j}^{p+i-j-1}\sum_{b=0}^{a+j}q_2^{a+j-b}q_3^{p+i-j-a-1}\Phi_{a,b}\end{aligned}$$

Since, $q_3^{p-1} = 1$ for $q_3 \in \mathbb{F}_p$, and clearly the power of q_3 is between 0 and $p-1$ in the second summation, while in the first summation $q_3's$ exponent has the range $1, \cdots i-j-1 \le p-1$. On the other hand, the power of q_2 depends on the values of a, and it is clear that $a's$

values in the second summation are greater than the corresponding one in the first summation.

Hence,

$$R_1 = \sum_{a=i-j}^{p+i-j-1} \sum_{b=0}^{a+j} q_2^{a+j-b} q_3^{p+i-j-a-1} \Lambda_{a,b},$$

where $\Lambda_{a,b} = \hat{\Phi}_{a,b} + \Phi_{a,b}$ such that $q_2^c q_3^d$ that relates with $\Phi_{a,b}$ and $q_2^n q_3^m$ that is linked with $\hat{\Phi}_{a,b}$ are identical, otherwise; $\Lambda_{a,b} = \Phi_{a,b}$ or $\Lambda_{a,b} = \hat{\Phi}_{a,b}$. $\Lambda_{a,b} \neq 0$ because $\hat{\Phi}_{a,b} \neq \Phi_{a,b}$ for all values of a, b in both, thus;

$$R_1 = \sum_{a=0}^{p-1} \sum_{b=0}^{a+i} q_2^{a+i-b} q_3^{p-1-a} \Lambda_{a,b} \tag{6.3}$$

Turning to,

$$\begin{aligned} R_2 &= \sum_{a=0}^{i-1} \sum_{b=0}^{p+a-j-2} q_2^{p+a-b-1} q_3^{p+i-j-a-2} W_{a,b} + \sum_{a=i}^{p+i-j-3} \sum_{b=0}^{p+2(i-1)-a-j-2} q_2^{p+i-b-2} q_3^{p+i-j-a-2} W_{a,b} \\ &= \sum_{a=0}^{i-j-2} \sum_{b=0}^{p+a-j-2} q_2^{p+a-b-1} q_3^{p+i-j-a-2} W_{a,b} + \sum_{a=i-j-1}^{i-1} \sum_{b=0}^{p+a-j-2} q_2^{p+a-b-1} q_3^{p+i-j-a-2} W_{a,b} + \\ &\quad \sum_{a=i}^{p+i-j-3} \sum_{b=0}^{p+2(i-1)-a-j-2} q_2^{p+i-b-2} q_3^{p+i-j-a-2} W_{a,b}, \end{aligned}$$

same argument that is used in case R_1 can be used here, so

$$\begin{aligned} R_2 &= \sum_{a=i-j-1}^{i-1} \sum_{b=0}^{p+a-j-2} q_2^{p+a-b-1} q_3^{p+i-j-a-2} W_{a,b} + \sum_{a=i}^{p+i-j-3} \sum_{b=0}^{p+2(i-1)-a-j-2} q_2^{p+i-b-2} q_3^{p+i-j-a-2} W_{a,b} \\ &= \sum_{a=0}^{j} \sum_{b=0}^{p+a+i-2j-3} q_2^{p+a+i-j-b-2} q_3^{p-a-1} \bar{W}_{a,b} + \sum_{a=i}^{p+i-j-3} \sum_{b=0}^{p+2(i-1)-a-j-2} q_2^{p+i-b-2} q_3^{p+i-j-a-2} W_{a,b}. \end{aligned}$$

When $a = 0$

$$R_1 = q_2^i q_3^{p-1} \Lambda_{0,0} + q_2^{i-1} q_3^{p-1} \Lambda_{0,1} + \cdots + q_2 q_3^{p-1} \Lambda_{0,i-1} + q_3^{p-1} \Lambda_{0,i},$$

and

$$R_0 = q_2^{p+i-j-2} q_3^{p-1} W_{0,0} + q_2^{p+i-j-3} q_3^{p-1} W_{0,1} + \cdots + q_2^{j+1} q_3^{p-1} W_{0,p+i-2j-3},$$

since $i > j$, then $p+i-j-2 \geq p-1$. If $p+i-j-2 > p$, then $q_2^{p+i-j-k} q_3^{p-1} W_{0,p+i-j-k} = q_2^{p-1} q_2^{i-j-k+1} q_3^{p-1} W_{0,p+i-j-k}$, so rearranging R_2 and adding it to R_2

$$R_1 + R_2 = q_2^{p-1} q_3^{p-1} \theta_{0,p-1} + q_2^{p-2} q_3^{p-1} \theta_{0,p-2} + \cdots + q_3^{p-1} \theta_{0,0}.$$

Note, because of; $\Lambda_{i,j} \neq W_{i,j}$, and $\Lambda_{i,j} \neq 0$ and $W_{i,j} \neq 0$, $\theta_{i,j} \neq 0$. Similarly, when one considers $a = 1, \cdots, p-1$. Hence,

$$R(q_2, q_3) = \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} q_2^{p-1-a} q_3^{p-1-b} \theta_{a,b}$$

For a fixed $b = c$ consider

$$R(q_2, q_3) = q_3^{p-1-c} \sum_{a=0}^{p-1} q_2^{p-1-a} \theta_{a,c}$$

let

$$\sum_{q_2=0}^{p-1} \sum_{q_3=0}^{p-1} q_3^{p-1-c} \alpha_{q_2,q_3} \sum_{a=0}^{p-1} q_2^{p-1-a} \theta_{a,c} = \sum_{a=0}^{p-1} \theta_{a,c} \sum_{q_3=0}^{p-1} \sum_{q_2=0}^{p-1} q_3^{p-1-c} q_2^{p-1-a} \alpha_{q_2,q_3} = 0,$$

since $\theta'_{a,c}s$ are distinct, we get

$$\sum_{q_3=0}^{p-1} \sum_{q_2=0}^{p-1} q_3^{p-1-c} q_2^{p-1-a} \alpha_{q_2,q_3} = 0 \qquad \text{for each } a,$$

the above homogeneous systems can be reduced to the following system

$$\sum_{q_2=0}^{p-1} q_2^{p-1-a} \alpha_{q_2,q_3} = 0.$$

Using *Vandermonde* determinant shows that there are p basis elements, for $0 \leq a \leq p-1$, but an alternative choice of b gives p different linearly independent elements, so we conclude the dimension in this case is p^2.

If $i \leq j$, then

$$\begin{aligned}
R(q_2, q_3) =& R_1 + R_2 \\
=& \sum_{a=0}^{p+i-j-1} \sum_{b=0}^{a+j} q_{a+j-b} q_3^{p+i-j-a-1} \Phi_{a,b} + \sum_{a=0}^{i-1} \sum_{b=0}^{p+a-j-2} q_2^{p+a-b-1} q_3^{p+i-j-a-2} W_{a,b} + \\
& \sum_{a=i}^{p+i-j-3} \sum_{b=0}^{p+2(i-1)-j-a-2} q_2^{p+i-b-2} q_3^{p+i-j-a-2} W_{a,b} \\
=& \sum_{b=0}^{j} q_2^{j-b} q_3^{p+i-j-1} \Phi_{0,b} + \sum_{a=0}^{p+i-j-2} \sum_{b=0}^{a+j+1} q_{a+j+1-b} q_3^{p+i-j-a-2} \Phi_{a+1,b} + \\
& \sum_{a=0}^{i-1} \sum_{b=0}^{p+a-j-2} q_2^{p+a-b-1} q_3^{p+i-j-a-2} W_{a,b} + \sum_{a=i}^{p+i-j-3} \sum_{b=0}^{p+2(i-1)-j-a-2} q_2^{p+i-b-2} q_3^{p+i-j-a-2} W_{a,b}
\end{aligned}$$

Excluding the first summation from previous expression then the remaining parts can be gathered (as we have done in previous case) and we get

$$R(q_2,q_3)=\sum_{b=0}^{j} q_2^{j-b}q_3^{p+i-j-1}\Phi_{0,b}+\sum_{a=0}^{p+i-j-2}\sum_{b=0}^{p-1} q_2^{p-1-b}q_3^{p+i-j-a-2}\theta_{a,b}$$

The first summation gives $j+1$ basis elements, while; the second one provides $(p+i-j-1)p$ linearly independent elements. Hence, the dimension is $(p+i-j)p-(p-1-j)$.

If $r\geq s+2$, then (from the case where $r=s+1$, and $i>j$(from relation 6.3) we infer the dimension of this case which is p^2. To sum up,

$$Dim\ C_7=\begin{cases}(i+1)p, & \text{if } i+j\leq p-1, \text{ and } r=s;\\ (p-j)p, & \text{if } i+j\geq p, \text{ and } r=s;\\ (i+1)p, & \text{if } j=p-1, \text{ and } r=s+1;\\ (p+i-j)p-(p-1-j), & \text{if } j\geq i, \text{ and } r=s+1;\\ p^2, & \text{if } i>j, \text{ and } r=s+1;\\ p^2, & \text{if } r\geq s+2.\end{cases}$$

Case 8: $g^{tr}_{r,i}(\bar{q_1},q_2,q_3)\cdot g^{tr}_{s,j}(0,\bar{t_2},t_3)$.

If $r\geq s+2$ and $s\geq 1$, then

$$\begin{aligned}C_8=&g^{tr}_{s,j}(0,1,t_3)\cdot g^{tr}_{r,i}(1,q_2,q_3)\\ =&(y_1+tz_1)^{p-1}\cdots(y_{p^s}+tz_{p^s})^j\cdot(x_1+q_2y_1+q_3z_1)^{p-1}\cdots(x_{p^s}+q_2y_{p^s}+q_3z_{p^s})^{p-1}\\ &\{(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^{p-1}+(p-1)(x_{p^{s+1}}+q_2y_{p^{s+1}}+q_3z_{p^{s+1}})^{p-2}\\ &\cdot\sum_{\substack{i_s+j_s+k_s=p,\\ i_s,j_s,k_s<p}}\frac{q_2^{j_s}q_3^{k_s}}{i_s!j_s!k_s!}x_{p^s}^{i_s}y_{p^s}^{j_s}z_{p^s}^{k_s}\}\\ &\{(x_{p^{s+2}}+q_2y_{p^{s+2}}+q_3z_{p^{s+2}})^{p-1}+(p-1)(x_{p^{s+2}}+q_2y_{p^{s+2}}+q_3z_{p^{s+2}})^{p-2}\\ &\cdot\sum_{\substack{i_{s+1}+j_{s+1}+k_{s+1}=p,\\ i_{s+1},j_{s+1},k_{s+1}<p}}\frac{q_2^{j_{s+1}}q_3^{k_{s+1}}}{i_{s+1}!j_{s+1}!k_{s+1}!}x_{p^{s+1}}^{i_{s+1}}y_{p^{s+1}}^{j_{s+1}}z_{p^{s+1}}^{k_{s+1}}\}\cdots\{(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^i+\\ &i(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^{i-1}\cdot\sum_{\substack{i_{r-1}+j_{r-1}+k_{r-1}=p,\\ i_{r-1},j_{r-1},k_{r-1}<p}}\frac{q_2^{j_{r-1}}q_3^{k_{r-1}}}{i_{r-1}!j_{r-1}!k_{r-1}!}x_{p^{r-1}}^{i_{r-1}}y_{p^{r-1}}^{j_{r-1}}z_{p^{r-1}}^{k_{r-1}}\}\end{aligned}$$

Let us consider

$$R(t,q_2,q_3) =(y_1+tz_1)^{p-1}\cdot\{(x_{p^{r-1}}+q_2y_{p^{r-1}}+q_3z_{p^{r-1}})^{p-1}+(p-1)(x_{p^{r-1}}+q_2y_{p^{r-1}}+q_3z_{p^{r-1}})^{p-2} \sum_{\substack{i_{r-2}+j_{r-2}+k_{r-2}=p,\\ i_{r-2},j_{r-2},k_{r-2}<p}} \frac{q_2^{j_{r-2}}q_3^{k_{r-2}}}{i_{r-2}!j_{r-2}!k_{r-2}!}x_{p^{r-2}}^{i_{r-2}}y_{p^{r-2}}^{j_{r-2}}z_{p^{r-2}}^{k_{r-2}}\}\{(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^i+ i(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^{i-1} \sum_{\substack{i_{r-1}+j_{r-1}+k_{r-1}=p,\\ i_{r-1},j_{r-1},k_{r-1}<p}} \frac{q_2^{j_{r-1}}q_3^{k_{r-1}}}{i_{r-1}!j_{r-1}!k_{r-1}!}x_{p^{r-1}}^{i_{r-1}}y_{p^{r-1}}^{j_{r-1}}z_{p^{r-1}}^{k_{r-1}}\}$$

We looking at the following part from $R(t,q_2,q_3)$ to investigate the dimension of C_8 for values of r and s.

$$Q(t,q_2,q_3) =(y_1+tz_1)^{p-1}\cdot Q(q_2,q_3),$$

where

$$Q(q_2,q_3) =(x_{p^{r-1}}+q_2y_{p^{r-1}}+q_3z_{p^{r-1}})^{p-1}\{(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^i+ i(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^{i-1} \sum_{\substack{i_{r-1}+j_{r-1}+k_{r-1}=p,\\ i_{r-1},j_{r-1},k_{r-1}<p}} \frac{q_2^{j_{r-1}}q_3^{k_{r-1}}}{i_{r-1}!j_{r-1}!k_{r-1}!}x_{p^{r-1}}^{i_{r-1}}y_{p^{r-1}}^{j_{r-1}}z_{p^{r-1}}^{k_{r-1}}\}.$$

Same technique that have been used in **Proposition 1** can be applied for $Q(q_2,q_3)$(replacing x_1,y_1,z_1 by $x_{p^{r-1}},y_{p^{r-1}},z_{p^{r-1}}$) to showing it provides p^2 linearly independent elements. On the other hand,

$$Q(t,q_2,q_3) = \sum_{n=0}^{p-1}(-1)^n t^n y_1^{p-1-n}z_1^n\cdot Q(q_2,q_3)$$

Set $\phi_n=(-1)^n y_1^{p-1-n}z_1^n Q(q_2,q_3)$, and assume that

$$\sum_{t=0}^{p-1}\sum_{n=0}^{p-1}t^n\xi_t\phi_n=\sum_{n=0}^{p-1}\phi_n\sum_{t=0}^{p-1}t^n\xi_t=0$$

the linearly independence of ϕ_n's gives $\sum_{t=0}^{p-1}t^n\xi_t=0$ for $0\le n\le p-1$, and *Vandermonde*'s determinant shows that the only solution for the homogeneous system $\sum_{t=0}^{p-1}t^n\xi_t=0$ will be the zero solution. Hence, we have p basis elements. Consequently, the dimension in this case is p^3.

If $s=0$ and $r\ge 2$, then

$$C_8 =(y_1+tz_1)^j\cdot Q(q_2,q_3)$$

where $Q(q_2, q_3)$ as in previous case, which involves p^2 basis elements, and same argument gives C_8 is written by $(j+1)p^2$ linearly independent elements. Note $C_7 \subset C_8$ in this case.

Case 9 $g^{tr}_{r,i}(\bar{q_1}, q_2, q_3) \cdot g^{tr}_{s,j}(\bar{t_1}, t_2, t_3)$.
The following calculation just shows this case will be disregarded because either $C_9 = C_7$ or $C_9 = C_8$. Firstly, we simplify such product, so consider

$$\begin{aligned}
Q =&(x_1 + q_2 y_1 + q_3 z_1)^{p-1}\{(x_p + q_2 y_p + q_3 z_p)^{p-1} + (p-1)(x_p + q_2 y_p + q_3 z_p)^{p-2} \\
&\sum_{\substack{i_0+j_0+k_0=p,\\ i_0,j_0,k_0<p}} \frac{q_2^{j_0} q_3^{k_0}}{i_0! j_0! k_0!} x_1^{i_0} y_1^{j_0} z_1^{k_0}\} \cdot (x_1 + t_2 y_1 + t_3 z_1)^{p-1}\{(x_p + t_2 y_p + t_3 z_p)^{p-1} \\
&+(p-1)(x_p + t_2 y_p + t_3 z_p)^{p-2} \sum_{\substack{i_0+j_0+k_0=p,\\ i_0,j_0,k_0<p}} \frac{t_2^{j_0} t_3^{k_0}}{i_0! j_0! k_0!} x_1^{i_0} y_1^{j_0} z_1^{k_0}\} \\
=&(x_1 + q_2 y_1 + q_3 z_1)^{p-1}(x_1 + t_2 y_1 + t_3 z_1)^{p-1} \cdot \{(x_p + q_2 y_p + q_3 z_p)^{p-1}(x_p + t_2 y_p + t_3 z_p)^{p-1} \\
&+(p-1)(x_p + q_2 y_p + q_3 z_p)^{p-1}(x_p + t_2 y_p + t_3 z_p)^{p-2} \sum_{\substack{i_0+j_0+k_0=p,\\ i_0,j_0,k_0<p}} \frac{t_2^{j_0} t_3^{k_0}}{i_0! j_0! k_0!} x_1^{i_0} y_1^{j_0} z_1^{k_0} \\
&+(p-1)(x_p + t_2 y_p + t_3 z_p)^{p-1}(x_p + q_2 y_p + q_3 z_p)^{p-2} \sum_{\substack{i_0+j_0+k_0=p,\\ i_0,j_0,k_0<p}} \frac{q_2^{j_0} q_3^{k_0}}{i_0! j_0! k_0!} x_1^{i_0} y_1^{j_0} z_1^{k_0} \\
&+(x_p + t_2 y_p + t_3 z_p)^{p-2}(x_p + q_2 y_p + q_3 z_p)^{p-2} \sum_{\substack{i_0+j_0+k_0=p,\\ i_0,j_0,k_0<p}} \frac{q_2^{j_0} q_3^{k_0}}{i_0! j_0! k_0!} x_1^{i_0} y_1^{j_0} z_1^{k_0} \\
&\cdot \sum_{\substack{i_0+j_0+k_0=p,\\ i_0,j_0,k_0<p}} \frac{t_2^{j_0} t_3^{k_0}}{i_0! j_0! k_0!} x_1^{i_0} y_1^{j_0} z_1^{k_0}\} \\
=&(x_1 + q_2 y_1 + q_3 z_1)^{p-1}(x_1 + t_2 y_1 + t_3 z_1)^{p-1}(x_p + q_2 y_p + q_3 z_p)^{p-1}(x_p + t_2 y_p + t_3 z_p)^{p-1}.
\end{aligned}$$

Continuing the same procedure by replacing x_1, y_1, z_1 by $x_{p^n}, y_{p^n}, z_{p^n}$ and x_p, y_p, z_p by $x_{p^{n+1}}, y_{p^{n+1}}, z_{p^{n+1}}$ for $1 \le n \le s-1$ yields

$$\begin{aligned}
C_9 =&g^{tr}_{r,i}(\bar{q_1}, q_2, q_3) \cdot g^{tr}_{s,j}(\bar{t_1}, t_2, t_3) \\
=&(x_1 + t_2 y_1 + t_3 z_1)^{p-1}(x_1 + q_2 y_1 + q_3 z_1)^{p-1} \cdots (x_{p^s} + t_2 y_{p^s} + t_3 z_{p^s})^{j}(x_{p^s} + q_2 y_{p^s} + q_3 z_{p^s})^{p-1} \\
&+\{(x_{p^{s+1}} + q_2 y_{p^{s+1}} + q_3 z_{p^{s+1}})^{p-1} + (p-1)(x_{p^{s+1}} + q_2 y_{p^{s+1}} + q_3 z_{p^{s+1}})^{p-2} \\
&\cdot \sum_{\substack{i_s+j_s+k_s=p,\\ i_s,j_s,k_s<p}} \frac{q_2^{j_s} q_3^{k_s}}{i_s! j_s! k_s!} x_{p^s}^{i_s} y_{p^s}^{j_s} z_{p^s}^{k_s}\} \cdots \{(x_{p^r} + q_2 y_{p^r} + q_3 z_{p^r})^{i} + i(x_{p^r} + q_2 y_{p^r} + q_3 z_{p^r})^{i-1} \\
&\cdot \sum_{\substack{i_{r-1}+j_{r-1}+k_{r-1}=p,\\ i_{r-1},j_{r-1},k_{r-1}<p}} \frac{q_2^{j_{r-1}} q_3^{k_{r-1}}}{i_{r-1}! j_{r-1}! k_{r-1}!} x_{p^{r-1}}^{i_{r-1}} y_{p^{r-1}}^{j_{r-1}} z_{p^{r-1}}^{k_{r-1}}\}
\end{aligned}$$

Now, consider

$$\begin{aligned}R_1 =&(x_1 + t_2y_1 + t_3z_1)^{p-1} \cdot (x_1 + q_2y_1 + q_3z_1)^{p-1}\\ &\sum_{m=0}^{p-1}(-1)^m x_1^{p-1-m}(t_2y_1+t_3z_1)^m \sum_{n=0}^{p-1}(-1)^n x_1^{p-1-n}(q_2y_1+q_3z_1)^n\\ =&\sum_{m=0}^{p-1}\sum_{n=0}^{p-1}(-1)^{n+m}x_1^{2p-2-m-n}(t_2y_1+t_3z_1)^m(q_2y_1+q_3z_1)^n\end{aligned}$$

put $k = m + n \Longrightarrow 0 \le k \le 2p-2$ and $n = k - m$

$$R_1 = \sum_{k=0}^{2p-2}\sum_{m=0}^{p-1}(-1)^k x_1^{2p-2-k}(t_2y_1+t_3z_1)^m(q_2y_1+q_3z_1)^{k-m}.$$

But, the total power of x_1 have to be $2p-2-k \le p-1 \Longrightarrow k \ge p-1$; otherwise $R_1 = 0$, so

$$\begin{aligned}R_1 =& \sum_{k=p-1}^{2p-2}\sum_{m=0}^{p-1}(-1)^k x_1^{2p-2-k}(t_2y_1+t_3z_1)^m(q_2y_1+q_3z_1)^{k-m}\\ =&\sum_{k=0}^{p-1}\sum_{m=0}^{p-1}(-1)^{p-1+k}x_1^{p-1-k}(t_2y_1+t_3z_1)^m(q_2y_1+q_3z_1)^{p-1+k-m}\\ =&\sum_{m=0}^{p-1}(t_2y_1+t_3z_1)^m(q_2y_1+q_3z_1)^{p-1-m}\sum_{k=0}^{p-1}(-1)^k x_1^{p-1-k}(q_2y_1+q_3z_1)^k\\ =&\{(q_2y_1+q_3z_1)-(t_2y_1+t_3z_1)\}^{p-1}(x_1+q_2y_1+q_3z_1)^{p-1}\\ =&\{(q_2-t_2)y_1+(q_3-t_3)z_1)\}^{p-1}(x_1+q_2y_1+q_3z_1)^{p-1}\end{aligned}$$

for a fixed q_2 and q_3, we have $0 \le q_2 - t_2 \le p-1$ and $0 \le q_3 - t_3 \le p-1$ unless $q_2 = t_2$ and $q_3 = t_3$ in this case R_1 will be zero. Thus

$$R_1 = (\hat{t}_2y_1 + \hat{t}_3z_1)^{p-1}(x_1 + q_2y_1 + q_3z_1)^{p-1}$$

where $\hat{t}_2, \hat{t}_3, q_2, q_3 \in \mathbb{F}_p$. Repeating the same process by replacing x_1, y_1, z_1 by $x_{p^n}, y_{p^n}, z_{p^n}$ for $1 \le n \le s$ provides the following

$$\begin{aligned}C_9 =&(t_1y_1+t_2z_1)^{p-1}\cdots(t_1y_{p^s}+t_2z_{p^s})^j\cdot(x_1+q_2y_1+q_3z_1)^{p-1}\cdots(x_{p^s}+q_2y_{p^s}+q_3z_{p^s})^{p-1}\\ &\cdots\{(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^i + i(x_{p^r}+q_2y_{p^r}+q_3z_{p^r})^{i-1}\\ &\cdot\sum_{\substack{i_{r-1}+j_{r-1}+k_{r-1}=p,\\ i_{r-1},j_{r-1},k_{r-1}<p}}\frac{q_2^{j_{r-1}}q_3^{k_{r-1}}}{i_{r-1}!j_{r-1}!k_{r-1}!}x_{p^{r-1}}^{i_{r-1}}y_{p^{r-1}}^{j_{r-1}}z_{p^{r-1}}^{k_{r-1}}\}\end{aligned}$$

So, if $t_1 = 0$, then $C_9 = C_7$, otherwise; $C_9 = C_8$. □

Chapter 7

General comments on $M_*(k)/L_*(k)$

7.1 Background and Existing Results

Between the space $M_n(k)$ and $L_n(k)$ there is a space that can be provided some information, and complete the following sequence to be exact

$$0 \longrightarrow L_n(k) \xrightarrow{\ i\ } M_n(k) \xrightarrow{\ \pi\ } M_n(k)/L_n(k) \longrightarrow 0,$$

where i is the inclusion of $L_n(k)$ into $M_n(k)$ and π the canonical projection. In case when $p = 2$, *Alghamdi* in [1] showed that this space is almost trivial for $k = 1, 2, 3$. Although for $k = 1, 2$ the space $M_n(k)$ is identical with $L_n(k)$ for all n, when $k = 3$ we see the deviation in the degrees $n = 2^{s+3} + 2^{s+1} + 2^s - 3$ for $s \geq 0$. In those degrees dim $M_n(3)/L_n(3) = 1$, such that dim $M_n(3) = 15$ and $L_n(3)$ has dimension 14 according to the following theorem that can be found in [2],

Theorem 7.1.1 (Alghamdi, Crabb and Hubbuck). $M_n(3)/L_n(3) = 0$ *unless* $n = 2^{s+3} + 2^{s+1} + 2^s - 3$ *for,* $s \geq 0$ *when* $L_n(3)$ *has dimension* 14, *while;* $M_n(3)$ *has dimension* 15.

Thus the minimal degree where the divergence between $M_n(3)$ and $L_n(3)$ is $n = 8$. In [2] the element $\theta = y_1z_1x_2y_2z_2 + x_1z_1(y_2z_4 + z_2y_4) + x_1y_1z_2z_4$ is elected to be the element that is in $M_8(3)$, but we can not see it in $L_8(3)$.

The picture is totally different when we look at the case where p is an odd prime. The space $M_n(k)/L_n(k)$ described in [6] as follows. When $k = 1$, $M_n(1) = L_n(1)$ and $M_n(1)/L_n(1) = 0$. While, the elements of $M_n(2)$ which are not in $L_n(2)$ are those in the image of the linear injection f in the higher degrees, in the degrees $p + 1 \leq n \leq p^2 + (i+1)p + j - 1$ are just $x_1^n y_1^m$ for some n, m multiplies by *Crossley* bracket C_{xy} or its power. For more details see [6].

7.2 The three variables case

In this case we will see a different pattern from what we have seen in the previous section, however; there are some similarities in some situations. Like in the case of two variables, the first non-zero dimension of $M_n(3)/L_n(3)$ occurs when $n = p+1$, with the *Crossley* brackets C_{xy}, C_{xz} and C_{yz} as basis elements, so dim $M_{p+1}/L_{p+1} = 3$ for an odd prime p. Similarly, according to the computer calculations the basis of M_n/L_n can be given as $x_1^i y_1^j z_1^k$ multiplies by C_{xy}, C_{xz} and C_{yz} or their powers such that $n < p^2+2p+2-3$.

On the other hand, for degree $n \geq p^2+2p+2-3$, M_n and L_n diverge further according as p is $3, 5, \cdots$, with elements we call them the **criminals**. When $n = p^2+2p+2-3$ and $p = 3$, then $n = 14$ we have $M_{14} = 16$ and $L_{14} = 15$, the following basis element can not be seen in L_{14}

$$\begin{aligned} D = & x_1 x_{p^2} y_1^2 z_1^2 + x_1^2 y_1 y_{p^2} z_1^2 + x_1^2 y_1^2 z_1 z_{p^2} + x_1 x_p y_1 y_p z_p^2 + x_1 x_p y_p^2 z_1 z_p + x_p^2 y_1 y_p z_1 z_p + \\ & x_1^2 y_p^2 z_p^2 + x_p^2 y_1^2 z_p^2 + x_p^2 y_p^2 z_1^2 + x_1^2 y_1 y_p z_1^2 z_p^2 + x_1^2 y_1^2 y_p^2 z_1 z_p + x_1^2 x_p^2 y_1^2 z_1 z_p. \end{aligned}$$

In the same degree form n, if $p = 5$, then $n = 34$, so we get dim $L_{34} = 90$ and dim $M_{34} = 96$, so dim $M_{34}/L_{34} = 6$. A choice for the basis elements which are just in M_{34} is the following:

$$\begin{aligned} 1) & x_1^3 x_{25} y_1^4 z_1^2 + x_5^4 y_1^2 y_5^2 z_1^2 + x_1 x_5^3 y_1 y_5^3 z_1^2 + x_1^2 x_5^2 y_5^4 z_1^2 + x_1^4 y_1^3 y_{25} z_1^2 + x_1^4 x_5^4 y_1^4 z_1 z_5 + 3x_5^4 y_1^3 y_5 z_1 z_5 + \\ & 3x_1 x_5^3 y_1^2 y_5^2 z_1 z_5 + 3x_1^2 x_5^2 y_1 y_5^3 z_1 z_5 + 3x_1^3 x_5 y_5^4 z_1 z_5 + x_1^4 y_1^4 y_5^4 z_1 z_5 + x_5^4 y_1^4 z_5^2 + x_1 x_5^3 y_1^3 y_5 z_5^2 + \\ & x_1^2 x_5^2 y_1^2 y_5^2 z_5^2 + x_1^3 x_5 y_1 y_5^3 z_5^2 + x_1^4 y_5^4 z_5^2 + x_1^4 y_1 y_5^3 z_1^4 z_5^2 - x_1^4 y_1^2 y_5^2 z_1^3 z_5^3 + 3x_1^4 y_1^3 y_5 z_1^2 z_5^4 + \\ & 3x_1^4 y_1^4 z_1 z_{25}, \end{aligned}$$

$$\begin{aligned} 2) & x_1^3 x_{25} y_1^3 z_1^3 + 3x_5^4 y_1 y_5^2 z_1^3 - x_1 x_5^3 y_5^3 z_1^3 + 2x_1^4 y_1^2 y_{25} z_1^3 + x_1^4 x_5^4 y_1^3 z_1^2 z_5 - x_5^4 y_1^2 y_5 z_1^2 z_5 + x_1 x_5^3 y_1 y_5^2 z_1^2 z_5 + \\ & 3x_1^2 x_5^2 y_5^3 z_1^2 z_5 + 2x_1^4 y_1^3 y_5^4 z_1^2 z_5 + 3x_5^4 y_1^3 z_1 z_5^2 + x_1 x_5^3 y_1^2 y_5 z_1 z_5^2 - x_1^2 x_5^2 y_1 y_5^2 z_1 z_5^2 + 2x_1^3 x_5 y_5^3 z_1 z_5^2 + \\ & x_1^4 y_1^4 y_5^3 z_1 z_5^2 - x_1 x_5^3 y_1^3 z_5^3 + 3x_1^2 x_5^2 y_1^2 y_5 z_5^3 + 2x_1^3 x_5 y_1 y_5^2 z_5^3 + x_1^4 y_5^3 z_5^3 + x_1^4 y_1 y_5^2 z_1^4 z_5^3 + \\ & 2x_1^4 y_1^2 y_5 z_1^3 z_5^4 + 2x_1^4 y_1^3 z_1^2 z_{25}, \end{aligned}$$

$$\begin{aligned} 3) & x_1^3 x_{25} y_1^2 z_1^4 + x_5^4 y_5^2 z_1^4 + 3x_1^4 y_1 y_{25} z_1^4 + x_1^4 x_5^4 y_1^2 z_1^3 z_5 + 3x_5^4 y_1 y_5 z_1^3 z_5 + x_1 x_5^3 y_5^2 z_1^3 z_5 + 3x_1^4 y_1^2 y_5^4 z_1^3 z_5 + \\ & x_5^4 y_1^2 z_1^2 z_5^2 + 3x_1 x_5^3 y_1 y_5 z_1^2 z_5^2 + x_1^2 x_5^2 y_5^2 z_1^2 z_5^2 - x_1^4 y_1^3 y_5^3 z_1^2 z_5^2 + x_1 x_5^3 y_1^2 z_1 z_5^3 + 3x_1^2 x_5^2 y_1 y_5 z_1 z_5^3 + \\ & x_1^3 x_5 y_5^2 z_1 z_5^3 + x_1^4 y_1^4 y_5^2 z_1 z_5^3 + x_1^2 x_5^2 y_1^2 z_5^4 + 3x_1^3 x_5 y_1 y_5 z_5^4 + x_1^4 y_5^2 z_5^4 + x_1^4 y_1 y_5 z_1^4 z_5^4 + x_1^4 y_1^2 z_1^3 z_{25}, \end{aligned}$$

$$\begin{aligned} 4) & x_1^2 x_{25} y_1^4 z_1^3 + 2x_5^3 y_1 y_5^3 z_1^3 - x_1 x_5^2 y_5^4 z_1^3 + 3x_1^3 y_1^3 y_{25} z_1^3 + x_1^3 x_5^4 y_1^4 z_1^2 z_5 - x_5^3 y_1^2 y_5^2 z_1^2 z_5 + 3x_1 x_5^2 y_1 y_5^3 z_1^2 z_5 + \\ & 2x_1^2 x_5 y_5^4 z_1^2 z_5 + 3x_1^3 y_1^4 y_5^4 z_1^2 z_5 + 3x_1^4 x_5^3 y_1^4 z_1 z_5^2 + x_5^3 y_1^3 y_5 z_1 z_5^2 + 2x_1 x_5^2 y_1^2 y_5^2 z_1 z_5^2 + 3x_1^2 x_5 y_1 y_5^3 z_1 z_5^2 - \\ & x_1^3 y_5^4 z_1 z_5^2 + 3x_5^3 y_1^4 z_5^3 + x_1 x_5^2 y_1^3 y_5 z_5^3 - x_1^2 x_5 y_1^2 y_5^2 z_5^3 + 2x_1^3 y_1 y_5^3 z_5^3 + 3x_1^3 y_1^2 y_5^2 z_1^4 z_5^3 + \\ & x_1^3 y_1^3 y_5 z_1^3 z_5^4 + x_1^3 y_1^4 z_1^2 z_{25}, \end{aligned}$$

$$\begin{aligned} 5) & x_1^2 x_{25} y_1^3 z_1^4 + 3x_5^3 y_5^3 z_1^4 + x_1^3 y_1^2 y_{25} z_1^4 + x_1^3 x_5^4 y_1^3 z_1^3 z_5 + x_5^3 y_1 y_5^2 z_1^3 z_5 + x_1 x_5^2 y_5^3 z_1^3 z_5 + x_1^3 y_1^3 y_5^4 z_1^3 z_5 + \\ & 3x_1^4 x_5^3 y_1^3 z_1^2 z_5^2 - x_5^3 y_1^2 y_5 z_1^2 z_5^2 + 2x_1 x_5^2 y_1 y_5^2 z_1^2 z_5^2 - x_1^2 x_5 y_5^3 z_1^2 z_5^2 + 3x_1^3 y_1^4 y_5^3 z_1^2 z_5^2 + 2x_5^3 y_1^3 z_1 z_5^3 + \\ & 3x_1 x_5^2 y_1^2 y_5 z_1 z_5^3 + 3x_1^2 x_5 y_1 y_5^2 z_1 z_5^3 + 2x_1^3 y_5^3 z_1 z_5^3 - x_1 x_5^2 y_1^3 z_5^4 + 2x_1^2 x_5 y_1^2 y_5 z_5^4 - x_1^3 y_1 y_5^2 z_5^4 + \\ & 3x_1^3 y_1^2 y_5 z_1^4 z_5^4 + 3x_1^3 y_1^3 z_1^3 z_{25}, \end{aligned}$$

$$\begin{aligned} 6) & x_1 x_{25} y_1^4 z_1^4 + 2x_5^2 y_5^4 z_1^4 + 2x_1^2 y_1^3 y_{25} z_1^4 + x_1^2 x_5^4 y_1^4 z_1^3 z_5 + 2x_5^2 y_1 y_5^3 z_1^3 z_5 + x_1 x_5 y_5^4 z_1^3 z_5 + 2x_1^2 y_1^4 y_5^4 z_1^3 z_5 + \\ & 3x_1^3 x_5^3 y_1^4 z_1^2 z_5^2 + 2x_5^2 y_1^2 y_5^2 z_1^2 z_5^2 + x_1 x_5 y_1 y_5^3 z_1^2 z_5^2 + 2x_1^2 y_5^4 z_1^2 z_5^2 + 2x_1^4 x_5^2 y_1^4 z_1 z_5^3 + 2x_5^2 y_1^3 y_5 z_1 z_5^3 + \\ & x_1 x_5 y_1^2 y_5^2 z_1 z_5^3 + 2x_1^2 y_1 y_5^3 z_1 z_5^3 + 2x_5^2 y_1^4 z_5^4 + x_1 x_5 y_1^3 y_5 z_5^4 + 2x_1^2 y_1^2 y_5^2 z_5^4 + 2x_1^2 y_1^3 y_5 z_1^4 z_5^4 + \\ & 2x_1^2 y_1^4 z_1^3 z_{25}. \end{aligned}$$

and so on for any odd prime dim $M_{p^2+2p+2-3}(3)/L_{p^2+2p+2-3}(3) = \frac{(p-1)(p-2)}{2}$.

The similarities between the criminals D and θ where $p=3$ and $p=2$ respectively are both the only elements in M_n/L_n, and they are non-symmetric elements, unlike; *Crossley* brackets. That is, there are another versions of those elements can be chosen to be the basis elements for M_n/L_n. For example, we can chose $\hat{\theta} = x_1y_1x_2y_2z_2 + x_1z_1(x_2y_4+y_2x_4)+ y_1z_1x_2x_4$ or $\bar{\theta} = y_1z_1x_2y_2z_2 + x_1y_1(y_2z_4+z_2y_4)+x_1z_1y_2y_4$ instead of θ. While, D could be replaced by

$$\begin{aligned}\hat{D} =& x_1x_{p^2}y_1^2z_1^2 + x_1^2y_1y_{p^2}z_1^2 + x_1^2y_1^2z_1z_{p^2} + x_1x_py_1y_pz_p^2 + x_1x_py_p^2z_1z_p + x_p^2y_1y_pz_1z_p+\\ & x_1^2y_p^2z_p^2 + x_p^2y_1^2z_p^2 + x_p^2y_p^2z_1^2 + x_1^2x_p^2y_1y_pz_1^2 + x_1x_py_1^2y_p^2z_1^2 + x_1x_py_1^2z_1^2z_p^2,\end{aligned}$$

or by

$$\begin{aligned}\bar{D} =& x_1x_{p^2}y_1^2z_1^2 + x_1^2y_1y_{p^2}z_1^2 + x_1^2y_1^2z_1z_{p^2} + x_1x_py_1y_pz_p^2 + x_1x_py_p^2z_1z_p + x_p^2y_1y_pz_1z_p+\\ & x_1^2y_p^2z_p^2 + x_p^2y_1^2z_p^2 + x_p^2y_p^2z_1^2 + x_1x_py_1^2z_1^2z_p^2 + x_1^2x_p^2y_1^2z_1z_p + x_1^2y_1^2y_p^2z_1z_p.\end{aligned}$$

Turning to $n=15$ and $p=3$, in this case we see a new pattern that is not in any of the previous cases. From [1] where $p=2$ in some degrees $M_n(3)$ could be calculated by $M_n = L_n \oplus f(M_{(n-3)/2})$, but in this degree $M_{15} = f(M_3) \oplus M_{15}/L_{15}$ where $L_{15} = f(M_3)$ which has dimension 7 and with basis elements given by $\{x_1^2x_p^iy_1^2y_p^jz_1^2z_p^k | i+j+k=p, 0 \leq i,j,k \leq p-1\}$. Whilst the criminals are the following linearly independent elements:

1) $x_1^2y_1^2z_1^2z_{p^2} - (x_1y_p - y_1x_p)z_1z_p^2 + (x_1x_py_p^2 + x_p^2y_1y_p)z_1^2z_p$.

2) $x_1^2z_1^2y_1^2y_{p^2} - (x_1z_p - z_1x_p)y_1y_p^2 + (x_1x_pz_p^2 + x_p^2z_1z_p)y_1^2y_p$.

3) $y_1^2z_1^2x_1^2x_{p^2} - (y_1z_p - z_1y_p)x_1x_p^2 + (y_1y_pz_p^2 + y_p^2z_1z_p)x_1^2x_p$.

4) $(x_1y_p - y_1x_p)z_1^2z_{p^2} + \{(x_1x_p^2y_1 + x_1^2x_py_p) - (x_py_1^2y_p + x_1y_1y_p^2)\}z_1z_p^2 - (x_1y_{p^2} - x_py_1y_p^2 + x_1x_p^2y_p - y_1x_{p^2})z_1^2z_p$.

5) $(x_1z_p - z_1x_p)y_1^2y_{p^2} + \{(x_1x_p^2z_1 + x_1^2x_pz_p) - (x_pz_1^2z_p + x_1z_1z_p^2)\}y_1y_p^2 - (x_1z_{p^2} - x_pz_1z_p^2 + x_1x_p^2z_p - z_1x_{p^2})y_1^2y_p$.

6) $(y_1z_p - z_1y_p)x_1^2x_{p^2} + \{(y_1y_p^2z_1 + y_1^2y_pz_p) - (y_pz_1^2z_p + y_1z_1z_p^2)\}x_1x_p^2 - (y_1z_{p^2} - y_pz_1z_p^2 + y_1y_p^2z_p - z_1y_{p^2})x_1^2x_p$.

7) $x_1y_1(x_1y_p - y_1x_p)z_{p^2} - (x_1^2y_p^2 - x_p^2y_1^2)z_1z_p^2 - (x_1x_py_p^2 - x_p^2y_1y_p)z_1^2z_p - (x_1^2y_1y_{p^2} + x_1x_py_1^2y_p^2 - x_1^2x_p^2y_1y_p - x_1x_{p^2}y_1^2)z_p + (x_1x_py_1y_{p^2} + x_p^2y_1^2y_p^2 - x_1^2x_p^2y_p^2 - x_1x_{p^2}y_1y_p)z_1$.

8) $x_1z_1(x_1z_p - z_1x_p)y_{p^2} - (x_1^2z_p^2 - x_p^2z_1^2)y_1y_p^2 - (x_1x_pz_p^2 - x_p^2z_1z_p)y_1^2y_p - (x_1^2z_1z_{p^2} + x_1x_pz_1^2z_p^2 - x_1^2x_p^2z_1z_p - x_1x_{p^2}z_1^2)y_p + (x_1x_pz_1z_{p^2} + x_p^2z_1^2z_p^2 - x_1^2x_p^2z_p^2 - x_1x_{p^2}z_1z_p)y_1$.

9) $y_1z_1(y_1z_p - z_1y_p)x_{p^2} - (y_1^2z_p^2 - y_p^2z_1^2)x_1x_p^2 - (y_1y_pz_p^2 - y_p^2z_1z_p)x_1^2x_p - (y_1^2z_1z_{p^2} + y_1y_pz_1^2z_p^2 - y_1^2y_p^2z_1z_p - y_1y_{p^2}z_1^2)x_p + (y_1y_pz_1z_{p^2} + y_p^2z_1^2z_p^2 - y_1^2y_p^2z_p^2 - y_1y_{p^2}z_1z_p)x_1$.

Although the previous list of elements show that how $M_*(3)$ in the higher degrees looks complicated, they are very nice example to see the prospective formula of those elements according to lemma 5.2.8 point of view.

The same situation can be seen in degrees of the form $n = ap^s + 2p - 3$ where L_n calculates from the product of three generators, applying lemma 6.2.2 implies that each element in L_n has to be in the image of f. While, dim $M_n(3) =$ dim $f(M_{ap^{s-1}+2-3}) + 13$, see appendix A.

Finally, in [8] *Crossley* had a conjecture to determine the upper bound of dimensions of $M_*(k)$[1] which is

Conjecture 7.2.1 (Crossley). *A set of generators for $P(k)$ as a module over $\mathcal{A}(p)$ can be chosen with at most*

$$\prod_{i=1}^{k}(2p^{i-1} - 1)$$

members in each degree.

According to the appendices A and B this conjecture is true for $M_*(3)$, and it seems to be in a higher degrees the dimensions of $M_*(3)$ become more stable than what it was in the lower degrees.

[1] In fact the conjecture is to determine the maximum number of generators that we need for the polynomial algebra in k-variables over a field $\mathbb{F}_p$ as a module over *Steenrod algebra* $A(p)$.

Appendices

Appendix A

Tables of computer calculations for $p = 3$

In this appendix we list the dimensions of the spaces $M_n(3)$, $L_n(3)$ and $M_n(3)/L_n(3)$ for $p = 3$ that are gotten via computer calculations the code is written by Mathematica program (the code is given in appendix C). I would like to thank Dr. *Crossley* for his help to write this code.

Table A.1: *Dimensions of* $M_n(3)$, $L_n(3)$ and $M_n(3)/L_n(3)$ where $1 \leq n \leq 21$

Deg n	$n = ap^\alpha + bp^\beta + cp^\gamma - 3$	**Dim** $M_n(3)$	**Dim** $L_n(3)$	$M_n(3)/L_n(3)$
$n = 1$	$1 = p + 1 - 3$	3	3	0
$n = 2$	$2 = p + 2 - 3$	6	6	0
$n = 3$	$3 = 2p - 3$	7	7	0
$n = 4$	$4 = 2p + 1 - 3$	9	6	3
$n = 5$	$5 = 2p + 2 - 3$	14	13	1
$n = 6$	$6 = p^2 - 3$	16	16	0
$n = 7$	$7 = p^2 + 1 - 3$	15	15	0
$n = 8$	$8 = p^2 + 2 - 3$	23	17	6
$n = 9$	$9 = p^2 + p - 3$	27	26	1
$n = 10$	$10 = p^2 + p + 1 - 3$	27	27	0
$n = 11$	$11 = p^2 + p + 2 - 3$	15	15	0
$n = 12$	$12 = p^2 + 2p - 3$	19	6	13
$n = 13$	$13 = p^2 + 2p + 1 - 3$	24	23	1
$n = 14$	$14 = p^2 + 2p + 2 - 3$	16	15	1
$n = 15$	$15 = 2p^2 - 3$	$16 = f(Deg(3)) + 9$	7	9
$n = 16$	$16 = 2p^2 + 1 - 3$	25	12	13
$n = 17$	$17 = 2p^2 + 2 - 3$	30	20	10
$n = 18$	$18 = 2p^2 + p - 3$	$35 = f(Deg(4)) + 26$	29	6
$n = 19$	$19 = 2p^2 + p + 1 - 3$	42	39	3
$n = 20$	$20 = 2p^2 + p + 2 - 3$	27	26	1
$n = 21$	$21 = 2p^2 + 2p - 3$	$26 = f(Deg(5)) + 12$	13	13

Table A.2: *Dimensions of* $M_n(3)$, $L_n(3)$ and $M_n(3)/L_n(3)$ where $22 \leq n \leq 61$

Deg n	$n = ap^\alpha + bp^\beta + cp^\gamma - 3$	**Dim** $M_n(3)$	**Dim** $L_n(3)$	$M_n(3)/L_n(3)$
$n = 22$	$22 = 2p^2 + 2p + 1 - 3$	39	39	0
$n = 23$	$23 = 2p^2 + 2p + 2 - 3$	27	27	0
$n = 24$	$24 = p^3 - 3$	$16 = f(Deg(6))$	16	0
$n = 25$	$25 = p^3 + 1 - 3$	32	26	6
$n = 26$	$26 = p^3 + 2 - 3$	36	36	0
$n = 27$	$27 = p^3 + p - 3$	$42 = f(Deg(7)) + 27$	41	1
$n = 28$	$28 = p^3 + p + 1 - 3$	60	39	21
$n = 29$	$29 = p^3 + p + 2 - 3$	41	26	15
$n = 30$	$30 = p^3 + 2p - 3$	$36 = f(Deg(8)) + 13$	17	19
$n = 31$	$31 = p^3 + 2p + 1 - 3$	58	52	6
$n = 32$	$32 = p^3 + 2p + 2 - 3$	42	39	3
$n = 33$	$33 = p^3 + p^2 - 3$	$27 = f(Deg(9))$	26	1
$n = 34$	$34 = p^3 + p^2 + 1 - 3$	52	39	13
$n = 35$	$35 = p^3 + p^2 + 2 - 3$	39	39	0
$n = 36$	$36 = p^3 + p^2 + p - 3$	$27 = f(Deg(10))$	27	0
$n = 37$	$37 = p^3 + p^2 + p + 1 - 3$	0	0	0
$n = 38$	$38 = p^3 + p^2 + p + 2 - 3$	10	0	10
$n = 39$	$39 = p^3 + p^2 + 2p - 3$	$16 = f(Deg(11)) + 1$	15	1
$n = 40$	$40 = p^3 + p^2 + 2p + 1 - 3$	14	0	14
$n = 41$	$41 = p^3 + p^2 + 2p + 2 - 3$	15	0	15
$n = 42$	$42 = p^3 + 2p^2 - 3$	$19 = f(Deg(12))$	6	13
$n = 43$	$43 = p^3 + 2p^2 + 1 - 3$	33	26	7
$n = 44$	$44 = p^3 + 2p^2 + 2 - 3$	29	26	3
$n = 45$	$45 = p^3 + 2p^2 + p - 3$	$24 = f(Deg(13))$	23	1
$n = 46$	$46 = p^3 + 2p^2 + p + 1 - 3$	0	0	0
$n = 47$	$47 = p^3 + 2p^2 + p + 2 - 3$	6	0	6
$n = 48$	$48 = p^3 + 2p^2 + 2p - 3$	$16 = f(Deg(14))$	15	1
$n = 49$	$49 = p^3 + 2p^2 + 2p + 1 - 3$	0	0	0
$n = 50$	$50 = p^3 + 2p^2 + 2p + 2 - 3$	0	0	0
$n = 51$	$51 = 2p^3 - 3$	$16 = f(Deg(15))$	7	9
$n = 52$	$52 = 2p^3 + 1 - 3$	26	13	13
$n = 53$	$53 = 2p^3 + 2 - 3$	39		
$n = 54$	$54 = 2p^3 + p - 3$	$51 = f(Deg(16)) + 26$		
$n = 55$	$55 = 2p^3 + p + 1 - 3$	39		
$n = 56$	$56 = 2p^3 + p + 2 - 3$	29	26	3
$n = 57$	$57 = 2p^3 + 2p - 3$	$43 = f(Deg(17)) + 13$		
$n = 58$	$58 = 2p^3 + 2p + 1 - 3$	52	52	0
$n = 59$	$59 = 2p^3 + 2p + 2 - 3$	39	39	0
$n = 60$	$60 = 2p^3 + p^2 - 3$	$35 = f(Deg(18))$	29	6
$n = 61$	$61 = 2p^3 + p^2 + 1 - 3$	65	52	13

Table A.3: *Dimensions of* $M_n(3)$, $L_n(3)$ and $M_n(3)/L_n(3)$ where $62 \le n \le 102$

Deg n	$n = ap^\alpha + bp^\beta + cp^\gamma - 3$	**Dim** $M_n(3)$	**Dim** $L_n(3)$	$M_n(3)/L_n(3)$
$n = 62$	$62 = 2p^3 + p^2 + 2 - 3$	52	52	0
$n = 63$	$63 = 2p^3 + p^2 + p - 3$	$42 = f(Deg(19))$	39	3
$n = 64$	$64 = 2p^3 + p^2 + p + 1 - 3$	0	0	0
$n = 65$	$65 = 2p^3 + p^2 + p + 2 - 3$	13	0	13
$n = 66$	$66 = 2p^3 + p^2 + 2p - 3$	$27 = f(Deg(20))$	26	1
$n = 67$	$67 = 2p^3 + p^2 + 2p + 1 - 3$	0	0	0
$n = 68$	$68 = 2p^3 + p^2 + 2p + 2 - 3$	0	0	0
$n = 69$	$69 = 2p^3 + 2p^2 - 3$	$26 = f(Deg(21))$	13	13
$n = 70$	$70 = 2p^3 + 2p^2 + 1 - 3$	39	39	0
$n = 71$	$71 = 2p^3 + 2p^2 + 2 - 3$	39	39	0
$n = 72$	$72 = 2p^3 + 2p^2 + p - 3$	$39 = f(Deg(22))$	39	0
$n = 73$	$73 = 2p^3 + 2p^2 + p + 1 - 3$	0	0	0
$n = 74$	$74 = 2p^3 + 2p^2 + p + 2 - 3$	0	0	0
$n = 75$	$75 = 2p^3 + 2p^2 + 2p - 3$	$27 = f(Deg(23))$	27	0
$n = 76$	$76 = 2p^3 + 2p^2 + 2p + 1 - 3$	0	0	0
$n = 77$	$77 = 2p^3 + 2p^2 + 2p + 2 - 3$	0	0	0
$n = 78$	$78 = p^4 - 3$	$16 = f(Deg(24))$	16	0
$n = 79$	$79 = p^4 + 1 - 3$	26	26	0
$n = 80$	$80 = p^4 + 2 - 3$	39		
$n = 81$	$81 = p^4 + p - 3$	$58 = f(Deg(25)) + 26$		
$n = 82$	$82 = p^4 + p + 1 - 3$	39	39	0
$n = 83$	$83 = p^4 + p + 2 - 3$	26	26	0
$n = 84$	$84 = p^4 + 2p - 3$	$49 = f(Deg(26)) + 13$		
$n = 85$	$85 = p^4 + 2p + 1 - 3$	52	52	0
$n = 86$	$86 = p^4 + 2p + 2 - 3$	39	39	0
$n = 87$	$87 = p^4 + p^2 - 3$	$42 = f(Deg(27))$	41	1
$n = 88$	$88 = p^4 + p^2 + 1 - 3$	78	52	26
$n = 89$	$89 = p^4 + p^2 + 2 - 3$	65	52	13
$n = 90$	$90 = p^4 + p^2 + p - 3$	$60 = f(Deg(28))$	39	21
$n = 91$	$91 = p^4 + p^2 + p + 1 - 3$	0	0	0
$n = 92$	$92 = p^4 + p^2 + p + 2 - 3$	13	0	13
$n = 93$	$93 = p^4 + p^2 + 2p - 3$	$41 = f(Deg(29))$	26	15
$n = 94$	$94 = p^4 + p^2 + 2p + 1 - 3$	0	0	0
$n = 95$	$95 = p^4 + p^2 + 2p + 2 - 3$	0	0	0
$n = 96$	$96 = p^4 + 2p^2 - 3$	$36 = f(Deg(30))$	17	19
$n = 97$	$97 = p^4 + 2p^2 + 1 - 3$	52		
$n = 98$	$98 = p^4 + 2p^2 + 2 - 3$	52		
$n = 99$	$99 = p^4 + 2p^2 + p - 3$	$58 = f(Deg(31))$	52	6
$n = 100$	$100 = p^4 + 2p^2 + p + 1 - 3$	0	0	0
$n = 101$	$101 = p^4 + 2p^2 + p + 2 - 3$	0	0	0
$n = 102$	$102 = p^4 + 2p^2 + 2p - 3$	$42 = f(Deg(32))$	39	3

Table A.4: *Dimensions of* $M_n(3)$, $L_n(3)$ and $M_n(3)/L_n(3)$ where $103 \leq n \leq 141$

$Deg \quad n$	$n = ap^\alpha + bp^\beta + cp^\gamma - 3$	**Dim** $M_n(3)$	**Dim** $L_n(3)$	$M_n(3)/L_n(3)$
$n = 103$	$103 = p^4 + 2p^2 + 2p + 1 - 3$	0	0	0
$n = 104$	$104 = p^4 + 2p^2 + 2p + 2 - 3$	0	0	0
$n = 105$	$105 = p^4 + p^3 - 3$	$27 = f(Deg(33))$	26	1
$n = 106$	$106 = p^4 + p^3 + 1 - 3$	39		
$n = 107$	$107 = p^4 + p^3 + 2 - 3$	39		
$n = 108$	$108 = p^4 + p^3 + p - 3$	$52 = f(Deg(34))$	39	13
$n = 109$	$109 = p^4 + p^3 + p + 1 - 3$	0	0	0
$n = 110$	$110 = p^4 + p^3 + p + 2 - 3$	0	0	0
$n = 111$	$111 = p^4 + p^3 + 2p - 3$	$39 = f(Deg(35))$	39	0
$n = 112$	$112 = p^4 + p^3 + 2p + 1 - 3$	0	0	0
$n = 113$	$113 = p^4 + p^3 + 2p + 2 - 3$	0	0	0
$n = 114$	$114 = p^4 + p^3 + p^2 - 3$	$27 = f(Deg(36))$	27	0
$n = 115$	$115 = p^4 + p^3 + p^2 + 1 - 3$	0	0	0
$n = 116$	$116 = p^4 + p^3 + p^2 + 2 - 3$	0	0	0
$n = 117$	$117 = p^4 + p^3 + p^2 + p - 3$	$0 = f(Deg(37))$	0	0
$n = 118$	$118 = p^4 + p^3 + p^2 + p + 1 - 3$	0	0	0
$n = 119$	$119 = p^4 + p^3 + p^2 + p + 2 - 3$	0	0	0
$n = 120$	$120 = p^4 + p^3 + p^2 + 2p - 3$	$10 = f(Deg(38))$	0	10
$n = 121$	$121 = p^4 + p^3 + p^2 + 2p + 1 - 3$	0	0	0
$n = 122$	$122 = p^4 + p^3 + p^2 + 2p + 2 - 3$	0	0	0
$n = 123$	$123 = p^4 + p^3 + 2p^2 - 3$	$16 = f(Deg(39))$	15	1
$n = 124$	$124 = p^4 + p^3 + 2p^2 + 1 - 3$	13	0	13
$n = 125$	$125 = p^4 + p^3 + 2p^2 + 2 - 3$	13	0	13
$n = 126$	$126 = p^4 + p^3 + 2p^2 + p - 3$	$14 = f(Deg(40))$	0	14
$n = 127$	$127 = p^4 + p^3 + 2p^2 + p + 1 - 3$	0	0	0
$n = 128$	$128 = p^4 + p^3 + 2p^2 + p + 2 - 3$	0	0	0
$n = 129$	$129 = p^4 + p^3 + 2p^2 + 2p - 3$	$15 = f(Deg(41))$	0	15
$n = 130$	$130 = p^4 + p^3 + 2p^2 + 2p + 1 - 3$	0	0	0
$n = 131$	$131 = p^4 + p^3 + 2p^2 + 2p + 2 - 3$	0	0	0
$n = 132$	$132 = p^4 + 2p^3 - 3$	$19 = f(Deg(42))$	6	
$n = 133$	$133 = p^4 + 2p^3 + 1 - 3$	26		
$n = 134$	$134 = p^4 + 2p^3 + 2 - 3$	26		
$n = 135$	$135 = p^4 + 2p^3 + p - 3$	$33 = f(Deg(43))$		
$n = 136$	$136 = p^4 + 2p^3 + p + 1 - 3$	0		
$n = 137$	$137 = p^4 + 2p^3 + p + 2 - 3$	0		
$n = 138$	$138 = p^4 + 2p^3 + 2p - 3$	$29 = f(Deg(44))$		
$n = 139$	$139 = p^4 + 2p^3 + 2p + 1 - 3$	0		
$n = 140$	$140 = p^4 + 2p^3 + 2p + 2 - 3$	0		
$n = 141$	$141 = p^4 + 2p^3 + p^2 - 3$	$24 = f(Deg(45))$		

Table A.5: *Dimensions of* $M_n(3)$, $L_n(3)$ and $M_n(3)/L_n(3)$ where $142 \leq n \leq 160$

Deg n	$n = ap^\alpha + bp^\beta + cp^\gamma - 3$	**Dim** $M_n(3)$	**Dim** $L_n(3)$	$M_n(3)/L_n(3)$
$n = 142$	$142 = p^4 + 2p^3 + p^2 + 1 - 3$	0		
$n = 143$	$143 = p^4 + 2p^3 + p^2 + 2 - 3$	0		
$n = 144$	$144 = p^4 + 2p^3 + p^2 + p - 3$	$0 = f(Deg(46))$		
$n = 145$	$145 = p^4 + 2p^3 + p^2 + p + 1 - 3$	0		
$n = 146$	$146 = p^4 + 2p^3 + p^2 + p + 2 - 3$	0		
$n = 147$	$147 = p^4 + 2p^3 + p^2 + 2p - 3$	$6 = f(Deg(47))$		
$n = 148$	$148 = p^4 + 2p^3 + p^2 + 2p + 1 - 3$	0		
$n = 149$	$149 = p^4 + 2p^3 + p^2 + 2p + 2 - 3$	0		
$n = 150$	$150 = p^4 + 2p^3 + 2p^2 - 3$	$16 = f(Deg(48))$		
$n = 151$	$151 = p^4 + 2p^3 + 2p^2 + 1 - 3$			
$n = 152$	$152 = p^4 + 2p^3 + 2p^2 + 2 - 3$			
$n = 153$	$153 = p^4 + 2p^3 + 2p^2 + p - 3$	$0 = f(Deg(49))$		
$n = 154$	$154 = p^4 + 2p^3 + 2p^2 + p + 1 - 3$			
$n = 155$	$155 = p^4 + 2p^3 + 2p^2 + p + 2 - 3$			
$n = 156$	$156 = p^4 + 2p^3 + 2p^2 + 2p - 3$	$0 = f(Deg(50))$		
$n = 157$	$157 = p^4 + 2p^3 + 2p^2 + 2p + 1 - 3$			
$n = 158$	$158 = p^4 + 2p^3 + 2p^2 + 2p + 2 - 3$			
$n = 159$	$159 = 2p^4 - 3$	$16 = f(Deg(51))$		
$n = 160$	$160 = 2p^4 + 1 - 3$			

Appendix B

Tables of computer calculations for $p = 5$

The following tables are for $p = 5$

Table B.1: *Dimensions of* $M_n(3)$ where $1 \leq n \leq 21$

Deg n	$n = ap^\alpha + bp^\beta + cp^\gamma - 3$	**Dim** $M_n(3)$
$n = 1$	$1 = 4 - 3$	3
$n = 2$	$2 = p - 3$	6
$n = 3$	$3 = p + 1 - 3$	10
$n = 4$	$4 = p + 2 - 3$	15
$n = 5$	$5 = p + 3 - 3$	18
$n = 6$	$6 = p + 4 - 3$	22
$n = 7$	$7 = 2p - 3$	26
$n = 8$	$8 = 2p + 1 - 3$	30
$n = 9$	$9 = 2p + 2 - 3$	37
$n = 10$	$10 = 2p + 3 - 3$	41
$n = 11$	$11 = 2p + 4 - 3$	42
$n = 12$	$12 = 3p - 3$	46
$n = 13$	$13 = 3p + 1 - 3$	50
$n = 14$	$14 = 3p + 2 - 3$	60
$n = 15$	$15 = 3p + 3 - 3$	66
$n = 16$	$16 = 3p + 4 - 3$	68
$n = 17$	$17 = 4p - 3$	66
$n = 18$	$18 = 4p + 1 - 3$	70
$n = 19$	$19 = 4p + 2 - 3$	84
$n = 20$	$20 = 4p + 3 - 3$	93
$n = 21$	$21 = 4p + 4 - 3$	97

Table B.2: *Dimensions of* $M_n(3)$ where $22 \leq n \leq 61$

Deg n	$n = ap^\alpha + bp^\beta + cp^\gamma - 3$	**Dim** $M_n(3)$
$n = 22$	$22 = p^2 - 3$	96
$n = 23$	$23 = p^2 + 1 - 3$	90
$n = 24$	$24 = p^2 + 2 - 3$	109
$n = 25$	$25 = p^2 + 3 - 3$	122
$n = 26$	$26 = p^2 + 4 - 3$	129
$n = 27$	$27 = p^2 + p - 3$	130
$n = 28$	$28 = p^2 + p + 1 - 3$	125
$n = 29$	$29 = p^2 + p + 2 - 3$	90
$n = 30$	$30 = p^2 + p + 3 - 3$	99
$n = 31$	$31 = p^2 + p + 4 - 3$	107
$n = 32$	$32 = p^2 + 2p - 3$	114
$n = 33$	$33 = p^2 + 2p + 1 - 3$	120
$n = 34$	$34 = p^2 + 2p + 2 - 3$	96
$n = 35$	$35 = p^2 + 2p + 3 - 3$	93
$n = 36$	$36 = p^2 + 2p + 4 - 3$	102
$n = 37$	$37 = p^2 + 3p - 3$	112
$n = 38$	$38 = p^2 + 3p + 1 - 3$	126
$n = 39$	$39 = p^2 + 3p + 2 - 3$	100
$n = 40$	$40 = p^2 + 3p + 3 - 3$	96
$n = 41$	$41 = p^2 + 3p + 4 - 3$	95
$n = 42$	$42 = p^2 + 4p - 3$	106
$n = 43$	$43 = p^2 + 4p + 1 - 3$	128
$n = 44$	$44 = p^2 + 4p + 2 - 3$	102
$n = 45$	$45 = p^2 + 4p + 3 - 3$	97
$n = 46$	$46 = p^2 + 4p + 4 - 3$	96
$n = 47$	$47 = 2p^2 - 3$	96
$n = 48$	$48 = 2p^2 + 1 - 3$	126
$n = 49$	$49 = 2p^2 + 2 - 3$	133
$n = 50$	$50 = 2p^2 + 3 - 3$	140
$n = 51$	$51 = 2p^2 + 4 - 3$	147
$n = 52$	$52 = 2p^2 + p - 3$	154
$n = 53$	$53 = 2p^2 + p + 1 - 3$	165
$n = 54$	$54 = 2p^2 + p + 2 - 3$	130
$n = 55$	$55 = 2p^2 + p + 3 - 3$	127
$n = 56$	$56 = 2p^2 + p + 4 - 3$	125
$n = 57$	$57 = 2p^2 + 2p - 3$	124
$n = 58$	$58 = 2p^2 + 2p + 1 - 3$	155
$n = 59$	$59 = 2p^2 + 2p + 2 - 3$	125
$n = 60$	$60 = 2p^2 + 2p + 3 - 3$	96
$n = 61$	$61 = 2p^2 + 2p + 4 - 3$	96

Table B.3: *Dimensions of* $M_n(3)$ where $62 \leq n \leq 102$

Deg n	$n = ap^\alpha + bp^\beta + cp^\gamma - 3$	**Dim** $M_n(3)$
$n = 62$	$62 = 2p^2 + 3p - 3$	96
$n = 63$	$63 = 2p^2 + 3p + 1 - 3$	139
$n = 64$	$64 = 2p^2 + 3p + 2 - 3$	114
$n = 65$	$65 = 2p^2 + 3p + 3 - 3$	96
$n = 66$	$66 = 2p^2 + 3p + 4 - 3$	96
$n = 67$	$67 = 2p^2 + 4p - 3$	96
$n = 68$	$68 = 2p^2 + 4p + 1 - 3$	142
$n = 69$	$69 = 2p^2 + 4p + 2 - 3$	118
$n = 70$	$70 = 2p^2 + 4p + 3 - 3$	97
$n = 71$	$71 = 2p^2 + 4p + 4 - 3$	96
$n = 72$	$72 = 3p^2 - 3$	96
$n = 73$	$73 = 3p^2 + 1 - 3$	146
$n = 74$	$74 = 3p^2 + 2 - 3$	153
$n = 75$	$75 = 3p^2 + 3 - 3$	161
$n = 76$	$76 = 3p^2 + 4 - 3$	170
$n = 77$	$77 = 3p^2 + p - 3$	180
$n = 78$	$78 = 3p^2 + p + 1 - 3$	210
$n = 79$	$79 = 3p^2 + p + 2 - 3$	169
$n = 80$	$80 = 3p^2 + p + 3 - 3$	160
$n = 81$	$81 = 3p^2 + p + 4 - 3$	155
$n = 82$	$82 = 3p^2 + 2p - 3$	153
$n = 83$	$83 = 3p^2 + 2p + 1 - 3$	201
$n = 84$	$84 = 3p^2 + 2p + 2 - 3$	165
$n = 85$	$85 = 3p^2 + 2p + 3 - 3$	130
$n = 86$	$86 = 3p^2 + 2p + 4 - 3$	127
$n = 87$	$87 = 3p^2 + 3p - 3$	125
$n = 88$	$88 = 3p^2 + 3p + 1 - 3$	186
$n = 89$	$89 = 3p^2 + 3p + 2 - 3$	155
$n = 90$	$90 = 3p^2 + 3p + 3 - 3$	125
$n = 91$	$91 = 3p^2 + 3p + 4 - 3$	96
$n = 92$	$92 = 3p^2 + 4p - 3$	96
$n = 93$	$93 = 3p^2 + 4p + 1 - 3$	165
$n = 94$	$94 = 3p^2 + 4p + 2 - 3$	139
$n = 95$	$95 = 3p^2 + 4p + 3 - 3$	114
$n = 96$	$96 = 3p^2 + 4p + 4 - 3$	96
$n = 97$	$97 = 4p^2 - 3$	96
$n = 98$	$98 = 4p^2 + 1 - 3$	166
$n = 99$	$99 = 4p^2 + 2 - 3$	173
$n = 100$	$100 = 4p^2 + 3 - 3$	180
$n = 101$	$101 = 4p^2 + 4 - 3$	190
$n = 102$	$102 = 4p^2 + p - 3$	202

Table B.4: *Dimensions of* $M_n(3)$ where $103 \le n \le 141$

Deg n	$n = ap^\alpha + bp^\beta + cp^\gamma - 3$	**Dim** $M_n(3)$
$n = 103$	$103 = 4p^2 + p + 1 - 3$	260
$n = 104$	$104 = 4p^2 + p + 2 - 3$	213
$n = 105$	$105 = 4p^2 + p + 3 - 3$	198
$n = 106$	$106 = 4p^2 + p + 4 - 3$	185
$n = 107$	$107 = 4p^2 + 2p - 3$	180
$n = 108$	$108 = 4p^2 + 2p + 1 - 3$	252
$n = 109$	$109 = 4p^2 + 2p + 2 - 3$	210
$n = 110$	$110 = 4p^2 + 2p + 3 - 3$	169
$n = 111$	$111 = 4p^2 + 2p + 4 - 3$	160
$n = 112$	$112 = 4p^2 + 3p - 3$	155
$n = 113$	$113 = 4p^2 + 3p + 1 - 3$	238
$n = 114$	$114 = 4p^2 + 3p + 2 - 3$	201
$n = 115$	$115 = 4p^2 + 3p + 3 - 3$	165
$n = 116$	$116 = 4p^2 + 3p + 4 - 3$	130
$n = 117$	$117 = 4p^2 + 4p - 3$	127
$n = 118$	$118 = 4p^2 + 4p + 1 - 3$	218
$n = 119$	$119 = 4p^2 + 4p + 2 - 3$	186
$n = 120$	$120 = 4p^2 + 4p + 3 - 3$	155
$n = 121$	$121 = 4p^2 + 4p + 4 - 3$	125
$n = 122$	$122 = p^3 - 3$	96
$n = 123$	$123 = p^3 + 1 - 3$	192
$n = 124$	$124 = p^3 + 2 - 3$	196
$n = 125$	$125 = p^3 + 3 - 3$	201
$n = 126$	$126 = p^3 + 4 - 3$	207
$n = 127$	$127 = p^3 + p - 3$	220
$n = 128$	$128 = p^3 + p + 1 - 3$	315
$n = 129$	$129 = p^3 + p + 2 - 3$	262
$n = 130$	$130 = p^3 + p + 3 - 3$	241
$n = 131$	$131 = p^3 + p + 4 - 3$	221
$n = 132$	$132 = p^3 + 2p - 3$	205
$n = 133$	$133 = p^3 + 2p + 1 - 3$	308
$n = 134$	$134 = p^3 + 2p + 2 - 3$	260
$n = 135$	$135 = p^3 + 2p + 3 - 3$	213
$n = 136$	$136 = p^3 + 2p + 4 - 3$	198
$n = 137$	$137 = p^3 + 3p - 3$	185
$n = 138$	$138 = p^3 + 3p + 1 - 3$	295
$n = 139$	$139 = p^3 + 3p + 2 - 3$	252
$n = 140$	$140 = p^3 + 3p + 3 - 3$	210
$n = 141$	$141 = p^3 + 3p + 4 - 3$	169

Table B.5: *Dimensions of* $M_n(3)$ where $142 \leq n \leq 165$

Deg n	$n = ap^\alpha + bp^\beta + cp^\gamma - 3$	**Dim** $M_n(3)$
$n = 142$	$142 = p^3 + 4p - 3$	160
$n = 143$	$143 = p^3 + 4p + 1 - 3$	276
$n = 144$	$144 = p^3 + 4p + 2 - 3$	238
$n = 145$	$145 = p^3 + 4p + 3 - 3$	201
$n = 146$	$146 = p^3 + 4p + 4 - 3$	165
$n = 147$	$147 = p^3 + p^2 - 3$	130
$n = 148$	$148 = p^3 + p^2 + 1 - 3$	251
$n = 149$	$149 = p^3 + p^2 + 2 - 3$	218
$n = 150$	$150 = p^3 + p^2 + 3 - 3$	186
$n = 151$	$151 = p^3 + p^2 + 4 - 3$	155
$n = 152$	$152 = p^3 + p^2 + p - 3$	125
$n = 153$	$153 = p^3 + p^2 + p + 1 - 3$	0
$n = 154$	$154 = p^3 + p^2 + p + 2 - 3$	36
$n = 155$	$155 = p^3 + p^2 + p + 3 - 3$	64
$n = 156$	$156 = p^3 + p^2 + p + 4 - 3$	84
$n = 157$	$157 = p^3 + p^2 + 2p - 3$	96
$n = 158$	$158 = p^3 + p^2 + 2p + 1 - 3$	37
$n = 159$	$159 = p^3 + p^2 + 2p + 2 - 3$	45
$n = 160$	$160 = p^3 + p^2 + 2p + 3 - 3$	67
$n = 161$	$161 = p^3 + p^2 + 2p + 4 - 3$	88
$n = 162$	$162 = p^3 + p^2 + 3p - 3$	107
$n = 163$	$163 = p^3 + p^2 + 3p + 1 - 3$	81
$n = 164$	$164 = p^3 + p^2 + 3p + 2 - 3$	80
$n = 165$	$165 = p^3 + p^2 + 3p + 3 - 3$	80

Appendix C

Mathematica code

This appendix is devoted to represent Mathematica code to compute the dimension and basis elements for $M_n(3)$, $\mathcal{W}_n^i(3)$ and $M_n(3)/\mathcal{W}_n^i(3)$ where $i = 1, 2, 3$.

```
p = 3; r = ; s = ; t = ;
d = r + s + t;
x1:=Subscript[x, 1]
y1:=Subscript[y, 1]
z1:=Subscript[z, 1]
xp:=Subscript[x, p]
yp:=Subscript[y, p]
zp:=Subscript[z, p]
xp2:=Subscript[x, p^2]
yp2:=Subscript[y, p^2]
zp2:=Subscript[z, p^2]
xp3:=Subscript[x, p^3]
yp3:=Subscript[y, p^3]
zp3:=Subscript[z, p^3]
xp4:=Subscript[x, p^4]
yp4:=Subscript[y, p^4]
zp4:=Subscript[z, p^4]
ml = 15
Cxy = (x1yp - y1xp);
Cxz = (x1zp - z1xp);
Cyz = (y1zp - z1yp);
Needs[Combinatorica]
```

```
ConvTab = Table[{0, 0, 0, 0, 0}, {i, 0, 100}];
For[i = 0, i ≤ 100, i++,
ID = IntegerDigits[i, p]; l = Length[ID];
ConvTab[[i + 1, 1]] = Mod[Product[Mod[Factorial[ID], p][[q]], {q, l}], p];
ConvTab[[i + 1, 2]] = Mod[(−Factorial[p − 1]/ConvTab[[i + 1, 1]]), p];
ConvTab[[i + 1, 3]] = Product[Subscript[x, p^(l − q)]^(ID[[q]]), {q, l}];
ConvTab[[i + 1, 4]] = Product[Subscript[y, p^(l − q)]^(ID[[q]]), {q, l}];
ConvTab[[i + 1, 5]] = Product[Subscript[z, p^(l − q)]^(ID[[q]]), {q, l}]; ];
Cosets = Table[{{0, 0, 0}, {0, 0, 0}, {0, 0, 0}}, {i, 1, (p + 1) ∗ (p^2 + p + 1)}];
n = 1; Cosets[[n]] = {{1, 0, 0}, {0, 1, 0}, {0, 0, 1}}; n++;
For[q = 0, q < p, q++, Cosets[[n]] = {{1, 0, 0}, {0, q, 1}, {0, 1, 0}}; n++];
For[q = 0, q < p, q++, Cosets[[n]] = {{q, 1, 0}, {1, 0, 0}, {0, 0, 1}}; n++];
For[q = 0, q < p, q++, For[a = 0, a < p, a++,
Cosets[[n]] = {{a, 1, 0}, {q, 0, 1}, {1, 0, 0}}; n++]; ];
For[q = 0, q < p, q++,
For[a = 0, a < p, a++,
Cosets[[n]] = {{a, q, 1}, {1, 0, 0}, {0, 1, 0}}; n++]; ];
For[q = 0, q < p, q++,
For[a = 0, a < p, a++,
For[b = 0, b < p, b++,
Cosets[[n]] = {{a, b, 1}, {q, 1, 0}, {1, 0, 0}}; n++]; ]; ];
Cosets;
Gpaction[xexp_, yexp_, zexp_, gmx_]:=
Module[{i, j, outco, CL, entry, gm = gmx}, outco = {};
If[xexp == 0, gm[[1, 1]] = 0; gm[[2, 1]] = 0; gm[[3, 1]] = 0];
If[yexp == 0, gm[[1, 2]] = 0; gm[[2, 2]] = 0; gm[[3, 2]] = 0];
If[zexp == 0, gm[[1, 3]] = 0; gm[[2, 3]] = 0; gm[[3, 3]] = 0];
Fx = (gm[[1, 1]] ∗ x + gm[[1, 2]] ∗ y + gm[[1, 3]] ∗ z);
Fy = (gm[[2, 1]] ∗ x + gm[[2, 2]] ∗ y + gm[[2, 3]] ∗ z);
Fz = (gm[[3, 1]] ∗ x + gm[[3, 2]] ∗ y + gm[[3, 3]] ∗ z);
Fxi = 1; Fzk = Table[1, {k, 1 + xexp + yexp + zexp}];
If[gm[[3, 1]] ≠ 0||gm[[3, 2]] ≠ 0||gm[[3, 3]] ≠ 0,
For[k = 1, k ≤ xexp + yexp + zexp, k++,
Fzk[[k + 1]] = Fzk[[k]] ∗ Fz; ]; ];
For[i = 0, i ≤ xexp + yexp + zexp, i++, Fyj = 1;
For[j = 0, j ≤ xexp + yexp + zexp − i, j++,
CL = CoefficientList[x^(xexp + 2) ∗ y^(yexp + 2) ∗ z^(zexp + 2) + Fxi ∗ Fyj∗
Fzk[[(xexp + yexp + zexp − i − j) + 1]], {x, y, z}];
entry = Mod[CL[[xexp + 1, yexp + 1, zexp + 1]], p]; If[entry > 0, outco =
```

```
Append[outco, {i, j, entry}]];
Fyj = Fyj * Fy; ]; Fxi = Fxi * Fx; ]; outco]
CohoBasisList = Compositions[r + s + t, 3]; degdim = Length[CohoBasisList];
flaglst = {}; flagmtx = {}; For[f = 1, f ≤ 52, f++, Print[Calculatingflag, f, outof52];
OCL = Gpaction[r, s, t, Cosets[[f]]]; OutIm = 0; NewRow = Table[0, {q, 1, degdim}];
For[q = 1, q ≤ Length[OCL], q++, i = OCL[[q, 1]]; j = OCL[[q, 2]]; k = r + s + t − i − j;
OutIm+ =Mod[OCL[[q, 3]] * ConvTab[[r + 1, 2]] * ConvTab[[s + 1, 2]]*
ConvTab[[t + 1, 2]] * ConvTab[[i + 1, 1]] * ConvTab[[j + 1, 1]] * ConvTab[[k + 1, 1]], p]*
ConvTab[[i + 1, 3]] * ConvTab[[j + 1, 4]] * ConvTab[[k + 1, 5]];
NewRow[[Flatten[Position[CohoBasisList, {i, j, k}]]]]+ =
Mod[OCL[[q, 3]] * ConvTab[[r + 1, 2]] * ConvTab[[s + 1, 2]] * ConvTab[[t + 1, 2]]*
ConvTab[[i + 1, 1]] * ConvTab[[j + 1, 1]] * ConvTab[[k + 1, 1]], p]; ];
flaglst = Append[flaglst, {Cosets[[f]], OutIm}];
flagmtx = Append[flagmtx, NewRow]; ];
flaglst//TableForm;
flagmtx//TableForm;
Steenrod[power_, exponents_]:=Module[{i, j, k, input, coeff, outexp, output},
output = {};
For[i = 0, i ≤ power, i++,
For[j = 0, j ≤ power − i, j++,
k = power − i − j; coeff = Mod[Binomial[exponents[[1]], i], p]*
Mod[Binomial[exponents[[2]], j], p] * Mod[Binomial[exponents[[3]], k], p];
outexp = exponents + (p − 1) * {i, j, k}; If[coeff ≠ 0, output =
Append[output, {coeff, outexp}]]; ]; ]; output];
Explist = Compositions[d, 3]; L = Length[Explist]; ElementList = Explist;
ExponentList = Explist; TopDegCoeff = Table[1, {i, L}];
For[i = 1, i ≤ L, i++, ElementList[[i]] = ConvTab[[Explist[[i, 1]] + 1, 3]]*
ConvTab[[Explist[[i, 2]] + 1, 4]] * ConvTab[[Explist[[i, 3]] + 1, 5]]; ExponentList[[i]] =
Flatten[Transpose[{Reverse[IntegerDigits[Explist[[i, 1]], p, ml/3]],
Reverse[IntegerDigits[Explist[[i, 2]], p, ml/3]], Reverse[IntegerDigits[Explist[[i, 3]], p, ml/3]]}]];
TopDegCoeff[[i]] = Mod[ConvTab[[Explist[[i, 1]] + 1, 1]] * ConvTab[[Explist[[i, 2]] + 1, 1]]*
ConvTab[[Explist[[i, 3]] + 1, 1]], p]; ]; Explist; ElementList; ExponentList; Length[ExponentList]
Explistlower = Compositions[d − (p − 1), 3]; Length[Explistlower]
P1Matrix = Table[0, {j, Length[Explistlower]}, {i, Length[Explist]}];
For[i = 1, i ≤ Length[Explistlower], i++, output = Steenrod[1, Explistlower[[i]]];
For[j = 1, j ≤ Length[output], j++, P1Matrix[[i, Position[Explist, output[[j, 2]]][[1, 1]]]]+ =
output[[j, 1]]; ]; ];
P1Matrix//TableForm;
```

```
HomologyP1Matrix = P1Matrix; If[Length[P1Matrix] > 0, HomologyP1Matrix =
Transpose[HomologyP1Matrix];
For[i = 1, i ≤ Length[ExponentList], i++, HomologyP1Matrix[[i]] =
Mod[TopDegCoeff[[i]] ∗ HomologyP1Matrix[[i]], p]; ]; HomologyP1Matrix =
Transpose[HomologyP1Matrix]; ]; HomologyP1Matrix//TableForm;
Length[HomologyP1Matrix]
power = p; Explistlower = Compositions[d − power ∗ (p − 1), 3]; PpMatrix =
Table[0, {j, Length[Explistlower]}, {i, Length[Explist]}];
For[i = 1, i ≤ Length[Explistlower], i++, output = Steenrod[power, Explistlower[[i]]];
For[j = 1, j ≤ Length[output], j++, PpMatrix[[i, Position[Explist, output[[j, 2]]][[1, 1]]]]+ =
output[[j, 1]]; ]; ]; HomologyPpMatrix = PpMatrix; If[Length[PpMatrix] > 0,
HomologyPpMatrix = Transpose[HomologyPpMatrix];
For[i = 1, i ≤ Length[ExponentList], i++, HomologyPpMatrix[[i]] =
Mod[TopDegCoeff[[i]] ∗ HomologyPpMatrix[[i]], p]; ]; HomologyPpMatrix =
Transpose[HomologyPpMatrix]; ]; HomologyPpMatrix//TableForm;
Length[HomologyPpMatrix]
power = p^2; Explistlower = Compositions[d − power ∗ (p − 1), 3];
Pp2Matrix = Table[0, {j, Length[Explistlower]}, {i, Length[Explist]}];
For[i = 1, i ≤ Length[Explistlower], i++, output = Steenrod[power, Explistlower[[i]]];
For[j = 1, j ≤ Length[output], j++, Pp2Matrix[[i, Position[Explist, output[[j, 2]]][[1, 1]]]]+ =
output[[j, 1]]; ]; ]; HomologyPp2Matrix = Pp2Matrix; If[Length[Pp2Matrix] > 0,
HomologyPp2Matrix = Transpose[HomologyPp2Matrix];
For[i = 1, i ≤ Length[ExponentList], i++, HomologyPp2Matrix[[i]] =
Mod[TopDegCoeff[[i]] ∗ HomologyPp2Matrix[[i]], p]; ]; HomologyPp2Matrix =
Transpose[HomologyPp2Matrix]; ];
HomologyPp2Matrix//TableForm; Length[HomologyPp2Matrix]
power = p^3; Explistlower = Compositions[d − power ∗ (p − 1), 3];
Pp3Matrix = Table[0, {j, Length[Explistlower]}, {i, Length[Explist]}];
For[i = 1, i ≤ Length[Explistlower], i++, output = Steenrod[power, Explistlower[[i]]];
For[j = 1, j ≤ Length[output], j++, Pp3Matrix[[i, Position[Explist, output[[j, 2]]][[1, 1]]]]+ =
output[[j, 1]]; ]; ]; HomologyPp3Matrix = Pp3Matrix; If[Length[Pp3Matrix] > 0,
HomologyPp3Matrix = Transpose[HomologyPp3Matrix];
For[i = 1, i ≤ Length[ExponentList], i++, HomologyPp3Matrix[[i]] =
Mod[TopDegCoeff[[i]] ∗ HomologyPp3Matrix[[i]], p]; ]; HomologyPp3Matrix =
Transpose[HomologyPp3Matrix]; ];
HomologyPp3Matrix//TableForm; Length[HomologyPp3Matrix]
```

```
CombinedMatrix = Join[HomologyP1Matrix, HomologyPpMatrix, HomologyPp2Matrix,
HomologyPp3Matrix];
TimedAnn = AbsoluteTiming[NullSpace[CombinedMatrix, Modulus → p]];
Ann = TimedAnn[[2]]; TimedAnn[[1]]Annlist = {};
For[i = 1, i ≤ Length[Ann], i++, newkerelement = 0;
For[j = 1, j ≤ Length[ElementList], j++, newkerelement+ =(Mod[1 + Ann[[i, j]], p] − 1)∗
ElementList[[j]]]; Annlist = Append[Annlist, newkerelement]; ];
Print[Theannihilatedelementsindegree, d, formaspaceofdimension, Length[Annlist], withbasis :];
Print[Annlist//TableForm];
Length[Annlist]
Combi = Join[flagmtx, Ann];
Redundancy = NullSpace[Transpose[Combi], Modulus → p];
Print[Degree =, d, .Spike =, flaglst[[1, 2]]]; (∗The1stcosetmxisI, sothe1stflagisthespike∗)
diml = 52 − Length[NullSpace[Transpose[flagmtx], Modulus → p]];
Print[Dim(flags) =, diml]; dimm = Length[Ann];
Print[Dim(M) =, dimm]; If[Length[Redundancy] == 52,
Print[Dim(M/L) =, dimm − diml],
Print[LdoesnotappeartobecontainedinM!]];
Redundancy//TableForm;
Essentials = {}; j = Length[Redundancy[[1]]];
For[i = 1, i ≤ Length[Redundancy], i++, If[Redundancy[[i, j]] == 0,
Essentials = Append[Essentials, j]; i−−; ]; j−−; ]; While[j > 0, Essentials =
Append[Essentials, j]; j−−]; EssentialsEssentialFlagList = {}; NonFlagAnnList = {};
For[i = 1, i ≤ Length[Essentials], i++, If[Essentials[[i]] > 52, NonFlagAnnList =
Append[NonFlagAnnList, Annlist[[Essentials[[i]] − 52]]], EssentialFlagList =
Append[EssentialFlagList, flaglst[[Essentials[[i]]]]]]; ];
Print[Abasisfortheflagsgeneratedbythespike, flaglst[[1, 2]], indegree, d, is :,
EssentialFlagList//TableForm];
Print[Column[{ThequotientofMbythissubspaceisspannedby :, NonFlagAnnList//TableForm}]];
```

Bibliography

[1] M. A. Alghamdi, Some problems in algebraic topology: Polynomial algebras over the Steenrod algebra, Ph.D. thesis. University of Aberdeen (1991).

[2] M. A. Alghamdi, M. C. Crabb and J. R. Hubbuck, Representations of the Homology of BV and the Steenrod algebra I, In Adams memorial symposium on algebraic Topology 2, Manchester 1990, eds. N. Ray and G. Walker, Lon. Math. Soc. Lect. Note Series 176, Cambridge Univ. Press, 1992, 217-234.

[3] N. Bourbaki, Algebra I, Elements of Mathematics, Springer-Verlag, Heidelberg, New York, 1989.

[4] D. P. Carlisle, R. M. W. Wood, The boundedness conjecture for the action of the Steenrod algebra on polynomials, In Adams memorial symposium on algebraic Topology 2, Manchester 1990, eds. N. Ray and G. Walker, Lon. Math. Soc. Lect. Note Series 176, Cambridge Univ. Press, 1992, 203-216.

[5] M. C. Crabb and J. R. Hubbuck, Representations of the Homology of BV and the Steenrod algebra II, In Algebraic Topology, New Trends in Localization and Periodcity, Sant Feliu de Guixols, 1994, Progr. Math., Vol. 136, Birkhäuser Vaerlag, Basel, Switzerland, 1996, 143-154.

[6] M. D. Crossley, Results concerning the Steenrod algebra, Ph.D. thesis. University of Aberdeen (1995).

[7] M. D. Crossley, $\mathcal{A}(p)$-annihilated elements in $H_*(\mathbb{C}P^\infty \times \mathbb{C}P^\infty)$, Math. Proc. Camb. Phil. Soc., Vol. 120, 1996, 441-453.

[8] M. D. Crossley, H^*V is of bounded type over $\mathcal{A}(p)$, Proc. Sympos. Pure Math., Amer. Math. Soc., Vol. 63, 1998, 183-190.

[9] M. D. Crossley, On the cohomology of an elementary abelian p-goup as a module over the Steenrod algebra, Preprint 1997.

[10] M. D. Crossley, Monomial basis for $H^*(\mathbb{C}P^\infty) \times \mathbb{C}P^\infty; \mathbb{F}_p)$ over $\mathcal{A}(p)$, Transactions of the Amer. Math. Soc., Vol. 351, No. 1, January 1999, 171-192.

[11] Masaki Kameko, Products of projective spaces as Steenrod modules, Ph.D. thesis, Johns Hopkins University (1990).

[12] Masaki Kameko, Generators of the cohomology of BV_3, J. Math. Kyoto Univ. 38 (1998), 587-593.

[13] Masaki Kameko, Generators of the cohomology of BV_4, Toyama University, preprint, 2003.

[14] F. P. Peterson, Generators of $H^*(\mathbb{R}P^\infty \wedge \mathbb{R}P^\infty)$ as a module over the Steenrod algebra, Abstracts Amer. Math. Soc. 833-55-89, April 1987.

[15] J. Milnor, J. Moore, On the structure of Hopf algebras, Ann. of Math. 81(1965), 211-264.

[16] Saunders Mac Lane, Homology, Springer-Verlag, Berlin, Gottingen, Heidelberg, 1963.

[17] J. Milnor, The Steenrod algebra and its dual, Ann. Math. 67 (1958), 150-171.

[18] Tran Ngoc Nam, Transfert algébrique et action du groups linéaire sur les puissances divisées modulo 2, Ann. Inst. Fourier (Grenoble) 58 (2008), 1785-1837.

[19] J. Repka and P. Selick, On the subalgebra of $H_*((\mathbb{R}P^\infty)^n; \mathbb{F}_2)$ annihilated by Steenrod operations, Journal of Pure and Applied Algebra 127 (1998), 273-288.

[20] Chen Shengmin and Shen Xinyao, On the action of Steenrod powers on polynomial algebras, In algebraic Topology, Barcelona 1990, eds. J. Aguade et al, Lect. Notes in Maths. Vol. 1509, 1992.

[21] William M. Singer, On the action of Steenrood squares on polynomial algebras, Amer. Math. Soc., Vol. 111, No. 2, 1991, 577-583.

[22] L. Smith, Polynomial invariants of finite groups, A. K. Peters Wellesley, Massachusetts, Research Notes in Mathematics, Vol. 6, 1995.

[23] Edwin H. Spanier, Algebric Topology, Mcgraw-Hill, Inc, Series in higher mathematics, USA, 1966.

[24] N. E. Steenrod and D. B. A. Epstein, Cohomology operations, Annals of Math. Studies No. 50, Princeton Univ. Press, 1962.

[25] Nguyễn Sum, The hit problem for the polynomial algebra of four variables, University of Quy Nhon, Viêt Nam, preprint, 2007.

[26] Nguyễn Sum, The negative answer to Kameko's conjecture on the hit problem, Advances in Mathematics, 225 (2010), 2365-2390.

[27] G. Walker and R. M. W. Wood, Flag modules and the hit problem for the Steenrod algebra, Math. Proc. Camb. Phil. Soc., 147 (2009), 143-171.

[28] Grant Walker and Reg Wood, Polynomials and the Steenrod Algebra, preprint, last updated 25 March 2010, available online, http://www.maths.manchester.ac.uk/ grant/bookMar10.pdf

[29] R. M. W. Wood, Steenrod squares of polynomials, In Advances in Homotopy Theory, eds. S.M. Salamon, B. Steer and W.A. Sutherland, Lon. Math. Soc. Lect. Note Series 139, 1989, 173-177.

[30] R. M. W. Wood, Steenrod squares of polynomials and the Peterson conjecture, Math. Proc. Camb. Phil. Soc., Vol. 105, 1989, 307-309.