NILPOTENCE IN THE MOD-P STEENROD ALGEBRA

by
Ismet KARACA

A Dissertation
Presented to the Graduate and Research Committee
of Lehigh University
in Candidacy for the Degree of
Doctor of Philosophy
in
Mathematics

Lehigh University
August 1996

This dissertation is accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

_____
(Date)

_____
Prof. Donald M. Davis
Department of Mathematics
Chairperson and Committee adviser

_____
Assoc.Prof. Bruce A. Dodson
Department of Mathematics

_____
Assoc. Prof. Kenneth G. Monks
Department of Mathematics

_____
Prof. Gilbert A. Stengle
Department of Mathematics

_____
Assoc.Prof. Susan Szczepanski
Department of Mathematics

Acknowledgments

I wish to express my highest gratitude to my adviser, Professor Donald M. Davis, for advising me throughout this thesis, and explaining me every problem clearly. I am grateful for helpful suggestion and conversation with B. Dodson, K. Monks, G. Stengle, and S. Szczepanski. I would like to thank Judy and the faculty at department of mathematics for being pleasant and fruitful. I would like to thank Turkish government for their financial support during my year of graduate study at Lehigh. Finally, I would like thank my parents for being so supportive through my graduate study in the United States.

Contents

Abstract

This thesis explores nilpotence in the Steenrod Algebra $\mathcal{A}$ for an odd prime p. Three major topic areas are discussed here. In Chapter 3, we show that the Milnor element P_t^s has nilpotence $p[\frac{s}{t}] + p$ in the mod-p Steenrod Algebra $\mathcal{A}$ if p is an odd prime number. A similar result was proved by K. Monks when $p = 2$. In Chapter 4, we find formulas for the nilpotence of elements $P(n)$ for certain values of n, and generalize other results proved by Monks when $p = 2$. In chapter 5, we adapt to odd primes results of Monks [19] regarding hit elements and antiautomorphism.

Chapter 1

Introduction

The study of Steenrod algebra began with Steenrod's work constructing stable cohomology operations acting on cohomology theory with $\mathbf{Z}_2$-coefficients. In [24] and [25] he defined operations, the Steenrod square operations

$$\mathrm{Sq}^i : H^k(X; \mathbf{Z}_2) \longrightarrow H^{k+i}(X; \mathbf{Z}_2)$$

which help us to solve some questions in algebraic topology. By composition these operations give rise to an algebra of operations, the mod-2 Steenrod algebra, acting on the $\mathbf{Z}_2$-cohomology groups of spaces. The structure of this algebra was elucidated by Adem [3], Cartan [7], and Serre [20]. In particular, they showed that the mod-2 Steenrod algebra is the tensor algebra on the Sq^i's modulo the Adem relations: For $0 < i < 2j$,

$$\mathrm{Sq}^i\mathrm{Sq}^j = \sum_{k=0}^{[\frac{i}{2}]} \binom{j-k-1}{i-2k} \mathrm{Sq}^{i+j-k}\mathrm{Sq}^k.$$

In [20] Serre also observed that the representability of the cohomology groups implies that this algebra is the complete algebra of stable cohomology operations. In [15] Milnor observed that the Steenrod algebra has the structure of a co-commutative Hopf algebra. Therefore the dual is a commutative algebra.

The problem of determining the nilpotence height of elements of the Steenrod algebra has been of recent interest. For prime 2, the nilpotence height of Sq^{2^n} was conjectured to be $2n + 2$ by Steve Wilson in 1975. In [9] Donald M. Davis showed

that $(\mathrm{Sq}^{2^n})^{2n+1} \neq 0$. At the same time, Davis verified by computer calculation that $(\mathrm{Sq}^{2^n})^{2n+2} = 0$ for $n \leq 5$. Kenneth Monks also verified this for $n = 6, 7$. In 1994 this conjecture was proved by Walker and Wood (see [28]). Later they generalized this result for odd primes p (see [29]).

The nilpotence height of Milnor elements P_t^s was determined by Kenneth Monks [18] when $p = 2$. We adapt Monks' results about the nilpotence height of Milnor elements P_t^s to odd primes in Theorem 3.1.1 which says that the nilpotence height of Milnor elements P_t^s is exactly $p([\frac{s}{t}] + 1)$. In [17] Monks found the nilpotence of certain families of elements Sq^n. In Theorem 4.1.1 and Theorem 4.1.2, we adapt these results to odd primes. For example, we prove that the nilpotence heights of $P(\frac{p^k((p-1)p^m-1)+1}{p-1})$ and $P(p^m - 1)$ are $m + 2$, $m + 1$ respectively. In Theorem 4.1.3, we find formulas for the nilpotence of elements $P(n)$ for the certain values of n. In Theorem 5.1.1 and Theorem 5.1.2, we generalize results of Monks [19] about hit polynomials and the antiautomorphism for odd primes.

Chapter 2

The Steenrod Algebra and Its Anti-automorphism

2.1 The Steenrod Algebra and Its Dual

In this chapter, we will review much of background knowledge needed for the rest of this dissertation. Let p be an odd prime number and $\mathbf{Z}_p = \mathrm{Z}/p\mathrm{Z}$. Let

$$\beta : H^q(X; \mathbf{Z}_p) \longrightarrow H^{q+1}(X; \mathbf{Z}_p)$$

be the Bockstein coboundary operator associated to the exact sequence

$$0 \to \mathbf{Z}_p \to \mathbf{Z}_{p^2} \to \mathbf{Z}_p \to 0.$$

It is known that β is natural for mapping of spaces, that $\beta^2 = 0$, and that

$$\beta(xy) = \beta(x)y + (-1)^q x\beta(y)$$

where $\dim x = q$. Let $P^i : H^q(X; \mathbf{Z}_p) \longrightarrow H^{q+2i(p-1)}(X; \mathbf{Z}_p)$ be a natural homomorphism which has the following axioms:

1)$P^0 : H^q(X; \mathbf{Z}_p) \longrightarrow H^q(X; \mathbf{Z}_p)$ is the identity homomorphism.

2)If $\dim x = 2k$, then $P^k(x) = x^p$.

3)If $\dim x > 2k$, then $P^k(x) = 0$.

4)**Cartan Formula:** If $x, y \in H^*(X; Z_p)$, then

$$P^k(xy) = \sum_i P^i(x) P^{k-i}(y)$$

5)**Adem Relations:** If $a < pb$, then

$$P^a P^b = \sum_{t=0}^{[\frac{a}{p}]} (-1)^{a+t} \binom{(p-1)(b-t)-1}{a-pt} P^{a+b-t} P^t$$

If $a \leq pb$ then

$$\begin{aligned} P^a \beta P^b &= \textstyle\sum_{t=0}^{[\frac{a}{p}]} (-1)^{a+t} \binom{(p-1)(b-t)}{a-pt} \beta P^{a+b-t} P^t \\ &+ \textstyle\sum_{t=0}^{[\frac{a-1}{p}]} (-1)^{a+t} \binom{(p-1)(b-t)-1}{a-pt-1} \beta P^{a+b-t} \beta P^t. \end{aligned}$$

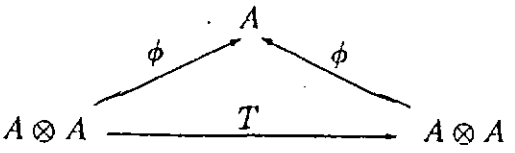
Let $M = (M_i)$ be a sequence of R-modules where R is a commutative ring and $i \geq 0$. Then M is called a **graded module.** We say the elements of M_i have degree i or dimension i. A homomorphism $f : A \to B$ of graded modules is a sequence of homomorphisms $f_i : A_i \to B_i$. If M and N are graded modules, we define the graded module $M \otimes N = \sum_i M_i \otimes N_{r-i}$. A graded R-module A is called a graded algebra if there is a homomorphism $\phi : A \otimes A \to A$ and a unit element 1. The algebra is said be associative if the following diagram is commutative;

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\phi \otimes 1} & A \otimes A \\ \downarrow{\scriptstyle 1 \otimes \phi} & & \downarrow{\scriptstyle \phi} \\ A \otimes A & \xrightarrow{\phi} & A \end{array}$$

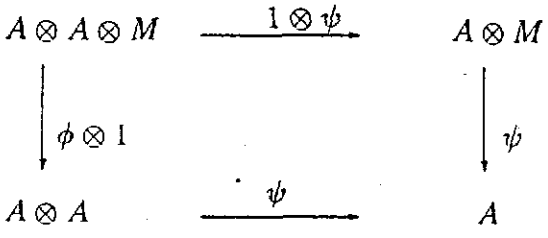
Let B be a graded algebra. Let $T : A \otimes B \longrightarrow B \otimes A$ be the map defined by

$$T(a \otimes b) = (-1)^{pq} b \otimes a$$

where $\dim a = p$ and $\dim b = q$. We say the algebra is commutative if the following diagram commutes;



A homomorphism $f : A \to B$ of algebras is a homomorphism of modules which commutes with multiplication, i.e. $f\phi_A = \phi_B(f \otimes f)$ and such that $f(1) = 1$. Let M be a graded module and A be a graded algebra. M is called an A-module if there is a map $\psi : A \otimes M \longrightarrow M$ which respects the unit of A and such that the following diagram commutes;



If B is a graded algebra, then $A \otimes B$ is given a graded algebra structure by the multiplication

$$A \otimes B \otimes A \otimes B \to A \otimes A \otimes B \otimes B \to A \otimes B.$$

If N is a B-module, then $M \otimes N$ is an $A \otimes B$-module by the mapping

$$A \otimes B \otimes M \otimes N \to A \otimes M \otimes B \otimes N \to M \otimes N.$$

The ground ring R may be regarded as a graded module such that $R_i = 0$ if $i > 0$. We say a graded algebra is **augmented** if there is an algebra homomorphism $\epsilon : A \longrightarrow R$.

Now we can define **the mod-p Steenrod algebra** $\mathcal{A}$ to be a graded associative algebra generated by the element P^i of degree $2i(p-1)$ and the element β of degree

1. A monomial in $\mathcal{A}$ can be written in the form

$$\beta^{\epsilon_0} P^{r_1} \beta^{\epsilon_1} P^{r_2} \beta^{\epsilon_2} \dots P^{r_k} \beta^{\epsilon_k}$$

where $\epsilon_i = 0$ or 1 and $r_i \geq 0$. We denote this monomial by P^I where $I = (\epsilon_0, r_1, \epsilon_1, \dots, r_k, \epsilon_k)$. A sequence I is called **admissible** if $r_i \geq pr_{i+1} + \epsilon_i$ for $i \geq 1$. Hence P^I will be called **admissible monomial** if I is admissible.

Proposition 2.1.1 *The admissible monomials P^I form a basis for the mod-p Steenrod algebra $\mathcal{A}$.*

This can be proved by using Adem relation (see [26]).

Let A be an augmented graded algebra over a commutative ring R with unit. We say A is a **Hopf algebra** if

1) There is a "diagonal map" of algebras $\psi : A \longrightarrow A \otimes A$.

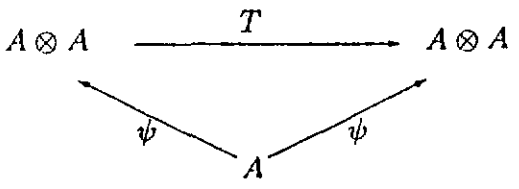
2) The following compositions are both the identity;

$$\begin{array}{ccccc} A & \longrightarrow & A \otimes A & \xrightarrow{\epsilon \otimes 1} & R \otimes A \\ & & \downarrow{\scriptstyle 1 \otimes \epsilon} & & \downarrow{\scriptstyle \simeq} \\ & & A \otimes R & \xrightarrow{\simeq} & A \end{array}$$

We say ψ is **associative** if the following diagram commutes;

$$\begin{array}{ccc} A & \xrightarrow{\psi} & A \otimes A \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi \otimes 1} \\ A \otimes A & \xrightarrow{1 \otimes \psi} & A \otimes A \otimes A \end{array}$$

We say ψ is **commutative** if the following diagram commutes;



Theorem 2.1.2 *The mod-p Steenrod algebra $\mathcal{A}$ is a Hopf algebra with commutative and associative diagonal map.*

We recall the structure of dual algebra $\mathcal{A}^*$ of $\mathcal{A}$. It was computed by Milnor [15].

Proposition 2.1.3 *There is a unique algebra map $\phi : \mathcal{A} \longrightarrow \mathcal{A} \otimes \mathcal{A}$ such that for all $i \geq 0$*

$$\phi(P^i) = \sum_{j+k=i} P^j \otimes P^k$$

and

$$\phi(\beta) = \beta \otimes 1 + 1 \otimes \beta.$$

This can be proved by using the Kunneth Theorem and Cartan formula. Since the mod-p Steenrod algebra is a co-commutative Hopf algebra, its dual $\mathcal{A}^*$ is a commutative Hopf algebra.

Theorem 2.1.4 (Milnor) *The algebra $\mathcal{A}^*$ is the tensor product of a polynomial algebra on generators ξ_i $i \geq 1$ of degree $2(p^i - 1)$ by an exterior algebra on generators τ_i $i \geq 0$ of degree $2p^i - 1$. Moreover the coproduct ϕ is given by the formula*

$$\phi(\xi_k) = \sum_{i=0}^{k} \xi_{k-i}^{p^i} \otimes \xi_i$$

and

$$\phi(\tau_k) = \tau_k \otimes 1 + \sum_{i=0}^{k-1} \xi_{k-i}^{p^i} \otimes \tau_i.$$

So the monomial basis in $\mathcal{A}^*$ can be written in the form

$$\xi^I = \tau_0^{\epsilon_0}\xi_1^{r_1}\tau_1^{\epsilon_1}\cdots$$

Then dual to the the monomial basis ξ^I is a basis for the mod-p Steenrod algebra known as Milnor basis. So $Q_0^{\epsilon_0}Q_1^{\epsilon_1}\cdots P(r_1,r_2,\ldots)$ will denote the dual of ξ^I.

The mod p Steenrod algebra is given as a graded $\mathbf{Z}_p$-module on the Milnor basis with product and coproduct defined in terms of that basis. So $\mathcal{A}$ is a $\mathbf{Z}_p$-module with basis symbols $Q_0^{\epsilon_0}Q_1^{\epsilon_1}\cdots P(r_1,r_2,\ldots)$ such that $\epsilon_i = 0$ or 1, $r_j \geq 0$. The degree of

$$Q_0^{\epsilon_0}Q_1^{\epsilon_1}\cdots P(r_1,r_2,\ldots)$$

is given by $\sum_i \epsilon_i(2p^i-1)+\sum_j 2r_j(p^j-1)$. The product is given by

$$P(r_1,r_2,\ldots)\cdot P(s_1,s_2,\ldots) = \sum_X \beta(X)P(t_1,t_2,\ldots) \tag{2.1}$$

where the sum is taken over all matrices $X=(x_{ij})$ satisfying

$$\sum_i x_{ij} = s_j \tag{2.2}$$

$$\sum_j x_{ij}p^j = r_i \tag{2.3}$$

$$\sum_{i+j=k} x_{ij} = t_k \tag{2.4}$$

$$\beta(X) = \prod_h (x_{h,0}, x_{h-1,1},\ldots,x_{0,h}) \in \mathbf{Z}_p, \tag{2.5}$$

where $(n_1,n_2,\ldots,n_h)$ is the multinomial coefficient $\frac{(n_1+n_2+\cdots n_h)!}{n_1!n_2!\cdots n_h!}$ mod p. The coproduct is given by

$$\phi(Q_r) = Q_r\otimes 1 + 1\otimes Q_r \tag{2.6}$$

$$\phi(P(r_1,r_2,\ldots)) = \sum_{s_i+t_i=r_i} P(s_1,s_2,\ldots)\otimes P(t_1,t_2,\ldots). \tag{2.7}$$

We say that a matrix $X=(x_{ij})$ is (R,S)-allowable if it satisfies the conditions (2.2), (2.3).

2.2 The Canonical Anti-automorphism

Let A be a Hopf algebra. There is a homomorphism $\chi : A \longrightarrow A$ defined by the properties:

(i) $\chi(1) = 1$

(ii) If $\phi(a) = \sum a'_i \otimes a''_i$ where $\dim a > 0$, then $\sum a'_i \chi(a''_i) = 0$ (see [16]).

So in the Steenrod algebra there exists a unique homomorphism $\chi : \mathcal{A} \longrightarrow \mathcal{A}$ satisfying (i) and (ii). It can be proved that χ is an anti-automorphism in the sense $\chi(ab) = \chi(b)\chi(a)$, χ is one-to-one and onto, and so it maps basis elements of $\mathcal{A}$ into new basis elements of $\mathcal{A}$. Similarly there is a canonical anti-automorphism for the dual Hopf algebra $\mathcal{A}^*$ with diagonal map $\phi(\xi_k) = \sum_{i=0}^{k} \xi_{k-i}^{p^i} \otimes \xi_i$. Defining relation becomes

$$\sum_{i=0}^{k} \xi_{k-i}^{p^i} \chi(\xi_i) = 0.$$

Donald M. Davis [8] proved nice formulae involving the canonical anti-automorphism χ of the mod-p Steenrod algebra.

Theorem 2.2.1

$$\chi(P^{p^{n-1}+p^{n-2}+\cdots+p+1}) = (-1)^n P^{p^{n-1}} P^{p^{n-2}} \cdots P^p P^1.$$

Theorem 2.2.1 follows easily by induction on n from the following two results. Let $S(i)$ denote the sum of all Milnor basis elements of the form P^R in dimension i.

Theorem 2.2.2 *([15])*

$$\chi(P^i) = (-1)^i S(2i(p-1)).$$

Proposition 2.2.3 *([8])*

$$P^m S(l) = \sum_R \binom{\sum p^i r_i}{pm} P^R.$$

Chapter 3

Nilpotence of the element P_t^s

3.1 The Main Results

In [17] it was shown that the element P_t^s has nilpotence height $2[\frac{s}{t}] + 2$ in the mod 2 Steenrod algebra. Here the method and result are generalized to show that for an odd prime p the element P_t^s has nilpotence height $p[\frac{s}{t}] + p$ in the mod p Steenrod algebra. Recall that P_t^s is the Milnor basis element $P(r_1, r_2, \ldots, r_t)$ with $r_t = p^s$ and $r_i = 0$ for $i < t$.

Theorem 3.1.1 *For all $s \geq 0$, $t \geq 1$,*

(i) $(P_t^s)^{p[\frac{s}{t}]+p} = 0$

(ii) $(P_t^s)^{p[\frac{s}{t}]+p-1} \neq 0.$

Thus the nilpotence height of P_t^s is exactly $p\left[\frac{s}{t}\right] + p$. The upper bound (i) on the nilpotence order was proved in [17] for the case $p = 2$. The lower bound (ii) was proved in [18] for the case $p = 2$. Here we generalize these arguments.

Let $P_t(r_1, r_2, \ldots, r_m)$ be the Milnor basis element $P(s_1, s_2, \ldots, s_{tm})$ where $s_{ti} = r_i$ and $s_j = 0$ if t does not divide j. In particular $P_t(p^s) = P_t^s$ and $P_1(n) = P(n)$.

If $R = (r_1, r_2, \ldots, r_m)$ is a sequence of nonnegative integers, we will write $P_t(R)$ for the corresponding Milnor basis element. The degree of $P_t(R)$ is $2\,|R|_t$ where $|R|_t = \sum_{i=1}^{\infty} (p^{it} - 1)\, r_i$ and the excess of $P_t(R)$ is $2e(R)$ where $e(R) = \sum_{i=1}^{\infty} r_i$. For

a fixed t let B_t be the vector subspace of A with basis the set of all $P_t(R)$. For $P_t^s \in B_t$ write $\widehat{P_t^s}$ for $(-1)^s\chi(P_t^s)$ where χ denotes the canonical anti-automorphism of B_t.

We will introduce the useful notation: each natural number a has a unique expansion

$$a = \sum_{i=0}^{\infty} \alpha_i(a)p^i \tag{3.1}$$

with $0 \leq \alpha_i(a) < p$. Let $0 \leq b < p^t$, and $i < t$. Then the following are obvious,

$$\alpha_i(a) = \alpha_{i+t}(p^t a + b) \tag{3.2}$$

$$\alpha_i(b) = \alpha_i(p^t a + b). \tag{3.3}$$

Definition 3.1.2 *We say that m and n have no carries if $\alpha_i(m) + \alpha_i(n) \leq p-1$ for all i. This is equivalent to the condition that the binomial coefficient $\binom{m+n}{m}$ is nonzero* mod$p$ *. If m and n have no carries, we will write $m \asymp n$.*

Define $\gamma_t(m) = \sum_{i=0}^{m-1} p^{it}$ for any integer $m \geq 0$ and $t \geq 1$ where $\gamma_t(0) = 0$. The following fact is immediate.

Fact 3.1.3 $\gamma_t(m+1) = p^t\gamma_t(m) + 1$.

Proposition 3.1.4 *For any $t \geq 1$, $m \geq 0$, and $i < t$,*

$$P_t((p-1)\,p^i\gamma_t(m+1)) \cdot P_t^{mt+i} = 0. \tag{3.4}$$

Proof: By Milnor's product formula, $P_t(a) \cdot P_t(b) = \sum u_j \cdot P_t(a+b-(p^t+1)j, j)$ where the sum is taken over all j such that $(a-p^tj) \asymp (b-j)$, and u_j is a unit mod p. So it is sufficient to show that $(p-1)p^i\gamma_t(m+1) - p^tj$ and $p^{mt+i} - j$ have at least one carry for any $0 \leq j \leq p^i(p-1)\gamma_t(m)$. This is the content of the following lemma.

Lemma 3.1.5 *For all $t \geq 1$, $m \geq 0$, $i < t$ and $0 \leq j \leq p^i(p-1)\gamma_t(m)$, there exists a nonnegative integer k such that $\alpha_{kt+i}(p^i(p-1)\gamma_t(m+1) - p^tj) + \alpha_{kt+i}(p^{mt+i} - j) \geq p$.*

Proof: We will proceed by induction on m. Let

$$X = (p-1)p^i\gamma_t(m+1) - p^t j \tag{3.5}$$

$$Y = p^{mt+i} - j. \tag{3.6}$$

If $m = 0$, then $j = 0$, $X = (p-1)p^i$, and $Y = p^i$. So we have $\alpha_i(X) + \alpha_i(Y) = p$.

Assume that for all $t \geq 1$, $0 \leq i < t$, and $0 \leq j \leq p^i(p-1)\gamma_t(m-1)$, there exists a nonnegative integer k such that $\alpha_{kt+i}(p^i(p-1)\gamma_t(m) - p^t j) + \alpha_{kt+i}(p^{(m-1)t+i} - j) \geq p$.

Choose $t \geq 1$, $i < t$, and $0 \leq j \leq p^i(p-1)\gamma_t(m)$. If $j = 0$, then

$$\begin{aligned} X &= (p-1)p^i\gamma_t(m+1) = (p-1)\left(p^{mt+i} + p^{(m-1)t+i} + p^{(m-2)t+i} + \cdots + p^{t+i} + p^i\right) \\ Y &= p^{mt+i} \end{aligned}$$

Hence $\alpha_{mt+i}(X) + \alpha_{mt+i}(Y) = p$.

Suppose $j \neq 0$.

Case 1: $\alpha_i(j-1) \neq p-1$.

$$X = (p-1)p^i(p^t\gamma_t(m) + 1) - p^t j = p^t[(p-1)p^i\gamma_t(m) - j] + (p-1)p^i.$$

Since $\alpha_i(j-1) \neq p-1$, $j-1 = p^{i+1}q + p^i h + r$ where $0 \leq r < p^i$ and $0 \leq h < p-1$.

$$\begin{aligned} Y &= p^{mt+i} - j = p^{mt+i} - (p^{i+1}q + p^i h + r + 1) \\ &= p^{i+1}[p^{mt-1} - (q+1)] + (p-1-h)p^i + (p^i - (r+1)). \end{aligned}$$

Since $r < p^i$, the term $(p^i - (r+1))$ is nonnegative and less than p^i. So $\alpha_i(X) + \alpha_i(Y) = 2p - h - 2 \geq p$.

Case 2: $\alpha_i(j-1) = p-1$.

Let $j - 1 = p^t q + r$ where $0 \leq r < p^t$. Since $\alpha_i(j-1) = p-1$, $p^i(p-1) \leq r < p^t$ by (3.3). In the assumption we have $j \leq p^i(p-1)\gamma_t(m)$. Then $p^t q + r + 1 \leq p^i(p-1)(p^t\gamma_t(m-1) + 1)$. Solving for $q+1$ shows

$$q + 1 \leq p^i(p-1)\gamma_t(m-1) + \frac{p^i(p-1) - r - 1 + p^t}{p^t}.$$

Since $p^i(p-1) \leq r$, $\frac{p^i(p-1)-r-1+p^t}{p^t} < 1$. Thus $q + 1 \leq p^i(p-1)\gamma_t(m-1)$ and so by the inductive hypothesis there exists a nonnegative integer k such that

$$\alpha_{kt+i}((p-1)p^i\gamma_t(m) - p^t(q+1)) + \alpha_{kt+i}(p^{(m-1)t+i} - (q+1)) \geq p.$$

Let k be any such value. We will show that $\alpha_{(k+1)t+i}(X) + \alpha_{(k+1)t+i}(Y) \geq p$ which will complete the induction and hence the proof.

Now since $\alpha_i(j-1) = p-1$, $\alpha_i(r) = p-1$. Hence $\alpha_i(p^t - 1 - r) = 0$. Therefore $p^t - 1 - r + (p-1)p^i < p^t$. Then we have

$$\alpha_{kt+i}((p-1)p^i\gamma_t(m) - p^t(q+1)) = \alpha_{kt+i}((p-1)p^i\gamma_t(m) - p^t(q+1) + p^t - 1 - r)$$

$$= \alpha_{(k+1)t+i}(p^t\left[(p-1)p^i\gamma_t(m) - p^t(q+1) + p^t - 1 - r\right] + (p-1)p^i) = \alpha_{(k+1)t+i}(X)$$

by (3.2) and (3.3).

$$Y = p^{mt+i} - (p^tq + r + 1) = p^t(p^{(m-1)t+i} - (q+1)) + (p^t - (1+r)).$$

Thus

$$\alpha_{kt+i}(p^{(m-1)t+i} - (q+1)) = \alpha_{(k+1)t+i}(p^t(p^{(m-1)t+i} - (q+1)) + (p^t - (1+r))) = \alpha_{(k+1)t+i}(Y)$$

by (3.2). By the induction hypothesis, $\alpha_{(k+1)t+i}(X) + \alpha_{(k+1)t+i}(Y) \geq p$. ■

Using Davis' method [8] we can derive the formulae,

Proposition 3.1.6

$$P_t(u) \cdot \hat{P}_t(v) = \sum_R \binom{|R|_t + e(R)}{p^t u} P_t(R) \tag{3.7}$$

$$\hat{P}_t(u) \cdot P_t(v) = \sum_R \binom{e(R)}{v} P_t(R) \tag{3.8}$$

where the sum is taken over all R for which $|R|_t = (p^t - 1)(u + v)$.

Proof: The formula (3.7) is exactly Corollary 1*a* in [10]. So we will prove formula (3.8). Using Gallant's Proposition 1 that $\chi(P_t^s)$ is $(-1)^s$ times the sum of all $P_t(R)$ in the appropriate dimension, we see that the product $\hat{P}_t(u) \cdot P_t(v)$ contains a term

$$\prod_i \binom{r_i}{s_i} P_t(r_1, r_2, \ldots)$$

for each Milnor matrix,

	0	...	0	v
*	0	...	0	s_1
0	0	...	0	0
⋮	⋮		⋮	⋮
0	0	...	0	0
$r_1 - s_1$	0	...	0	s_2
0	0	...	0	0
⋮	⋮		⋮	⋮
0	0	...	0	0
$r_2 - s_2$	0	...	0	s_3
0	0	...	0	0
⋮	⋮		⋮	⋮

such that $v = \sum_i s_i$. Thus

$$\hat{P}_t(u) \cdot P_t(v) = \sum_R \sum_S \prod_i \binom{r_i}{s_i} P_t(R)$$

where S ranges over sequences $(s_1, s_2, \ldots)$ having $\sum_i s_i = v$. The equation

$$\sum_S \prod_i \binom{r_i}{s_i} = \binom{\sum_i r_i}{v}$$

follows immediately from considering the coefficient of x^v in the expansion of

$$(1+x)^{r_1} \cdot (1+x)^{r_2} \cdots (1+x)^{r_n}.$$

Hence we have

$$\hat{P}_t(u) \cdot P_t(v) = \sum_R \binom{\sum_i r_i}{v} P_t(R) = \sum_R \binom{e(R)}{v} P_t(R). \quad \blacksquare$$

Using these formulae, we can prove the following proposition.

Proposition 3.1.7 *If a, b and t are positive integers with $a \geq t$, then*

$$\hat{P}_t(p^a(p-1)) \cdot P_t(p^{a+b} - p^a(p-1)) = P_t(p^{a+b} - p^{a-t}(p-1)) \cdot \hat{P}_t(p^{a-t}(p-1)). \quad (3.9)$$

Proof: Using (3.7) and (3.8), we have

$$P_t(p^{a+b} - p^{a-t}(p-1)) \cdot \hat{P}_t(p^{a-t}(p-1)) = \sum_R \binom{|R|_t + e(R)}{p^{a+b+t} - p^a(p-1)} P_t(R)$$

and

$$\hat{P}_t(p^a(p-1)) \cdot P_t(p^{a+b} - p^a(p-1)) = \sum_R \binom{e(R)}{p^{a+b} - p^a(p-1)} P_t(R)$$

where $1 \leq e(R) \leq p^{a+b}$ and $|R|_t = (p^t - 1)p^{a+b}$.

In order to prove these sums are equal, we need to show that their binomial coefficients are equivalent mod p. Note that

$$\binom{e(R)}{p^{a+b} - p^a(p-1)} = \binom{e(R)}{e(R) - p^{a+b} + p^a(p-1)} \tag{3.10}$$

$$\binom{|R|_t + e(R)}{p^{a+b+t} - p^a(p-1)} = \binom{|R|_t + e(R)}{e(R) - p^{a+b} + p^a(p-1)}. \tag{3.11}$$

Case 1: If $1 \leq e(R) < p^{a+b} - p^a(p-1)$, then both binomial coefficients are zero because $e(R) - p^{a+b} + p^a(p-1)$ is a negative integer.

Case 2: If $p^{a+b} - p^a(p-1) \leq e(R) < p^{a+b}$, then

$$\binom{|R|_t + e(R)}{e(R) - p^{a+b} + p^a(p-1)} = \binom{\sum_{i=a+b}^{a+b+t-1} \alpha_i(|R|_t)p^i + \sum_{i=0}^{a+b-1} \alpha_i(e(R))p^i}{\sum_{i=0}^{a+b-1} \alpha_i(e(R) - p^{a+b} + p^a(p-1))p^i}$$

$$\equiv \prod_{i=a+b}^{a+b+t-1} \binom{\alpha_i(|R|_t)}{0} \prod_{i=0}^{a+b-1} \binom{\alpha_i(e(R))}{\alpha_i(e(R) - p^{a+b} + p^a(p-1))} \bmod p$$

$$\equiv \binom{e(R)}{e(R) - p^{a+b} + p^a(p-1)} \bmod p.$$

Hence

$$\binom{|R|_t + e(R)}{p^{a+b+t} - p^a(p-1)} \equiv \binom{e(R)}{p^{a+b} - p^a(p-1)} \bmod p.$$

Case 3: If $e(R) = p^{a+b}$, then

$$\binom{e(R)}{p^{a+b} - p^a(p-1)} = \binom{p^{a+b}}{p^a(p-1)} \equiv 0 \bmod p$$

and

$$\binom{|R|_t + e(R)}{p^{a+b+t} - p^a(p-1)} = \binom{p^{a+b+t}}{p^a(p-1)} \equiv 0 \bmod p.$$

So the result holds. ■

If n, k and t are positive integers with $n = k + mt$ for some m, we define

$$(X_t)_k^n = P_t\left(p^n(p-1)\right) \cdot P_t\left(p^{n-t}(p-1)\right) \cdots P_t\left(p^k(p-1)\right) \tag{3.12}$$

The following corollary is immediate from Proposition 3.0.10.

Corollary 3.1.8 *Let $m \geq 1$, $c \geq 0$, and $a = c + mt$. Then*

$$\chi((X_t)_{c+t}^a) \cdot P_t\left(p^{a+b} - p^a(p-1)\right) = P_t\left(p^{a+b} - p^c(p-1)\right) \cdot \chi((X_t)_c^{a-t}).$$

For any Milnor basis element θ, define $\kappa_\theta : A \longrightarrow A$ by

$$\phi(x) = \sum \kappa_\theta(x) \otimes \theta \tag{3.13}$$

where ϕ is the diagonal map in A. These operations were first defined by Kristensen [12]. We will call it "stripping by θ". It follows from (3.13) that stripping a Milnor basis element by $\theta = P(t_1, t_2 \ldots)$ is given by

$$\kappa_\theta\left(P(r_1, r_2, \ldots)\right) = P(r_1 - t_1, r_2 - t_2, \ldots) \tag{3.14}$$

where the right hand side is taken to be 0 if $r_i < t_i$ for any i (see [28] and [29] for more details).

For any $x, y \in A$,

$$\sum \kappa_{P(R)}(x \cdot y) \otimes P(R) = (\sum \kappa_{P(I)}(x) \otimes P(I))(\sum \kappa_{P(J)}(y) \otimes P(J))$$

$$= \sum \kappa_{P(I)}(x)\kappa_{P(J)}(y) \otimes P(I)P(J) = \sum \lambda_R^{I,J} \kappa_{P(I)}(x)\kappa_{P(J)}(y) \otimes P(R)$$

where $\lambda_R^{I,J} = \langle P(I)P(J), \xi^R \rangle$ and the sums are taken over all I, J, R such that $R = I + J$. So

$$\kappa_{P(R)}(x \cdot y) = \sum_{I,J,R} \lambda_R^{I,J} \kappa_{P(I)}(x)\kappa_{P(J)}(y).$$

In particular, if $\kappa_t^s = \kappa_{P_t^s}$, then $\kappa_t^s(x \cdot y) = \sum_{j=0}^t \kappa_{t-j}^{s+j}(x)\kappa_j^s(y)$ follows from the formula $\phi(\xi_k) = \sum_{i=0}^k \xi_{k-i}^{p^i} \otimes \xi_i$.

Lemma 3.1.9 *If x and y belong to B_t then stripping by P_t^s is a derivation, i.e.*

$$\kappa_t^s(x \cdot y) = \kappa_t^s(x) \cdot y + x \cdot \kappa_t^s(y). \tag{3.15}$$

Proof: The proof follows from the formula above since all of the other terms in the sum correspond to stripping by Milnor basis elements which are not in B_t and therefore give zero. ■

Definition 3.1.10 *A sequence $R = (r_1, r_2, \ldots)$ is called a t-representation of a positive integer m if $m = \sum_i \gamma_t(i) r_i$. A function $\mu_t(m) = \min\{\sum_i r_i : (r_1, r_2, \ldots)$ is a t-representation of $m\}$ is called a minimum excess function.*

Lemma 3.1.11 *For $m \geq 0$,*

$$\mu_t(m) = \min\{e(P_t(R)) : |R|_t = (p^t - 1)m\}.$$

Proof: There is a $1-1$ correspondence between Milnor basis elements $P_t(R)$ satisfying $|R|_t = (p^t - 1)m$ and t-representations of m given by

$$P_t(R) \longleftrightarrow m = \sum_i r_i \gamma_t(i).$$

Under this correspondence, $e(P_t(R))$ corresponds to the number $\sum_i r_i$ which is used in determining $\mu_t(m)$. The lemma follows immediately from this observation. ■

Thus we have following lemma which is analogous to Davis' formula (Theorem 2.2.1).

Lemma 3.1.12 *For all $m \geq 0$ and $t \geq 1$,*

$$\widehat{P}_t((p-1)p^{t-1}\gamma_t(m)) = (X_t)_{t-1}^{mt-1}.$$

Proof: We will prove it by induction on m. If $m = 1$ then the result holds since $P_t(p^{t-1}(p-1))$ is the only $P_t(R)$ in this dimension. Assume that the result holds for $m-1$. By (3.7),

$$(X_t)_{t-1}^{mt-1} = P_t((p-1)p^{mt-1}) \cdot (X_t)_{t-1}^{(m-1)t-1} = P_t((p-1)p^{mt-1}) \cdot \widehat{P}_t((p-1)p^{t-1}\gamma_t(m-1))$$

$$= \sum_R \binom{|R|_t + e(R)}{(p-1)p^{(m+1)t-1}} P_t(R)$$

where the sum is taken over all R such that $|R|_t = \sum_i (p^{it}-1)r_i = (p-1)p^{t-1}(p^{mt}-1)$. By Lemma 3.1.11,

$$\mu_t((p-1)p^{t-1}\gamma_t(m)) \leq \sum_i r_i \leq (p-1)p^{t-1}\gamma_t(m).$$

By [10], the t-representation of $(p-1)p^{t-1}\gamma_t(m)$ with $r_m = (p-1)p^{t-1}$ and all other $r_i = 0$ has minimal $\sum_i r_i$. Hence $\mu_t((p-1)p^{t-1}\gamma_t(m)) = (p-1)p^{t-1}$. So we have

$$(p-1)p^{t-1}(p^{mt}-1) + (p-1)p^{t-1} \leq \sum_i p^{it} r_i \leq (p-1)p^{t-1}\gamma_t(m+1);$$

that is,

$$(p-1)p^{(m+1)t-1} \leq \sum_i p^{it} r_i \leq (p-1)p^{t-1}\gamma_t(m+1).$$

Hence $\left(\frac{\sum_i p^{it} r_i}{(p-1)p^{(m+1)t-1}}\right) \equiv 1 \bmod p$. By Proposition 1 in [10],

$$\hat{P}_t((p-1)p^{t-1}\gamma_t(m)) = \sum_R P_t(R) \tag{3.16}$$

where the sum is taken over all R such that $|R|_t = (p-1)p^{t-1}(p^{mt}-1)$. Therefore we have $(X_t)_{t-1}^{mt-1} = \hat{P}_t((p-1)p^{t-1}\gamma_t(m))$. ■

The following lemma is analogous to Lemma 1.4 in [29] .

Lemma 3.1.13 *(i) For $s \geq 0$ and $t \geq 1$ let κ_t^s denote the operation of stripping by P_t^s. Then*

$$\kappa_t^s(\hat{P}_t(k)) = \hat{P}_t(k - p^s)$$

where $P_t(k-p^s) = 0$ for $k < p^s$.

(ii) Let Θ be an element in B_t which gives zero when stripped by P_t^s, and assume $\Theta \cdot \hat{P}_t(ip^s) \cdot (P_t^s)^m = 0$. Then $\Theta \cdot \hat{P}_t((i-1)p^s) \cdot (P_t^s)^{m+1} = 0$.

Proof: (i) We will prove it by induction on k. Note that

$$\sum_{n \in Z} P_t(n) \cdot \chi(P_t(k-n)) = 0.$$

Hence we have

$$\sum_{n \in Z} (-1)^{k-n} P_t(n) \cdot \hat{P}_t(k-n) = 0 \tag{3.17}$$

with the convention that $P_t(i) = 0$ and $\hat{P}_t(i) = 0$ if $i < 0$. Applying the derivation κ_t^s to (3.17), we have

$$\kappa_t^s(\hat{P}_t(k)) + \sum_{n>0}(-1)^n\{\kappa_t^s(P_t(n)) \cdot \hat{P}_t(k-n) + P_t(n) \cdot \kappa_t^s(\hat{P}_t(k-n))\} = 0.$$

By the induction hypothesis, we obtain

$$\kappa_t^s(\hat{P}_t(k)) + \sum_{n\neq 0}(-1)^n P_t(n-p^s) \cdot \hat{P}_t(k-n) + \sum_{m\neq p^s}(-1)^{m-p^s} P_t(m-p^s) \cdot \hat{P}_t(k-m) = 0.$$

All terms cancel except the term with $n = p^s$ in the first sum. Hence

$$\kappa_t^s(\hat{P}_t(k)) = \hat{P}_t(k-p^s).$$

This completes the induction.

(ii) If $\Theta \cdot \hat{P}_t(ip^s) \cdot (P_t^s)^m = 0$ then

$$\kappa_t^s(\Theta) \cdot \hat{P}_t(ip^s) \cdot (P_t^s)^m + \Theta \cdot \kappa_t^s(\hat{P}_t(ip^s)) \cdot (P_t^s)^m + \Theta \cdot \hat{P}_t(ip^s) \cdot \kappa_t^s\,(P_t^s)^m = 0.$$

By part (i),

$$\Theta \cdot \hat{P}_t((i-1)p^s) \cdot (P_t^s)^m + m\Theta \cdot \hat{P}_t(ip^s) \cdot (P_t^s)^{m-1} = 0.$$

So

$$\Theta \cdot \hat{P}_t((i-1)p^s) \cdot (P_t^s)^{m+1} = -m\Theta \cdot \hat{P}_t(ip^s) \cdot (P_t^s)^m = 0. \quad \blacksquare$$

Let E be the exterior sub-algebra of A generated by $\{P_t^0 | t \geq 1\}$. There is an algebra isomorphism between A and $A//E$. This isomorphism $F : A \longrightarrow A//E$ is given by

$$F\,(P(t_1, t_2, t_3 \ldots)) = [P(pt_1, pt_2, pt_3 \ldots)]$$

where $[x]$ is equivalence class in $A//E$ of $x \in A$ (see [14]). Suppose $(P_t^s)^n = 0$. Then $[0] = [P_t^s]^n = F((P_t^{s-1})^n)$. Since F is an algebra isomorphism, $(P_t^{s-1})^n = 0$. So by iterating we see that if $(P_t^s)^n = 0$ then $(P_t^i)^n = 0$ for all $i \leq s$. This proves the following lemma.

Lemma 3.1.14 *Let $t > 1$.*

(i) If Theorem 3.1.1(i) holds for all $s \equiv -1 \bmod t$, then it holds for all s.

(ii) If Theorem 3.1.1(ii) holds for all $s \equiv 0 \bmod t$, then it holds for all s.

3.2 The Proof of The Main Result

The proof the Theorem 3.1.1(i) now follows by imitating the proof of [17] for the case $p = 2$. We proceed by proving the following two equations by induction on k for $1 \leq k \leq m$.

$$\chi((X_t)_{kt-1}^{mt-1}) \cdot \left(P_t^{mt-1}\right)^{p(k-1)+1} = 0 \tag{3.18}$$

$$\chi((X_t)_{kt-1}^{(m-1)t-1}) \cdot \left(P_t^{mt-1}\right)^{pk} = 0. \tag{3.19}$$

If $k = 1$ then

$$\chi((X_t)_{t-1}^{mt-1}) \cdot P_t^{mt-1} = P_t\left((p-1)p^{t-1}\gamma_t(m)\right) \cdot P_t^{mt-1} = 0$$

by Lemma 3.1.12 and Proposition 3.1.4.

Next we show that equation (3.18) for k implies equation (3.19) for k. The assumption says that

$$\chi((X_t)_{kt-1}^{(m-1)t-1})\chi(P_t(P^{mt-1}(p-1)))\left(P_t^{mt-1}\right)^{p(k-1)+1} = 0.$$

On applying Lemma 3.1.13 $(p-1)$ times with $\Theta = \chi((X_t)_{kt-1}^{(m-1)t-1})$, we obtain

$$\chi((X_t)_{kt-1}^{(m-1)t-1}) \cdot \left(P_t^{mt-1}\right)^{pk} = 0,$$

as desired.

Now we show that equation (3.19) for k implies equation (3.18) for $k+1$. Indeed we have the following equations with $z = p^{mt} - p^{kt-1}(p-1)$. At the second step we use Corollary 3.1.8 with $a = mt-1$, $b = 1$, and $c = kt-1$. The induction hypothesis is used at the third step.

$$\begin{aligned}
\chi((X_t)_{(k+1)t-1}^{mt-1}) \cdot \left(P_t^{mt-1}\right)^{pk+1} &= \chi((X_t)_{kt-1+t}^{mt-1}) \cdot (P_t^{mt-1}) \cdot \left(P_t^{mt-1}\right)^{pk} \\
&= P_t(z) \cdot \chi((X_t)_{kt-1}^{mt-1-t}) \cdot \left(P_t^{mt-1}\right)^{pk} \\
&= P_t(z) \cdot 0 = 0.
\end{aligned}$$

Thus by induction on k we see that both equation (3.18) and (3.19) hold for $1 \leq k \leq m$. Equation (3.19) for $k = m$ proves the theorem for all $s \equiv -1 \bmod t$. By Lemma 3.1.14(i) this proves Theorem 3.1.1(i).

Proof of Theorem 3.1.1(*ii*): We follow the method of Davis, using properties of the coproduct ϕ in A to find elements $\xi^{R_{m,t}(i)}$ in the dual algebra A^* for $i < pm$ such that

$$\langle \left(P_t^{(m-1)t}\right)^i, \xi^{R_{m,t}(i)} \rangle \neq 0. \tag{3.20}$$

If $i = kp + w$ with $0 \leq k \leq m-1$ and $0 \leq w \leq p-1$, then let

$$\xi^{R_{m,t}(i)} = \xi_t^{r_1(i)} \xi_{2t}^{r_2(i)} \cdots \xi_{(k+1)t}^{r_{k+1}(i)} \tag{3.21}$$

where $r_l(i) = a_l(i) + b_l(i)$ such that

$$a_l(i) = \begin{cases} (w-p+1)p^{(m-1)t} & \text{if } l = 1 \\ 0 & \text{if } l > 1 \end{cases}$$

and

$$b_l(i) = \begin{cases} (p-1)p^{(m-k-1)t} & \text{if } l = k+1 \\ (p^{t+1}-p+1)p^{(m-k-1)t} & \text{if } l = k \\ (p^t-1)p^{(m-l-1)t+1} & \text{if } 1 \leq l < k \end{cases}$$

For example,

1. for $k = 0$, $R_{m,t}(i) = (wp^{(m-1)t})$
2. for $k = 1$, $R_{m,t}(i) = ((w+1)p^{(m-1)t} - (p-1)p^{(m-2)t}, (p-1)p^{(m-2)t})$
3. for $k = 2$, $R_{m,t}(i) = ((w+1)p^{(m-1)t} - p^{(m-2)t+1}, p^{(m-2)t+1} - (p-1)p^{(m-3)t}, (p-1)p^{(m-3)t})$
4. for $k = 3$, $R_{m,t}(i) = ((w+1)p^{(m-1)t} - p^{(m-2)t+1}, (p^t-1)p^{(m-3)t+1}, p^{(m-3)t+1} - (p-1)p^{(m-4)t}, (p-1)p^{(m-4)t})$

The proof of (3.20) depends on the following calculation.

Lemma 3.2.1

$$\phi(\xi^{R_{m,t}(i)}) = (z\xi^{R_{m,t}(i-1)} + \xi') \otimes \xi_t^{p^{(m-1)t}} + \sum_j a_j \otimes b_j$$

where $b_j \neq \xi_t^{p^{(m-1)t}}$ *for all* j, ξ' *is divisible by* $\xi_t^{p^{(m-1)t+1}}$, *and* $z = w$ *if* $w > 0$, $z = 1$ *if* $w = 0$.

This implies (3.20), since it follows by induction on i that

$$\langle \left(P_t^{(m-1)t}\right)^i, \xi^{R_{m,t}(i)}\rangle = \langle \left(P_t^{(m-1)t}\right)^{i-1}, w\xi^{R_{m,t}(i-1)}\rangle \langle P_t^{(m-1)t}, \xi_t^{p^{(m-1)t}}\rangle \neq 0,$$

since the evaluation of ξ' on all elements of the subalgebra $A(mt-1)$ is zero. By Lemma 3.1.14(ii), this implies Theorem 3.1.1(ii).

Proof of Lemma 3.2.1 Let $R_{m,t}(i)$ be as in (3.21) above. Since we are only interested in terms of the form $A \otimes \xi_t^{p^{(m-1)t}}$, we will work mod terms involving ξ_{jt} for $j > 1$ in the second factor. So we have

$$\phi(\xi^{R_{m,t}(i)}) = \phi(\prod_{l=1}^{k+1} \xi_{lt}^{r_l(i)}) = \prod_{l=1}^{k+1} \phi(\xi_{lt})^{r_l(i)} \equiv \prod_{l=1}^{k+1} (\xi_{lt} \otimes 1 + \xi_{(l-1)t}^{p^t} \otimes \xi_t)^{r_l(i)}. \quad (3.22)$$

Note that

$$\sum_{l=1}^{k+1} r_l(i) = (w+1)p^{(m-1)t}.$$

We only want terms of the form $A \otimes \xi_t^{p^{(m-1)t}}$. When $w = 0$, the only such term is obtained from the product $\prod_{l=1}^{k+1} (\xi_{(l-1)t}^{p^t \cdot} \otimes \xi_t)^{r_l(i)}$ and hence

$$A = \prod_{l=1}^{k+1} \xi_{(l-1)t}^{p^t r_l(i)} = \prod_{l=1}^{k} \xi_{lt}^{p^t b_{l+1}(i)} = \prod_{l=1}^{k} \xi_{lt}^{b_l(i-1)} = \xi^{R_{m,t}(i-1)}$$

since $i - 1 = (k-1)p + p - 1$.

Suppose $w > 0$. The l-th factor of (3.22) can be written as

$$\begin{cases} (\xi_{(k+1)t}^{p^{(m-k-1)t}} \otimes 1 + \xi_{kt}^{p^{(m-k)t}} \otimes \xi_t^{p^{(m-k-1)t}})^{p-1} & \text{if } l = k+1 \\ (\xi_{kt}^{p^{(m-k-1)t}} \otimes 1 + \xi_{(k-1)t}^{p^{(m-k)t}} \otimes \xi_t^{p^{(m-k-1)t}})^{p^{t+1}-p+1} & \text{if } l = k \\ (\xi_{lt}^{p^{(m-l-1)t+1}} \otimes 1 + \xi_{(l-1)t}^{p^{(m-l)t+1}} \otimes \xi_t^{p^{(m-l-1)t+1}})^{p^t-1} & \text{if } 1 < l < k \\ (\xi_t^{p^{(m-2)t+1}} \otimes 1 + 1 \otimes \xi_t^{p^{(m-2)t+1}})^{(w+1)p^{t-1}-1} & \text{if } l = 1,\ 1 < k \\ (\xi_t^{p^{(m-2)t}} \otimes 1 + 1 \otimes \xi_t^{p^{(m-2)t}})^{(w+1)p^t-p+1} & \text{if } l = 1,\ k = 1 \end{cases}$$

We expand each of these factors. If we choose for each l the term with the j_l-th power of the second term, then we must have ($k \geq 2$)

$$j_1 p^{(m-2)t+1} + \sum_{l=2}^{k-1} j_l p^{(m-l-1)t+1} + j_k p^{(m-k-1)t} + j_{k+1} p^{(m-k-1)t} = p^{(m-1)t} \quad (3.23)$$

and $\binom{(m+1)p^{t-1}-1}{j_1}$ is a unit, $0 \le j_l \le p^t - 1$ for $2 \le l \le k-1$, $\binom{p^{t+1}-p+1}{j_k}$ is a unit, and $0 \le j_{k+1} \le p-1$.

To satisfy (3.23) we must have $j_{k+1} + j_k \equiv 0 \bmod p^{t+1}$. Since $\binom{p^{t+1}-p+1}{j_k}$ is a unit, either $j_k \equiv 0 \bmod p$ or $j_k \equiv 1 \bmod p$. Therefore either $j_{k+1} = 0$ or $p-1$ since $j_{k+1} \le p-1$.

If $j_{k+1} = 0$, then $j_k = 0$. So we have following equation

$$j_1 p^{(m-2)t+1} + \sum_{l=2}^{k-1} j_l p^{(m-l-1)t+1} = p^{(m-1)t}. \tag{3.24}$$

Since $j_{k-1}p^{(m-k)t+1} \equiv 0 \bmod p^{(m-k+1)t+1}$, j_{k-1} is multiple of p^t. Therefore $j_{k-1} = 0$ since $j_{k-1} \le p^t - 1$. By a similar argument, $j_{k-2} = j_{k-3} = \cdots = j_2 = 0$. So we have $j_1 p^{(m-2)t+1} = p^{(m-1)t}$ which implies $j_1 = p^{t-1}$. Therefore we obtain a term of the form $A \otimes \xi_t^{p^{(m-1)t}}$ with $A = A_1 A_2 \cdots A_k A_{k+1}$ where

$$\begin{aligned}
A_1 &= w\xi_t^{wp^{(m-1)t} - p^{(m-2)t+1}} \\
A_2 &= \xi_{2t}^{(p^t-1)p^{(m-3)t+1}} \\
&\cdots \\
A_{k-1} &= \xi_{(k-1)t}^{(p^t-1)p^{(m-k)t+1}} \\
A_k &= \xi_{kt}^{(p^{t+1}-p+1)p^{(m-k-1)t}} \\
A_{k+1} &= \xi_{(k+1)t}^{(p-1)p^{(m-k-1)t}}.
\end{aligned}$$

Hence $A = \xi^{R_{m,t}(i-1)}$.

If $j_{k+1} = p-1$, then we have $j_k = p^{t+1} - p + 1$. From (3.23),

$$j_1 p^{(m-2)t+1} + \sum_{l=2}^{k-2} j_l p^{(m-l-1)t+1} + j_{k-1}p^{(m-k)t+1} + p^{(m-k)t+1} = p^{(m-1)t}.$$

So $j_{k-1} \equiv -1 \bmod p^t$. Hence $j_{k-1} = p^t - 1$ since $j_{k-1} \le p^t - 1$. By a similar argument, $j_{k-2} = j_{k-3} = \cdots = j_2 = p^t - 1$. If we put these j_l in the equation (3.23) for $2 \le l \le k-2$, we will have $(j_1 + 1)p^{(m-2)t+1} = p^{(m-1)t}$. This implies that $j_1 = p^{t-1} - 1$. Therefore we obtain the other term of the form $B \otimes \xi_t^{p^{(m-1)t}}$ with

Chapter 4

Nilpotence Of Certain $P(n)$

4.1 The Main Results

In this chapter we shall adapt to odd primes results proved by Monks [17] and find formulas for nilpotence of certain $P(n)$.

Theorem 4.1.1 *Suppose* $r_i \equiv p-1 \bmod p$ *for* $1 \leq i \leq m$. *Then*

(*i*) $Nil(P(r_1,\ldots,r_m) \leq \min\{k | r_m < p^{(k-1)m+1}-1\}$.

(*ii*) $Nil(P(r_1,\ldots,r_m)) = Nil(P(p^k r_1 + p^k - 1,\ldots,p^k r_{m-1} + p^k - 1, p^k r_m - \frac{p^k-1}{p-1}))$ *for all* $k \in N$.

Theorem 4.1.2 (*i*) *For* $m \geq 0$, $k \geq 1$,

$$Nil(P(\frac{p^k((p-1)p^m-1)+1}{p-1})) = m+2.$$

(*ii*) *For* $m \geq 0$,

$$Nil(P(p^m-1)) = m+1.$$

Theorem 4.1.3 *For* $n \geq 2$,

$$Nil(P(n)) = \begin{cases} [\frac{p}{n}]+1 & \text{if } n < p \\ 2p & \text{if } n = p. \end{cases}$$

For any integer l, let

$$\nu_p(l) = \min\{m | l \equiv 0 \bmod p^m\}.$$

Proposition 4.1.4 *If $l \equiv -1 \bmod p$, then $Nil(P(l)) > \nu_p(l+1)$.*

Our method of proving this involves introducing sub-algebras O_k of $\mathcal{A}$ defined as follows:

Definition 4.1.5 *O_k is the Z_p-subspace of $\mathcal{A}$ whose basis is the set of Milnor basis elements*

$$B_k = \{P(r_1, r_2, \ldots, r_m) \ : \ r_i \equiv -1 \bmod p^{k+1} \text{ for } i < m \text{ and } (p-1)r_m \equiv 1 \bmod p^{k+1}\}.$$

We will denote $\mathcal{O} = O_0$.

The following two results will be proved later.

Proposition 4.1.6 *O_k is a subalgebra of A for all $k \in N$.*

Proposition 4.1.7 *There is an algebra monomorphism $\lambda : \mathcal{O} \to \mathcal{O}$ defined by*

$$\lambda(P(r_1, r_2, \ldots, r_m)) = P(pr_1 + p - 1, pr_2 + p - 1, \ldots, pr_{m-1} + p - 1, pr_m - 1).$$

If $\lambda^{(0)}$ is the identity map on $\mathcal{O}$, and $\lambda^{(k)} = \lambda \circ \lambda^{(k-1)}$ for $k > 1$, then $\lambda^{(k)}$ is also a monomorphism for every k. It is easy to check that

$$\lambda^{(k)}(P(r_1, r_2, \ldots, r_m)) = P(p^k r_1 + p^k - 1, \ldots, p^k r_{m-1} + p^k - 1, p^k r_m - \frac{p^k - 1}{p - 1}).$$

From the definition of λ, we have $\lambda(O_k) = O_{k+1}$, and hence the restriction of λ to O_k is an isomorphism between O_k and O_{k+1}. Therefore for any $a \in \mathcal{O}$ the nilpotence of a is equal to the nilpotence of $\lambda^{(k)}(a)$ for $k \in N$. This explanation proves part (ii) of Theorem 4.1.1.

Let $n = \sum_{i=0}^{\infty} \alpha_i(n) p^i$ be the p-adic expansion of an integer n where $0 \leq \alpha_i(n) < p$.

Lemma 4.1.8 *Let $m = \sum_i \alpha_i(m)p^i$ and $n = \sum_i \alpha_i(n)p^i$ be p-adic expansions. Then*

$$\binom{m}{n} \equiv \prod_i \binom{\alpha_i(m)}{\alpha_i(n)} \pmod{p}.$$

Proof: Note that

$$(1+x)^m = (1+x)^{\sum_i \alpha_i(m)p^i} \equiv (1+x^{p^i})^{\sum_i \alpha_i(m)} = \prod_i (1+x^{p^i})^{\alpha_i(m)} = \prod_i \sum_j \binom{\alpha_i(m)}{j} x^{j \cdot p^i}$$

From this observation, the coefficient $\binom{m}{n}$ of x^n in the expansion $(1+x)^m$ is equivalent to

$$\prod_i \binom{\alpha_i(m)}{\alpha_i(n)}. \quad \blacksquare$$

Corollary 4.1.9 $(n_1, n_2, \ldots, n_k) \equiv (pn_1 + p - 1, pn_2, \ldots, pn_j, \ldots, pn_k) \bmod p.$

Proof: For $l \leq k$, let $S_l = n_l + n_{l+1} + \cdots + n_k$. Then using Lemma 4.1.8, we have

$$\begin{aligned}(n_1, n_2, \ldots, n_k) &= \binom{S_1}{n_1} \cdot \binom{S_2}{n_2} \cdots \binom{S_{k-1}}{n_{k-1}} \\ &\equiv \binom{pS_1+p-1}{pn_1+p-1} \cdot \binom{pS_2}{pn_2} \cdots \binom{pS_{k-1}}{pn_{k-1}} \bmod p \\ &= (pn_1 + p - 1, pn_2, \ldots, pn_k). \quad \blacksquare\end{aligned}$$

Lemma 4.1.10 *Let $P(r_1, r_2, \ldots, r_m), P(s_1, s_2, \ldots, s_n) \in \mathcal{O}$. If $\beta(X)P(t_1, t_2, \ldots, t_l)$ is a nonzero term in $P(r_1, r_2, \ldots, r_m) \cdot P(s_1, s_2, \ldots, s_n)$, then*

$$P(t_1, t_2, \ldots, t_l) \in \mathcal{O}, \tag{4.1}$$

$$l = m + n, \tag{4.2}$$

and

$$x_{ij} \equiv \begin{cases} 0 \bmod p & \text{if } j > 0 \text{ and } i < m \\ p - 1 \bmod p & \text{if } j = 0,\ i \leq m \text{ or } i = m,\ j \leq n. \end{cases} \tag{4.3}$$

Proof: By (2.3), we have

$$r_i = \sum_j p^j x_{ij}.$$

Since $P(r_1, r_2, \ldots, r_m) \in \mathcal{O}$, $r_i \equiv p-1 \bmod p$ for $i \leq m$. Hence $x_{i0} \equiv p-1 \bmod p$ for $i \leq m$. When we combine this result with (2.5) and Corollary 4.1.9, we have $x_{ij} \equiv 0 \bmod p$ for $i+j \leq m$ and $j > 0$. Let $d < n$ and assume that $x_{mj} \equiv p-1 \bmod p$ for $0 < j \leq d$, and $x_{ij} \equiv 0 \bmod p$ for $i+j \leq m+d$, $j > 0$, and $i < m$. Since $P(s_1, s_2, \ldots, s_n) \in \mathcal{O}$, $s_{d+1} \equiv p-1 \bmod p$. Hence $x_{m,d+1} \equiv p-1 \bmod p$ by (2.2). Using (2.5) again, $x_{ij} \equiv 0 \bmod p$ for $i+j = m+d+1$ and $j > d+1$. Thus by finite induction on d, we have shown that $x_{ij} \equiv p-1 \bmod p$ if and only if $j = 0$, $i \leq m$ or $i = m$, $j \leq n$.

By (2.3), $P(t_1, t_2, \ldots, t_l) \in \mathcal{O}$ and $t_l = x_{mn} \equiv p-1 \bmod p$, $m+n = l$. ■

4.2 The Proof of The Main Results

Proof of Proposition 4.1.7: It is convenient to define $\lambda(R)$ by

$$\lambda(r_1, r_2, \ldots, r_m) = (pr_1 + p - 1, pr_2 + p - 1, \ldots, pr_{m-1} + p - 1, pr_m - 1).$$

It is easy to check that λ is injective. It remains to show that λ is a homomorphism. Let $R = (r_1, r_2, \ldots, r_m)$, $S = (s_1, s_2, \ldots, s_n)$, and $T = (t_1, t_2, \ldots, t_{m+n})$. Let $\hat{X} = (\hat{x}_{ij})$ be a $(\lambda(R), \lambda(S))$-allowable matrix. Using the proof of Lemma 4.0.11, we have $\hat{x}_{ij} \equiv p-1 \bmod p$ if and only if $j = 0$, $i \leq m$ or $i = m$, $j \leq n$. So we can define

$$\hat{x}_{ij} = \begin{cases} px_{ij} + p - 1 & \text{if } j = 0,\ i \leq m \text{ or } i = m\ ,\ j < n \\ px_{ij} - 1 & \text{if } j = n,\ i = m \\ px_{ij} & \text{otherwise.} \end{cases}$$

So we would like to show that $\hat{X} = (\hat{x}_{ij})$ is $(\lambda(R), \lambda(S))$-allowable if and only if $X = (x_{ij})$ is (R, S)-allowable, and that $\beta(X) = \beta(\hat{X})$.

Define

$$\epsilon_j = \begin{cases} p-1 & \text{if } j < n \\ -1 & \text{if } j = n \end{cases}$$

Let $\lambda(P(S)) = P(\hat{s}_1, \hat{s}_2, \ldots, \hat{s}_n)$ where $\hat{s}_j = p \cdot s_j + \epsilon_j$. We will check condition (2.2).

$$\sum_{i=0}^{m} \hat{x}_{ij} = \hat{s}_j \iff \sum_{i=0}^{m-1} p \cdot \hat{x}_{ij} + p \cdot x_{mj} + \epsilon_j = p \cdot s_j + \epsilon_j \iff \sum_{i=0}^{m} x_{ij} = s_j.$$

Let $\lambda(P(R)) = P(\hat{r}_1, \hat{r}_2, \ldots, \hat{r}_m)$ where $\hat{r}_i = p \cdot r_i + p - 1$ for $1 \leq i < m$ and $\hat{r}_m = p \cdot r_m - 1$. If $1 \leq i < m$, then

$$\sum_{j=0}^{n} p^j \cdot \hat{x}_{ij} = \hat{r}_i \iff \sum_{j=1}^{n} p^{j+1} \cdot x_{ij} + p \cdot x_{i0} + p - 1 = p \cdot r_i + p - 1 \iff \sum_{j=0}^{n} p^j \cdot x_{ij} = r_i.$$

If $i = m$, then

$$\sum_{j=0}^{n} p^j \cdot \hat{x}_{mj} = \hat{r}_m \iff \sum_{j=0}^{n-1} p^j \cdot (p \cdot x_{mj} + p - 1) + p^n(p \cdot x_{mn} - 1) = pr_m - 1$$

$$\iff \sum_{j=0}^{n-1} p^{j+1} \cdot x_{mj} + (p-1) \sum_{j=0}^{n-1} p^j + p^{n+1} x_{mn} - p^n = pr_m - 1$$

$$\iff \sum_{j=0}^{n} p^j x_{mj} = r_m.$$

So condition (2.3) holds for both $\hat{X}$ and X.

By Corollary 4.1.9, $(a_1, a_2, \ldots, a_h) \equiv (p \cdot a_1 + \gamma_1, p \cdot a_2 + \gamma_2, \ldots, p \cdot a_h + \gamma_h) \bmod p$ where $\gamma_i = p - 1$ for at most one $1 \leq i \leq h$ and is zero otherwise. Hence

$$\prod_h (x_{h,0}, x_{h-1,1}, \ldots, x_{0,h}) \equiv \prod_h (\hat{x}_{h,0}, \hat{x}_{h-1,1}, \ldots, \hat{x}_{0,h}) \pmod{p}.$$

Let $P(t_1, t_2, \ldots t_{m+n})$ be the summand of $P(R) \cdot P(S)$ associated with X and let $P(\hat{T}) = P(\hat{t}_1, \hat{t}_2, \ldots \hat{t}_{m+n})$ be the summand of $\lambda(P(R)) \cdot \lambda(P(S))$ associated with $\hat{X}$. Then for $h < m + n$,

$$\hat{t}_h = \sum_{i+j=h} \hat{x}_{ij} = \sum_{i+j=h} p \cdot x_{ij} + p - 1 = p \cdot t_h - 1$$

and

$$\hat{t}_{mn} = \hat{x}_{mn} = p \cdot x_{mn} - 1 = p \cdot t_{mn} - 1.$$

Therefore $P(\hat{T}) = \lambda(P(T))$. ■

Proof of Proposition 4.1.6:

By lemma 4.1.10 , $x \cdot y \in \mathcal{O}$ for all $x, y \in B_0$. Since $\lambda^{(k)}(\mathcal{O}) = O_k$ and λ is an algebra homomorphism, the result holds. ■

Proof of Theorem 4.1.1(ii):

Let $P(T) = P(t_1, \ldots, t_l)$ be any summand of $P(r_1, \ldots, r_m)^{k-1} = P(R)^{k-1}$ with nonzero coefficient. By Lemma 4.1.10, we have $l = (k-1)m$. Let $X = (x_{ij})$ be any (R, S)-allowable matrix with nonzero coefficient. As shown in the proof of Lemma 4.1.10 , $x_{ij} \equiv p-1 \bmod p$ if $i = m$ and $j \leq (k-1)m$. From this and (2.5), we have

$$r_m = \sum_{j=0}^{(k-1)m} p^j \cdot x_{m,j} \geq \sum_{j=0}^{(k-1)m} (p-1)p^j = p^{(k-1)m+1} - 1.$$

Hence when $r_m < p^{(k-1)m+1} - 1$, an (R, S)-allowable matrix with nonzero coefficient does not exist. Therefore $P(R)^k = 0$. ■

Proof of Proposition 4.0.4: Let $l = p^m a - 1$ where a is not divisible by p. For each $1 \leq h \leq m$, we can define $S_{l,h} = (s_{l,h,1}, s_{l,h,2}, \ldots, s_{l,h,h})$ by

$$s_{l,h,i} = \begin{cases} (p-1)(p^{m-i}a + 1) & \text{if } 1 \leq i < h \\ p^{m-h+1}a - 1 & \text{if } i = h. \end{cases}$$

We shall prove that $\beta(Y)P(S_{l,h})$ is a nonzero term in $P(l)^h$ for $1 \leq h \leq m$ by induction on h, where $Y = (y_{ij})$ is the matrix associated with $P(l)P(l)^{h-1}$, and hence $P(l)^m \neq 0$.

If $h = 1$, then $P(S_{l,1})$ is a nonzero term in $P(l)$. By induction hypothesis, assume that $P(S_{l,h})$ has a nonzero coefficient in $P(l)^h$ for $h < m$. Suppose that $P(S_{l,h+1})$ is a nonzero term in $P(l)P(R)$ for some $P(R) = P(r_1, r_2, \ldots, r_h)$ such that $P(R)$ is a nonzero term in $P(l)^h$. Let $X = (x_{ij})$ be the associated matrix. By (2.4), we have $x_{1h} = s_{l,h+1,h+1} = p^{m-h}a - 1$ and from (2.3)

$$l = \sum_{j=0}^{h} x_{1j}p^j = \sum_{j=0}^{h-1} x_{1j}p^j + p^m a - p^h$$

and hence $\sum_{j=0}^{h-1} x_{1j}p^j = p^h - 1$. By (4.3), we have $x_{1j} \equiv p-1 \bmod p$. Since $\sum_{j=0}^{h-1} x_{1j}p^j = p^h - 1$, (2.3) holds if and only if $x_{1j} = p-1$ for $1 \leq j < h$. However by (2.2) and (2.4), for $1 \leq j < h$ we have

$$r_j = x_{0j} + x_{1j} = (s_{l,h+1,j} - p + 1) + p - 1 = (p-1)p^{m-j}a + p - 1 = s_{l,h,j}$$

and

$$\begin{aligned} r_h &= x_{0h} + x_{1h} = (s_{l,h+1,h} - p + 1) + s_{l,h+1,h+1} \\ &= (p-1)(p^{m-h}a + 1) - p + 1 + p^{m-(h+1)+1}a - 1 \\ &= p^{m-h+1}a - 1 = s_{l,h,h}. \end{aligned}$$

So we have proved that if $\beta(X)P(S_{l,h+1})$ is a nonzero term in $P(l)P(R)$, then $P(R) = P(S_{l,h})$. Moreover by our construction, the conditions (2.2) and (2.3) hold for the matrix X associated with $P(l)P(R)$. Since $s_{l,h,j} \equiv p-1 \bmod p$, the multinomial coefficient $(p-1, s_{l,h,j} - p + 1)$ is a unit. Therefore $P(S_{l,h+1})$ has nonzero coefficient in $P(l)P(S_{l,h})$ extending the induction. ■

Proof of Theorem 4.1.2(ii): We know that $Nil(P(p^m-1)) \leq m+1$ by Theorem 4.1.1(i) and $Nil(P(p^m - 1)) > m$ by Proposition 4.1.3. Hence $Nil(P(p^m - 1)) = m + 1$. ■

Proof of Theorem 4.1.2(i): For $k \geq 1$, $m \geq 0$, we have

$$\lambda^{(k-1)}(P(p^{m+1} - 1)) = P(p^{k-1}(p^{m+1} - 1) - \frac{p^{k-1} - 1}{p-1}) = P(\frac{p^k((p-1)p^m - 1) + 1}{p-1}).$$

Thus using Theorem 4.1.1(ii) and Theorem 4.1.2(ii),

$$Nil(P(\frac{p^k((p-1)p^m - 1) + 1}{p-1})) = Nil(P(p^{m+1} - 1)) = m + 2. \quad ■$$

Proof of Theorem 4.1.3: When $n = p$, it is proved by Walker and Wood (see [29]).

Let $n < p$. Claim $P(n)^j = uP(nj)$ if $nj < p$ where u is nonzero. We will prove this by induction on j.

If $j = 1$, it is true. Suppose the statement is true for $j - 1$. By induction hypothesis,

$$P(n)^j = P(n)P(n)^{j-1} = uP(n)P(n(j-1)).$$

Since $n < p$, $P(n)^j = u\binom{jn}{n}P(jn)$.

Suppose $j = [\frac{p}{n}] + 1$. Then $nj \geq p$. By our claim, $P(n)^{j-1} = uP((j-1)n)$. Then $P(n)^j = P(n)P(n)^{j-1} = uP(n)P((j-1)n)$. Since $nj \geq p$,

$$P(n)^j = u\binom{jn}{n}P(jn) = 0 \bmod p.$$

This completes the proof. ■

Chapter 5

On The Action of Steenrod Operations In Polynomial Algebras

5.1 The Main Results

Let $P_s = Z_p[x_1, x_2, \ldots, x_s]$. A polynomial $N \in P_s$ is said to be hit if it is in the image of the action $\bar{A} \otimes P_s \longrightarrow P_s$, i.e. $N \in \bar{A}P_s$ where $\bar{A}$ is the augmentation ideal of $\mathcal{A}$, i.e. $N = \sum_i P^i M_i$ for some $M_i \in P_s$.

We are interested in determining the image of the action $\bar{A} \otimes P_s \longrightarrow P_s$: the space of elements in P_s that are hit by positive dimensional Steenrod operations. In [30], when $p = 2$ Wood showed that if $\alpha(d+s) > s$ then every polynomial of degree d in P_s is hit where $\alpha(d+s)$ denotes the number of ones in the binary expansion of $d+s$. In [23] Singer generalized Wood's result conjectured by Peterson and identified a larg er class of hit polynomials. In [22] Silverman generalized a result of Wood and proved a conjecture of Singer. In [19] Monks extended a result of Wood to determine a new family of hit polynomials in P_s.

The following results are odd-primary analogues of results of Monks [19].

Theorem 5.1.1 *Let H and K be polynomials of degree $2h$, $2k$ respectively. If $h <$*

$\mu_t(k)$, *then* HK^{p^t} *is hit.*

Theorem 5.1.2 *For* $s, t \geq 1$, $0 \leq k < s$, *and* $k < t$,

$$\widehat{P_t}(p^s - p^k) = P_t((p-1)p^{s-1})P_t((p-1)p^{s-2}) \cdots P_t((p-1)p^k).$$

We list some lemmas we need to prove Theorem 5.1.1 and Theorem 5.1.2. Most of these lemmas involve the function μ_t defined in Definition 3.1.10. The following lemma is analogous to Lemma 2.1 in [19].

Lemma 5.1.3 *For all* $t, m \geq 1$, $\mu_t(m) \leq \frac{p^t-1}{p-1}\mu_1(m)$.

Proof: There exist positive integers $l_1, l_2, \ldots, l_{\mu_1(m)}$ such that

$$m = \sum_{i=1}^{\mu_1(m)} \gamma_1(l_i).$$

For each l_i, let $l_i = tq_i + r_i$ where q_i and r_i are non-negative integers and $0 \leq r_i < t$.

$$\begin{aligned} m &= \textstyle\sum_{i=1}^{\mu_1(m)} \gamma_1(l_i) = \sum_{i=1}^{\mu_1(m)} \frac{p^{tq_i+r_i}-1}{p-1} \\ &= \textstyle\sum_{i=1}^{\mu_1(m)} [\frac{p^t-p^{r_i}}{p-1}\frac{p^{tq_i}-1}{p^t-1} + \frac{p^{r_i}-1}{p-1}\frac{p^{t(q_i+1)}-1}{p^t-1}] \\ &= \textstyle\sum_{j=1}^{\frac{p^t-p^{r_i}}{p-1}} \sum_{i=1}^{\mu_1(m)} \gamma_t(q_i) + \sum_{j=1}^{\frac{p^{r_i}-1}{p-1}} \sum_{i=1}^{\mu_1(m)} \gamma_t(q_i+1) \end{aligned}$$

This yields a t-decomposition of m with $\frac{p^t-1}{p-1}\mu_1(m)$ terms. This completes the proof. ■

Lemma 5.1.4 *If* $m \leq p^t$ *then* $\mu_t(m) = m$.

Proof: Let $m \leq p^t$. Then $m \leq p^t < p^t + 1 = \gamma_t(2)$. The only possible t-decomposition of m is a sequence of m ones because γ_t is strictly increasing. ■

Let $L = (l_1, l_2, \ldots, l_n)$ be any sequence of nonnegative integers. Define

$$|L| = \sum_{i=1}^{n} l_i \tag{5.1}$$

$$\nu(L) = \max_i l_i \tag{5.2}$$

and

$$Y_t(L) = \sum_{i=1}^{n} \gamma_t(l_i). \tag{5.3}$$

Suppose that $l_1 \geq l_2 \geq \cdots \geq l_n$ and that $|L| \geq 1$. For this sequence, we can define

$$\delta(L) = (l_1', l_2', \ldots, l_n') \tag{5.4}$$

where

$$l_i' = \begin{cases} l_i - 1 & \text{if } l_i = l_1 \text{ and } (l_{i+1} \neq l_1 \text{ or } i = n) \\ l_i & \text{if otherwise.} \end{cases} \tag{5.5}$$

It is easy to verify that

$$l_1' \geq l_2' \geq \cdots \geq l_n' \tag{5.6}$$

$$|\delta(L)| = |L| - 1 \tag{5.7}$$

$$\nu(\delta(L)) \leq \nu(L) \tag{5.8}$$

and

$$Y_t(\delta(L)) = Y_t(L) - p^{t(\nu(L)-1)}. \tag{5.9}$$

We can define δ^r to be the r-fold composition of δ with itself (δ^0 is the identity function) for $0 \leq r \leq |L|$. Let $F_L = (f_1, f_2, \ldots, f_{|L|})$ be the sequence given by

$$f_i = Y_t(\delta^{i-1}(L)) - Y_t(\delta^i(L)). \tag{5.10}$$

Since $\delta^{|L|}(L) = (0, 0, \ldots, 0)$ and $Y_t(\delta^{|L|}(L)) = 0$,

$$\begin{aligned} |F_L| &= \textstyle\sum_{i=1}^{|L|} [Y_t(\delta^{i-1}(L)) - Y_t(\delta^i(L))] = Y_t(\delta^0(L)) - Y_t(\delta^{|L|}(L)) \\ &= Y_t(L). \end{aligned} \tag{5.11}$$

Lemma 5.1.5 *If $m < (p-1)p^s$, then $\mu_t(m) \leq \mu_t(m + (p-1)p^s)$.*

Proof: Assume that $L = (l_1, l_2, \ldots, l_n)$ is a t-decomposition of $m + (p-1)p^s$. Without loss of generality we can also assume that $l_1 \geq l_2 \geq \cdots \geq l_n$. By definition we have $Y_t(L) = m + (p-1)p^s$ and so by (5.11)

$$\sum_{i=0}^{|L|} f_i = m + (p-1)p^s.$$

So F_K is a non-increasing sequence whose power is $m+(p-1)p^s$. We need following lemma

Lemma 5.1.6 *If* $(p-1)p^b \leq a < p^{b+1}$, $\sum_{i=1}^{r} p^{x_i} = a$, *and* $p^{x_1} \geq p^{x_2} \geq \cdots \geq p^{x_r}$ *then there is a* $q \in \{1, \ldots, r\}$ *such that* $\sum_{i=1}^{q} p^{x_i} = (p-1)p^b$.

Proof: If $a = (p-1)p^b$ then we can take $q = r$ and we are done. Assume that $(p-1)p^b < a$. Since $p^{b+1} > a$, we have $p^b \geq p^{x_1} \geq p^{x_2} \geq \cdots \geq p^{x_{q+1}}$. Let q be the largest integer such that $\sum_{i=1}^{q} p^{x_i} \leq (p-1)p^b$. Then $(p-1)p^b - \sum_{i=1}^{q} p^{x_i} \equiv 0 \bmod p^{x_{q+1}}$ and $(p-1)p^b < \sum_{i=1}^{q+1} p^{x_i}$ and hence $\sum_{i=1}^{q} p^{x_i} = (p-1)p^b$. ■

From Lemma 5.1.6 there exists $q \in \{1, \ldots, |L|\}$ such that $\sum_{i=1}^{q} f_i = (p-1)p^s$. Thus

$$\sum_{i=1}^{q} [Y_t(\delta^{i-1}(L)) - Y_t(\delta^i(L))] = Y_t(L) - Y_t(\delta^q(L)) = m + (p-1)p^s - Y_t(\delta^q(L)) = (p-1)p^s$$

and hence $Y_t(\delta^q(L)) = m$. Therefore $\mu_t(m) \leq \mu_t(m + (p-1)p^s)$. ■

Using this result we can prove

Lemma 5.1.7 $\mu_t(p^s - p^k) \geq (p-1)p^k$ *where* s, t, *and* k *are any integers such that* $s, t \geq 1$, $0 \leq k < s$, *and* $k < t$.

Proof: We will prove it by induction on s. If $s = k+1$ then $\mu_t(p^s - p^k) = \mu_t((p-1)p^k) = (p-1)p^k$ by Lemma 5.1.4. Assume that it is true for $s-1$. Then by Lemma 5.1.5, $\mu_t(p^s - p^k) = \mu_t((p-1)p^{s-1} + p^{s-1} - p^k) \geq \mu_t(p^{s-1} - p^k)$. By inductive hypothesis, $\mu_t(p^{s-1} - p^k) \geq (p-1)p^k$. Hence $\mu_t(p^s - p^k) \geq (p-1)p^k$. ■

5.2 The Proof of The Main Results

The key idea in Wood's argument which is that for any $u, w \in P_s$ and any $\theta \in \mathcal{A}$, we have $u \cdot \theta w \equiv \widehat{\theta} u \cdot w$ modulo hit elements. In particular, if $e(\widehat{\theta}) > \deg(u)$, then $u \cdot \theta w$ is hit. Using this we will prove Theorem 5.1.1. We accomplish this with the aid of the following lemma.

Lemma 5.2.1 *If $N \in P_s$ is any element of degree $2k$, then for any $t \geq 1$,*

$$P_t(k) \cdot N = N^{p^t}. \tag{5.12}$$

Proof: We will prove this by induction on the number of variables in N. Suppose

$$N = x_{i_1}^{h_1} x_{i_2}^{h_2} \cdots x_{i_n}^{h_n}.$$

Let $n = 1$. Then

$$P_t(k)x^k = (x^k)^{p^t}. \tag{5.13}$$

So the result holds for $n = 1$. Assume that the result holds for all monomials comprised of less than n variables. Let $N_1 = x_{i_1}^{h_1} x_{i_2}^{h_2} \cdots x_{i_{n-1}}^{h_{n-1}}$ so that $N = N_1 x_{i_n}^{h_n}$. Let $\psi : \mathcal{A} \longrightarrow \mathcal{A} \otimes \mathcal{A}$ be the diagonal map of $\mathcal{A}$. Then $\psi(P_t(k)) = \sum_{i=0}^{k} P_t(k-i) \otimes P_t(i)$. So

$$\begin{aligned} P_t(k) \cdot N &= \textstyle\sum_{i=0}^{k} P_t(k-i)N_1 \cdot P_t(i)x_{i_n}^{h_n} \\ &= \textstyle\sum_{i=0}^{h_n-1} P_t(k-i)N_1 \cdot P_t(i)x_{i_n}^{h_n} + P_t(k-h_n)N_1 \cdot P_t(h_n)x_{i_n}^{h_n} \\ &\quad + \textstyle\sum_{i=h_n+1}^{k} P_t(k-i)N_1 \cdot P_t(i)x_{i_n}^{h_n}. \end{aligned}$$

Since $e(P_t(k-i)) > \frac{1}{2}\deg(N_1)$, $\sum_{i=0}^{h_n-1} P_t(k-i)N_1 \cdot P_t(i)x_{i_n}^{h_n} = 0$. Similarly $\sum_{i=h_n+1}^{k} P_t(k-i)N_1 \cdot P_t(i)x_{i_n}^{h_n} = 0$ because $e(P_t(i)) > \frac{1}{2}\deg(x_{i_n}^{h_n})$. By induction, we have

$$P_t(k) \cdot N = P_t(h_n - i)N_1 \cdot P_t(i)x_{i_n}^{h_n} = N_1^{p^t}(x_{i_n}^{h_n})^{p^t}.$$

Hence we obtain $P_t(k) \cdot N = N^{p^t}$. ■

Wood's argument shows that $HK^{p^t} \equiv \widehat{P}_t(k)H \cdot K$ modulo hit elements. Hence if $e(\widehat{P}_t(k)) > h$, then $\widehat{P}_t(k)H = 0$ and hence HK^{p^t} is hit. Therefore it remains to show that $e(\widehat{P}_t(k)) = \mu_t(k)$. The following lemma was proved by Gallant [10].

Lemma 5.2.2

$$\widehat{P}_t(k) = \sum_{R} P_t(R)$$

where $|R|_t = (p^t - 1)k$.

By Lemma 3.1.11, $\mu_t(k)$ is exactly the minimum excess of the element $P_t(R)$ where $|R|_t = (p^t-1)k$. On the other hand, $\widehat{P}_t(k)$ is the summand of all $P_t(R)$ where $|R|_t = (p^t-1)k$ by Lemma 5.2.2. Hence $e(\widehat{P}_t(k)) = \mu_t(k)$. This completes the proof of Theorem 5.1.1.

Proof of Theorem 5.1.2 : We will prove this by induction on s. Suppose that $s = k+1$. Since for $k < t$ the only nonzero element $P_t(R)$ of B_t with $|R|_t = (p^t-1)(p-1)p^k$ is $P_t((p-1)p^k)$, $\widehat{P}_t(p^s-p^k) = \widehat{P}_t((p-1)p^k) = P_t((p-1)p^k)$. This proves the theorem for $s = k+1$.

Assume that it is true for $s-1$. Using the induction hypothesis and Corollary 1.a in [10], we have

$$\begin{aligned} P_t((p-1)p^{s-1})P_t((p-1)p^{s-2})\cdots P_t((p-1)p^k) &= P_t((p-1)p^{s-1})\widehat{P}_t(p^{s-1}-p^k) \\ &= \textstyle\sum_R \binom{\sum_i p^{it}r_i}{(p-1)p^{t+s-1}} P_t(R). \end{aligned}$$

where the sum is taken over all R such that $|R|_t = (p^t-1)(p^s-p^k)$. Since $\widehat{P}_t(p^s-p^k)$ is the sum of all $P_t(R)$ where $|R|_t = (p^t-1)(p^s-p^k)$, it is sufficient to show that

$$\binom{\sum_i p^{it}r_i}{(p-1)p^{t+s-1}} \equiv 1 \bmod p.$$

By Lemma 5.1.3 and Lemma 5.1.7, $\sum_i r_i \geq \mu_t(p^s-p^k) \geq (p-1)p^k$. For $s > k$ and $t \geq 1$ we have

$$(p-1)(p^k-p^{s+t-1}) + (p^t-1)(p^s-p^k) = (p^s-p^{k+1})(p^{t-1}-1) \geq 0.$$

Hence

$$\sum_i p^{it}r_i = \sum_i (p^{it}-1)r_i + \sum_i r_i \geq (p^t-1)(p^s-p^k) + (p-1)p^k \geq (p-1)p^{s+t-1}$$

On the other hand,

$$(p^t-1)\sum_i r_i \leq \sum_i (p^{it}-1)r_i = (p^t-1)(p^s-p^k).$$

So $\sum_i r_i \leq p^s - p^k$. Using this inequality, we have

$$\begin{aligned} \textstyle\sum_i p^{it}r_i &= \textstyle\sum_i (p^{it}-1)r_i + \sum_i r_i \\ &\leq (p^t-1)(p^s-p^k) + p^s - p^k \\ &\leq p^{s+t}. \end{aligned}$$

Hence $\binom{\sum_i p^{l_i} r_i}{(p-1)p^{t+s-1}} \equiv 1 \bmod p$ by Lucas's theorem [13] . This completes the proof.
■

Bibliography

[1] J.F. Adams and H.R. Margolis, Modules Over The Steenrod Algebra, Topology 10 (1971) 271-282.

[2] J.F. Adams and H.R. Margolis, Sub-Hopf-Algebra of The Steenrod Algebra, Proc.Camb.Phil.Soc. 76 (1974) 45-52.

[3] J. Adem, The iteration of the Steenrod Squares in Algebraic Topology, Proc. Nat. Acad. Sci. U.S.A. 38 (1952) 720-726.

[4] D.W. Anderson and D.M. Davis, A Vanishing Theorem in Homological Algebra, Comment. Math. Helvet. 48 (1973) 318-327.

[5] D. Arnon, Monomial Bases in the Steenrod Algebra, Pure and Applied Algebra, 96 (1994) 215-223.

[6] D.P. Carlisle and R.M.W. Wood, On an Ideal Conjecture in the Steenrod Algebra, preprint (1994).

[7] H. Cartan, Sur l'iteration des Operations de Steenrod, Comm. Math. Helvet. 29 (1955) 40-58.

[8] D.M. Davis, The Anti-automorphism of the Steenrod Algebra, Proc. Amer. Math. Soc. 44 (1974) 235-236.

[9] D.M. Davis, On the height of Sq^{2^n}, preprint (1985).

[10] A.M. Gallant, Excess and Conjugation in the Steenrod Algebra, Proc. Amer. Math. Soc. 76 (1979) 161-166.

[11] B. Gray, *Homotopy Theory*, Academic Press (1975).

[12] L.Kristensen, On a Cartan Formula For Secondary Cohomology Operations, Math. Scand. 16 (1965) 97-115.

[13] E. Lucas, Théorie des Functions Numériques Simplement Preiodiques, American J. Math. 1 (1878), 184-250, 289-321.

[14] H.R. Margolis, *Spectra and The Steenrod Algebra*, North Holland Math.Library (1983).

[15] J. Milnor, The Steenrod Algebra and Its Dual, Ann. of Math. 67 (1958) 150-171.

[16] J. Milnor and J. Moore, On the Structure of Hopf Algebra, Ann. of Math. 81 (1965) 211-264.

[17] K.G. Monks, Nilpotence in the Steenrod Algebra, Bol.Soc.Mat.Mexicana 37 (1992) 401-416.

[18] K.G. Monks, The Nilpotence Height of P_t^s, Proc. Amec. Math. Soc. 124 (1996) 1297-1303.

[19] K.G. Monks, Polynomial Modules Over the Steenrod Algebra, Preprint (1993).

[20] J.P. Serre, Cohomologie Modulo 2 des Complexes d'Eilenberg-Maclane, Comm. Math. Helv. 29 (1953) 198-232.

[21] J.H. Silverman, Conjugation and Excess in the Steenrod Algebra, Proc. Amer. Math. Soc. 119 (1993) 657-661.

[22] J.H. Silverman, Hit Monomials and the Canonical Anti-automorphism, preprint (1994).

[23] W. Singer On the Action of Steenrod Squares on Polynomial Algebra, Proc. A.M.S. 111 (1991), 577-583.

[24] N.E. Steenrod, Products of Cocyles and Extensions of Mappings, Ann. of Math. 48 (1947) 290-320.

[25] N.E. Steenrod, Reduced Powers of Cohomology classes, Ann. of Math. 56 (1952) 47-67.

[26] N.E. Steenrod and D.B.A. Epstein, Cohomology Operations, Princeton University Press, 1962.

[27] P.D.Straffin,Jr., Identities for Conjugation in the Steenrod Algebra, Proc. Amer. Math. Soc. 49 (1975) 253-255.

[28] G.Walker and R.M.W. Wood, The Nilpotence Height of Sq^{2^n}, Proc. Amer. Math. Soc. 124 (1996) 1291-1295.

[29] G.Walker and R.M.W. Wood, The Nilpotence Height of P^{p^n} preprint (1995).

[30] R.M.W. Wood, Steenrod Squares of Polynomials and The Peterson Conjecture, Math. Proc. Camb. Phil. Soc. 105 (1989), 307-309.

[31] R.M.W. Wood, A Note on bases and Relations in the Steenrod Algebra, Bull. London Math. Soc. 27 (1996) 380-320

[32] R.M.W. Wood, Differential Operators and The Steenrod Algebra, preprint (1995).

Vita

Ismet KARACA was born in Afyon, TURKEY in 1969. He received his B.S. degree in mathematics from University of Anadolu in 1989. As soon as he graduated as a top student in his class, he became teaching assistant at this university. In September 1989 he successfully passed an examination which is offered by Ministry of Education in Turkey. As a result he was awarded to study mathematics in the United States. He received his M.S. degree in mathematics from University of Miami, Florida in 1994.