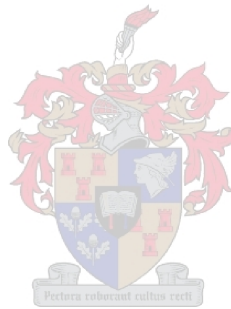


ARITHMETIC OF CARLITZ POLYNOMIALS

Alex Samuel BAMUNOBA



Thesis presented for the degree of **Doctor of Philosophy**
in the Faculty of Science at the University of Stellenbosch

Supervisor : Arnold KEET (PhD)

December 2014

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by the University of Stellenbosch will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: November 10, 2014

Abstract

In 1938, L. Carlitz constructed a class of polynomials parametrised by the elements of $\mathbb{F}_q[T]$. However, the relevance of his work was not widely recognised until decades later, e.g., in the works of Lubin - Tate (1960's) and V. Drinfeld (1970's). Since then, many results have appeared which are strikingly similar to those known about classical cyclotomic polynomials and cyclotomic number fields. Although the existence of these polynomials was discovered by L. Carlitz, it was S. Bae (in 1998) who popularised them. He did so by outlining properties of Carlitz cyclotomic polynomials well known for classical cyclotomic polynomials.

In this thesis, we extend this list of similarities by answering two elementary questions described below. Firstly, in 1987, J. Suzuki proved that every rational integer appears as a coefficient in some classical cyclotomic polynomial. It is this result that motivated us to ask, what is the actual set of coefficients of Carlitz cyclotomic polynomials? In short, the answer is $\mathbb{F}_q[T]$ and we prove this as follows, for each $m \in \mathbb{F}_q[T]$, we explicitly construct a Carlitz cyclotomic polynomial $\Phi_M(x)$ that contains m as a coefficient. In addition, we present analogues of several properties of coefficients of cyclotomic polynomials. In the second question, we were interested in the Carlitzian analogues of some famous numbers related to the factorisation of $x^n - y^n$. The first steps were made by D. Goss when he revealed the correct Carlitzian analogue of $x^n - y^n$. Imitating his constructions, we define the Carlitzian analogues of Zsigmondy primes, Fermat pseudoprimes, Wieferich primes and present a few results about them. Admittedly, little is known about the classical non Wieferich primes but in this formulation, we prove infinitude of non Carlitz Wieferich primes in $\mathbb{F}_q[T]$. We also describe algorithms used to compute (fixed) Carlitz Wieferich primes as well as compute new examples in the cases where $q = p = 3, 5, 7, 11, 13, 19, 29, 31, 37$ using SAGE software.

Opsomming

In 1938 het L. Carlitz 'n klas polinome gekonstrueer wat deur elemente van $\mathbb{F}_q[T]$ geparametriseer word. Die relevansie van sy werk is egter nie erken tot 'n paar dekades later nie, bv. in die werk van Lubin-Tate (1960's) en Drinfeld (1970's). Sedertdien het heelwat resultate verskyn wat soortgelyk is aan resultate oor klassieke siklotomiese polinome en siklotomiese liggame. Alhoewel L. Carlitz hierdie polinome ontdek het, was dit S. Bae (in 1998) wat hulle gewild gemaak het. Hy het dit gedoen deur eienskappe van Carlitz siklotomiese polinome en die welbekende eienskappe van klassieke siklotomiese polinome uiteen te set.

In hierdie tesis brei ons hierdie lys van ooreenkomstes uit deur twee elementêre vrae, wat onder beskryf word, op te los. Eerstens het J. Suzuki in 1987 bewys dat elke rasionale heelgetal as 'n koëffisiënt in minstens een klassieke siklotomiese polinoom voorkom. Dit is hierdie resultaat wat ons laat vra het wat die versameling koëffisiënte van Carlitz siklotomiese polinome is. Kortliks is die antwoord $\mathbb{F}_q[T]$ en ons bewys deur vir elke $m \in \mathbb{F}_q[T]$ 'n eksplisiete Carlitz siklotomiese polinoom $\Phi_M(x)$ te konstrueer wat m as koëffisiënt het. Daarbenewens bied ons verskeie eienskappe van koëffisiënte van siklotomiese polinome aan. In die tweede vraag was ons geïnteresseerd in die Carlitz analoë van sekere beroemde getalle verwant aan die faktoriserings van $x^n - y^n$. Die eerste treë is geneem deur D. Goss toe hy die korrekte analoog van $x^n - y^n$ gevind het. Deur sy konstruksies na te boots, definieer ons die Carlitz analoë van Zsigmondy priemgetalle, Fermat pseudopriemgetalle, Wieferich priemgetalle en bied ons 'n paar resultate oor hulle aan. Ons erken dat daar min bekend is oor klassieke nie-Wieferich priemgetalle, maar in hierdie formulering kan ons bewys dat daar oneindig veel nie-Carlitz-Wieferich priemgetalle in $\mathbb{F}_q[T]$ bestaan. Ons beskryf ook algoritmes om (bepaalde) Carlitz-Wieferich priemgetalle te bereken en om, met behulp van die SAGE sagteware pakket, nuwe voorbeelde in die gevalle $q = p = 3, 5, 7, 11, 13, 19, 29, 31, 37$ te gee.

Dedication

To my beloved mother,

"If I have not seen as far as others, it is because there were giants standing on my shoulders",

- H. Abelson.

Acknowledgements

First off, thank you to the Almighty God that has made this dream a reality. A thank you to my promoter, A. Keet (PhD), his broad knowledge of number theory, questions and hands-on approach to theory have provided me with many wonderful opportunities to learn. I am especially grateful for his patience with all kinds of questions. His commitment to communicating mathematics clearly and energetically at all times is a true model for me. Equally, a thank you to Professor F. Breuer for his role as a mentor and a teacher have been invaluable to me. Thank you to Professor B. Green, the AIMS Director (2012 / 2013) for the financial support rendered while doing my research and the excellent teaching opportunity at AIMS for my professional development. Once again, I thank you and I cordially commend this. Thank you to professors, I. Rewitzky, S. Wagner, F. Nyabadza, B. Bartlett (PhD) and A. Rabenantoandro (PhD student) for your friendliness and encouragement to pursue mathematics. A special thank you to Ms. O. Marais, Ms. L. Adams, Mrs. W. Isaacs and Mr. B. Jacobs for making life so simple in the department, I enjoyed working with you, baie dankie!

I am much honoured that professors L. Taelman and G. Rück have agreed to referee this thesis and I would like to thank them for their effort and for agreeing to serve on my jury. This thesis was written with financial support from the University of Stellenbosch and the DAAD In - Country Scholarship (A/13/90157). I thank both parties for their generosity.

Last but not the least, I am indebted to my family for their patience during all these years. Mr. & Mrs. D. Nyombi and family, B. Kirabo (PhD) and family, Maama J. Kigula, Mr. & Mrs. W. Olemo, the prayers worked and may God continue blessing you. I would like to give a special thank you to my high school mathematics teachers, S. Kyewalyanga (PhD) and Mr. W. Wafula, you were very inspirational, thumbs up! While doing my PhD, I have come to appreciate the presence of a number of friends especially J. Njagarah (PhD), Y. Nyonyi (PhD), Ms. R. Benjamin (PhD student), Ms. N. Numan, Mr. C. Wall, the AIMS – SA tutors and classes of 2012 / 2013 for your jokes and encouragement. Njagarah, *I will never forget the sleepless nights in the office!* Lastly, I thank my wife, S. Raleo, for all the emotional support as well as the occasional phone-calls to check on my well-being while far away from home.

Contents

Declaration	i
Abstract	ii
Opsomming	iii
Dedication	iv
Acknowledgements	v
Introduction	1
Objectives	1
Outline	1
Results	3
1 Preliminaries	4
1.1 Arithmetic in $\mathbb{F}_q[T]$	4
1.2 Arithmetic functions in $\mathbb{F}_q[T]$	8
2 Carlitz cyclotomic polynomials	12
2.1 Carlitz polynomials and Carlitz cyclotomic polynomials	12
2.2 Elementary properties of Carlitz cyclotomic polynomials	15
3 Coefficients	24

Contents	vii
3.1 On the coefficients of Carlitz cyclotomic polynomials	24
3.2 Statement and proof of an analogue to Suzuki's Theorem	30
4 The Carlitz Bang Zsigmondy Theorem and Carlitz Wieferich primes (Part I)	35
4.1 Zsigmondy and non Zsigmondy primes in $\mathbb{F}_q[T]$	35
4.2 Primitive and non primitive factors of $\mathcal{P}_N(x, y)$	39
4.3 Fermat pseudoprimes in $\mathbb{F}_q[T]$ and Wieferich primes in $\mathbb{F}_p[T]$	47
5 Carlitz Wieferich primes (Part II)	63
5.1 Some results from the theory of finite fields	64
5.2 Computing G -fixed Carlitz Wieferich primes in $\mathbb{F}_q[T]$	67
Appendix A	73
A.1 Algorithms for computing $\rho_m(x)$ and $\Phi_m(x)$	73
Bibliography	

List of Tables

3.1	Analogy between classical and Carlitz cyclotomic polynomials.	34
4.1	Normal elements in subfields of $\overline{\mathbb{F}}_3$ and the corresponding c - Wieferich primes.	58
4.2	Normal elements in subfields of $\overline{\mathbb{F}}_5$ and the corresponding c - Wieferich primes.	58
5.1	Normal elements in subfields of $\overline{\mathbb{F}}_{3^2}$ and the product of Wieferich primes.	70
5.2	Normal elements in subfields of $\overline{\mathbb{F}}_{5^2}$ and the product of Wieferich primes.	70

List of Notations

\mathbb{Z}	ring of integers	1
\mathbb{Z}_+	set of positive integers	1
a, d, m, n, s, t	positive integers in \mathbb{Z}	1
p	odd prime number in \mathbb{Z}	1
\mathbb{F}_q	finite field with q elements, where q is a power of an odd prime p	1
A	ring of polynomials in the variable T over \mathbb{F}_q	1
A_+	set of monic polynomials in A	1
a, b, f, g, m, D, N	monic polynomials in A	1
P	monic irreducible polynomial (or <i>prime polynomial</i>) in A	1
k	rational function field of A	1
K	completion of k with respect to the place at ∞	1
\mathbb{C}_∞	completion of the algebraic closure of K	1
$\rho_m(x)$	Carlitz m - polynomial	2
$\Phi_m(x)$	Carlitz m - cyclotomic polynomial	2
$\mathcal{A}_P(\Phi_{P^s}(x))$	prime height of $\Phi_{P^s}(x)$	2
$\mathcal{H}(\Phi_m(x))$	absolute height of $\Phi_m(x)$	2

Throughout this thesis, we shall adhere to the above notations. Although we have standardised our notation, we may at a few times deviate from it. Some notation that is only used briefly (*e.g.*, notation used only in a single proof or two proofs) has not been listed.

List of Algorithms

1	Computing Carlitz - Wieferich primes I.	53
2	Computing Carlitz - Wieferich primes II.	57
3	Computing Carlitz - Wieferich primes III.	63
4	Computing Carlitz - Wieferich primes IV.	70
5	Computing $\rho_m(\tau)$ using Lemma 2.2.1.	73
6	Computing $\Phi_m(x)$ using Proposition 2.2.2.	74
7	Computing $\Phi_m(x)$ by repeated polynomial division I.	75
8	Computing $\Phi_m(x)$ by repeated polynomial division II.	75

Introduction

This thesis is categorised in the area of number theory. It majorly deals with settling a recent question on the coefficients of Carlitz cyclotomic polynomials and at the same time applying the theory of Carlitz polynomials to understand further arithmetic in the ring $A := \mathbb{F}_q[T]$. It utilises the close analogy between number fields and function fields, extending ideas advanced by L. Carlitz [8], D. Goss [12], D. Thakur [29], S. Bae [3], and other contemporaries.

Objectives

The objectives of this thesis are but not limited to

- review the arithmetic theory of Carlitz (cyclotomic) polynomials.
- state, and prove an analogue of Suzuki's Theorem for Carlitz cyclotomic polynomials.
- discuss two applications of Carlitz polynomials in the study of arithmetic in A .

Outline

The thesis is organised as follows.

- In chapter 1 section 1.1, we give a gentle introduction to the study of number theory in function fields with special attention to A , the ring of polynomials in T over a finite field \mathbb{F}_q . We explain (without proof), the sequence of inclusions $pA \subset A \subset k \subset K \subset \mathbb{C}_\infty$ which is analogous to $p\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ in the classical setting. In section 1.2, we introduce ordinary and absolute arithmetic functions for the ring A . The importance of these functions will be realised as we gradually use them in the document. The facts presented in this chapter are well-known, except possibly for a few definitions and results in section 1.2, and even these should already be known to an expert.

This analogy does not stop in \mathbb{Q} but extends to finite extensions of \mathbb{Q} . In fact almost the whole of algebraic and analytic number theory can be repackaged in terms of the arithmetic and analysis of algebraic function fields. This is the approach taken by G. Salvador [23] and M. Rosen [22]. F. Breuer has often informally referred to this analogy as the *magic mirror*. Indeed it is a mirror in which problems in number theory can be reformulated in terms of function fields where algebraic, geometric and analytic arguments can be used to solve them or provide more insights and more conjectures.

- In chapter 2 section 2.1, we utilise these *magic mirror* concepts to explain recent developments in the theory of Carlitz polynomials. We develop most of the theory algebraically from scratch starting with the Carlitz module homomorphism ρ from A into $k\{\tau\}$, the twisted polynomial ring over k , (a.k.a., the endomorphism ring \mathbb{G}_a over k). We introduce the Carlitz m -polynomial $\rho_m(x)$ and its irreducible factors $\Phi_D(x)$, the Carlitz D -cyclotomic polynomial. These are the Carlitzian analogues of exponentiation in \mathbb{C} , the n th unital polynomial $x^n - 1$ and the d th - cyclotomic polynomial $\Phi_d(x)$. In section 2.2, we survey their properties so as to lay the foundation for later chapters.
- In chapter 3 section 3.1, we discuss our current findings on coefficients of the Carlitz cyclotomic polynomials. We give explicit formulas for prime height $\mathcal{A}_p(\Phi_{p^s}(x))$ of $\Phi_{p^s}(x)$ and absolute height $\mathcal{H}(\Phi_m(x))$ of $\Phi_m(x)$. In section 3.2, we prove a weaker A -analogue of a result due to C. Ji, W. Li and P. Moree [16] to which the Carlitzian version of Suzuki's Theorem is a corollary. In this context, Suzuki's Theorem is the statement that, *every $m \in A$ occurs as a coefficient in some Carlitz cyclotomic polynomial over A .*
- In chapter 4, we apply the theory of Carlitz polynomials developed in chapters 1 and 2 to study further arithmetic in A . In section 4.1, we characterise the existence of Zsigmondy and non Zsigmondy primes for the pair $\langle f, N \rangle$. Section 4.2 begins with S. Bae's work in [3] and we prove a number of results concerning *integers* analogous to $x^n - y^n$, its factorisation and composition properties. In addition, we explore analogues of Zsigmondy primes and give another proof to the Carlitzian analogue of the Bang - Zsigmondy Theorem. We give an upper bound on the number of Zsigmondy factors of $\Phi_N(f)$ and also establish infinitude of Carlitz Fermat pseudoprimes in A . Like A. Wieferich, we relate the Fermat - Goss - Denis Theorem, (a.k.a, *the Carlitz analogue to Fermat's Last Theorem*) to D. Thakur's definition of Carlitz Wieferich primes [28]. We go on to prove several results on Carlitz Wieferich primes including algorithms for their computation. Lastly, we give a heuristic that indicates finitude of these primes.
- In chapter 5, we extend our chapter 4 results on Carlitz Wieferich primes to $\mathbb{F}_q[T]$. We generalise our algorithms to those for computing G -fixed Carlitz Wieferich primes, where G is a non trivial proper subgroup of \mathbb{F}_q . We reveal *the infinitude of non Carlitz Wieferich primes in $\mathbb{F}_q[T]$, where $q > 2$.* This unconditionally establishes an analogue of J.

Silverman's result in [24]. Silverman proved that the abc - Conjecture implies infinitude of the classical non Wieferich primes.

- Lastly, in Appendix A, we describe algorithms used for computing $\rho_m(x)$ and $\Phi_m(x)$.

Results

The thesis brings to light some results that are believed to be original. For example, in chapter 3, we prove analogues of several results concerning coefficients of classical cyclotomic polynomials like D. Lehmer and O. Hölder's results, i.e., Theorems 3.1.5 and 3.1.6. We also prove Theorem 3.2.3, an $\mathbb{F}_q[T]$ analogue of Suzuki's Theorem for coefficient of elementary cyclotomic polynomials. In chapter 4 section 4.1, we characterise the analogues of Zsigmondy and non Zsigmondy primes. We also establish an upper bound for the number of Zsigmondy primes of $\langle f, N \rangle$, this is Theorem 4.1.10. In section 4.2, we give another proof to Theorem 4.2.9, the analogue of Bang - Zsigmondy Theorem. In the same chapter, we define Carlitz Fermat a - pseudoprimes and indicate their infinitude in Remark 4.3.2. We construct Carlitz Wieferich primes in $\mathbb{F}_q[T]$ and prove a few results about them. For example, in Theorem 4.3.18, we show infinitude of Carlitz Wieferich primes in $\mathbb{F}_2[T]$. In Theorem 5.2.8, we show infinitude of non Carlitz Wieferich primes in $\mathbb{F}_q[T]$. For odd p , our examples of Carlitz Wieferich primes in $\mathbb{F}_p[T]$ are invariant under translation, an important property utilised in their computation. Lastly, in Appendix A, we develop algorithms for computing Carlitz polynomials and Carlitz cyclotomic polynomials with their computation complexities.

The following papers were prepared within the thesis.

Journal articles

1. On some properties of Carlitz cyclotomic polynomials, [6].
2. A note on Carlitz Wieferich primes, (Submitted).

Chapter 1

Preliminaries

In this chapter, we shall lay the foundations for later results by reviewing the main concepts in the arithmetic of $\mathbb{F}_q[T]$. The concepts presented are fairly standard, and are only included to obtain a self-contained manuscript. For details, refer to any standard textbook on the arithmetic of function fields also known as *number theory in function fields*, e.g., [12] and [22].

1.1 Arithmetic in $\mathbb{F}_q[T]$

Let \mathbb{F}_q be a finite field with q elements, $q = p^s$, for some $s \in \mathbb{Z}_+$, p the characteristic of \mathbb{F}_q , and A be $\mathbb{F}_q[T]$, the univariate polynomial ring in the variable T defined over \mathbb{F}_q . A has many properties associated with the development of the theory of algebraic function fields (or *the theory of algebraic curves over finite fields*) in common with the ring of integers \mathbb{Z} in the development of algebraic number theory. We shall see these properties in this chapter. It is these properties that lie at the heart of the study of number theory in function fields.

Every element a in A has the form $a = \alpha_n T^n + \cdots + \alpha_1 T + \alpha_0$, where $\alpha_i \in \mathbb{F}_q$ and $n \in \mathbb{Z}_{\geq 0}$. If $\alpha_n \neq 0$, we say that, the sign of A denoted by $\text{sgn}(a)$, is α_n . If $\text{sgn}(a) = +1$, then a is referred to as a *monic* or *positive* polynomial. The set of all monic polynomials in A will be denoted by A_+ and will play the role of \mathbb{Z}_+ . The ring \mathbb{Z} is in bijection with A via the correspondence $\alpha_n q^n + \cdots + \alpha_1 q + \alpha_0 \longleftrightarrow \alpha_n T^n + \cdots + \alpha_1 T + \alpha_0$, where the integer represented on the left-hand side is assumed to be written in its base q expansion. When q is not prime, then there is no longer a canonical correspondence between the numbers $0, 1, \dots, q-1$ and elements of \mathbb{F}_q . However, if we pick any labelling of the elements of \mathbb{F}_q by $\{0, 1, \dots, q-1\}$ in which 0 corresponds to 0, this gives a lexicographic ordering on A . In addition to $\alpha_n \neq 0$, we say a has degree $\deg(a) = n$. We conventionally set $\text{sgn}(0) := 0$ and $\deg(0) := -\infty$. If $a, b \in A$ are non zero, then we have $\deg(ab) = \deg(a) + \deg(b)$ and $\deg(a + b) \leq \max\{\deg(a), \deg(b)\}$,

which is the so called *Strong Triangle Inequality* in non archimedean analysis. It turns out that the degree map $\deg : A \rightarrow \mathbb{Z} \cup \{\pm\infty\}$ defines a non archimedean (discrete) valuation on A .

It is an easy exercise to show that the ring A is an integral domain, and as a result, we can construct k , the field of fractions of A . We call k , the rational function field of A . Algebraically, this corresponds to the field of rational functions on an algebraic curve \mathbb{P}^1 defined over finite field \mathbb{F}_q . In terms of arithmetic, k is analogous to \mathbb{Q} , the field of rational numbers. Moreover, the degree map endows A with a division algorithm stated in Proposition 1.1.1 below.

Proposition 1.1.1 (Division Algorithm, ([22], Proposition 1.1)). *Let $f, g \in A$, with $g \neq 0$, then there exists uniquely determined $h, R \in A$ such that $f = hg + R$ and $\deg(R) < \deg(g)$.*

So A is a euclidean domain, a principal ideal domain (PID) and a unique factorisation domain (UFD). This allows a quick proof of the finiteness of the residue class rings of A below.

Proposition 1.1.2 ([22], Proposition 1.2). *Suppose $0 \neq a \in A$, then $\#(A/aA) = q^{\deg(a)}$.*

Proof. Let $\deg(a) = s$, by Proposition 1.1.1, $A_a = \{m \in A : \deg(m) < s\}$ is a complete set of representatives for A/aA . Each $m \in A_a$ is of the form $m = \alpha_{s-1}T^{s-1} + \cdots + \alpha_1T + \alpha_0$. Since the coefficients vary independently over \mathbb{F}_q , there are q^s possible such polynomials. \square

Definition 1.1.3. *Let $0 \neq a \in A$, then $|a| := \#(A/aA) = q^{\deg(a)}$. If $a = 0$, then $|a| := 0$.*

This measure of the size of a is analogous to the usual absolute value in \mathbb{R} restricted to \mathbb{Z} .

To understand the *multiplicative* structure of A , we need to first know the structure of A^* , the group of units in A . Suppose a is a unit in A , by definition, there exists b in A , such that $ab = 1$, that is, a constant polynomial in A . So the only units in A are the non zero constant polynomials. This means that, each non zero constant in \mathbb{F}_q is a unit in A . So $A^* = \mathbb{F}_q^*$. Just as every non zero integer can be made positive after multiplication by ± 1 , so can every non zero polynomial in A be made monic by multiplication with a suitable $\alpha \in \mathbb{F}_q^*$. Since every finite subgroup of the multiplicative group of a field is cyclic, we have \mathbb{F}_q^* is a finite cyclic group with $q - 1$ elements and so is A^* , i.e., $A^* = \mathbb{F}_q^*$, (this compares to $\mathbb{Z}^* = \{\pm 1\}$).

Let $a \in A$ be non constant. a is *irreducible* if whenever $a = a_1b_1$, then either a_1 or b_1 is a constant polynomial, i.e., a cannot be written as a product of two polynomials each of positive degree. a is a *prime* if whenever a divides a_2b_2 , then either a divides a_2 or a divides b_2 . In every PID, the notion of being irreducible and prime are equivalent (up to multiplication by units in a PID). So the terms irreducible and prime in A will be used interchangeably. However, it is conventional to require every prime polynomial to be monic. We define a prime P as any monic irreducible in A . This is analogous to a prime $p \in \mathbb{Z}_+$.

Every non constant polynomial m in A can be written as a product of a non zero constant and a monic polynomial. Therefore, every non zero proper ideal of A has a unique monic generator. Since A is also a UFD, every non constant $m \in A$ can be written uniquely as

$$m = \alpha \prod_{i=1}^s P_i^{e_i}, \quad (1.1)$$

where $\alpha \in \mathbb{F}_q^*$, P_i are distinct monic irreducible polynomials, i.e., primes, and $e_i \in \mathbb{Z}_{\geq 1}$. This is analogous to the *Fundamental Theorem of Arithmetic* in \mathbb{Z} which asserts, *every integer $n \neq 0$ can be written as a product of primes in \mathbb{Z} and the factorisation is unique up to multiplication by ± 1 .*¹ One of the aims of algebraic number theory is to restore the notion of unique factorisation to rings of integers. We now study the structure of A/mA and $(A/mA)^*$, its group of units.

Theorem 1.1.4 (Chinese Remainder Theorem, ([22], Proposition 1.4)). *Let $m_1, \dots, m_t \in A$ be pairwise coprime and $m = m_1 \cdots m_t$. Then we have the following isomorphisms,*

1. $A/mA \cong (A/m_1A) \times \cdots \times (A/m_tA)$.
2. $(A/mA)^* \cong (A/m_1A)^* \times \cdots \times (A/m_tA)^*$.

Let m be a non constant polynomial with the prime decomposition as in Equation (1.1), then

$$(A/mA)^* \cong (A/P_1^{e_1}A)^* \times \cdots \times (A/P_t^{e_t}A)^*.$$

It suffices to determine the structure of the groups $(A/P^{e_i}A)^*$ where P is a prime.

Proposition 1.1.5. *Let $P \in A$ be a prime, then $(A/PA)^*$ is cyclic of order $|P| - 1$.*

Proof. Since A is a PID and P is a non zero prime in A , PA is a maximal ideal, so A/PA is a finite field. In particular, $(A/PA)^*$ a finite cyclic group of order $|P| - 1$. \square

Proposition 1.1.6. *Let P be a non zero prime in A , $e \in \mathbb{Z}_+$, then $\#(A/P^eA)^* = |P|^{e-1}(|P| - 1)$. The kernel of the canonical map $\theta : (A/P^eA)^* \rightarrow (A/PA)^*$ is a P -group of order $|P|^{e-1}$. As $e \rightarrow \infty$, the minimal number of generators in the kernel $(A/P^eA)^*(1)$ tends to infinity.*

Proof. See ([22], Proposition 1.6). \square

The structure of these groups gets very complicated and causes problems in the more advanced parts of the theory [22]. This is one of the many sources of non analogies that exist between the multiplicative structures of \mathbb{Z} and A . In general, it looks like the analogy between \mathbb{Z} and A completely breaks down after this. However, we recover this beautiful

¹The Fundamental Theorem of Arithmetic for A is true because A is a UFD. In general this is false. However, in Dedekind domains (generalisation of the rings \mathbb{Z} and A), an equivalent statement which is *unique factorisation at the level of ideals*; is obtained by replacing primes with prime ideals in the Dedekind domain.

analogy by using the Carlitz module, but this comes at the cost of trading the multiplicative structure in A for the additive A -module structure, see chapter 2. The additive structures of \mathbb{Z} and A are completely different, even though analogous facts and constructions exist in both cases, the methods of proof and intuition are completely different. Good references to explicit material on additive number theory for both \mathbb{Z} and A include the texts [11] and [19].

Let m be a non zero polynomial in A and $A_m = \{a \in A : \deg(a) < \deg(m)\}$ be the set of representatives of A/mA . Since $1 \in (A/mA)$ is a unit, by standard theory of associates, every non zero residue class a is a unit in A/mA if and only if $(a, m) = 1$. The units form a multiplicative group $(A/mA)^*$ and $A_m^* := \{a \in A : \deg(a) < \deg(m), (a, m) = 1\}$ is a complete set of representatives of $(A/mA)^*$. We define $\varphi(m) := \#(A/mA)^*$. This definition gives us the polynomial version of the Euler totient function. Its properties such as multiplicativity follow trivially from counting principles in A . Having defined the Euler totient function in A , the analogue of Euler's and Fermat's Little Theorems follow naturally.

Proposition 1.1.7 (Euler's Theorem). *Let $a, m \in A$ with $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Proof. $\#(A/mA)^* = \varphi(m)$. By standard group theory (Lagrange's Theorem), $\bar{a}^{\varphi(m)} = 1$ for all $\bar{a} \in (A/mA)^*$. If $(a, m) = 1$, then $\bar{a} = a + mA \in (A/mA)^*$, so $a^{\varphi(m)} \equiv 1 \pmod{m}$. \square

Corollary 1.1.8 (Fermat's Little Theorem). *Let $a \in A$ with $(a, P) = 1$, then $a^{|P|-1} \equiv 1 \pmod{P}$.*

Proof. Since P is irreducible, we have $(a, P) = 1$ if and only if $P \nmid a$. Corollary 4.3.5 follows from Proposition 1.1.7 and the fact that, for an irreducible polynomial P , $\varphi(P) = |P| - 1$. \square

Like in classical number theory, the above theorems play an important role in the study of arithmetic of function fields, e.g., in the proof of the analogue of Wilson's Theorem and more pertinent, in our study of elementary cyclotomic polynomials and cyclotomic extensions.

Proposition 1.1.9 ([22], Proposition 1.9). *Let $P \in A$ be a prime, and x be an indeterminate, then*

$$x^{|P|-1} - 1 \equiv \prod_{-\infty < \deg(a) < \deg(P)} (x - a) \pmod{P}.$$

Corollary 1.1.10 (Wilson's Theorem, ([22], Proposition 1.9, Corollary 2)).

$$\prod_{-\infty < \deg(a) < \deg(P)} a \equiv -1 \pmod{P}. \quad (1.2)$$

Proof. Set $x = 0$ in Proposition 1.1.9. If the characteristic of \mathbb{F}_q is 2, the result follows since $1 = -1$ in \mathbb{F}_2 . Otherwise, $|P| - 1$ is even and still the result follows. \square

It is interesting to note that in the polynomial version of Wilson's Theorem, the L.H.S. of the congruence depends on the degree of P , (in some sense, 'size' of P) and not on P itself.

Let us now fix our notation. Take $s \in \mathbb{Z}_+$, $q = p^s$, $A = \mathbb{F}_q[T]$, $k = \mathbb{F}_q(T)$ ². Mimicking the construction of \mathbb{R} from \mathbb{Q} by completion using the usual absolute value, we complete k using the absolute value coming from a chosen place at ∞ of k . Let $v_\infty : k \rightarrow \mathbb{Z} \cup \{\infty\}$ be the valuation associated to this place and $\frac{1}{T}$ be its uniformiser. The standard absolute value $|\cdot|_\infty$, (also denoted as $|\cdot|$) coming from this place is $q^{-v_\infty(\cdot)}$. This turns k into a metric space. The notions of Cauchy-ness, convergence and completeness all make sense in terms of this absolute value (or $\frac{1}{T}$ -topology). We denote the associated completion k_∞ of k by K ³. Therefore, K is complete and moreover locally compact in the $\frac{1}{T}$ -topology, however K is not algebraically closed. Unlike the archimedean place at infinity in \mathbb{Q} , the infinite place of k is non archimedean. We are now aware of the following analogy: $A \sim \mathbb{Z}$, $k \sim \mathbb{Q}$ and $k \sim \mathbb{R}$.

If we let \bar{K} be the algebraic closure of K , we are tempted to think of \bar{K} as being analogous to \mathbb{C} in the sense that it is algebraically closed. However, $[\bar{K} : K] = \infty$, so \bar{K} is neither complete nor locally compact. We resolve the completeness problem by taking the completion of \bar{K} to get \mathbb{C}_∞ . This has an added advantage that \mathbb{C}_∞ is still algebraically closed. This is *analogous to \mathbb{C} in the sense that it is algebraically closed and is complete*. This will be enough for our study⁴. However \mathbb{C}_∞ is still not locally compact and hence not spherically complete. A *spherically complete field* is the maximal complete non archimedean field *with respect to a given place*. We now have the following sequence of inclusions: $PA \subset A \subset k \subset K \subset \mathbb{C}_\infty$. Although $\mathbb{C} \sim \mathbb{C}_\infty$, it is important to point out that, \mathbb{C}_∞ is much larger and spacious than the classical \mathbb{C} . This is because \mathbb{C}_∞ is an infinite extension over K as opposed to \mathbb{C} , a quadratic extension of \mathbb{R} .

1.2 Arithmetic functions in $\mathbb{F}_q[T]$

We have understood elementary arithmetic, done some algebra and analysis in A by constructing special fields k , K , and \mathbb{C}_∞ . We now do basic analytic number theory. An arithmetic function \mathcal{F} is a real or complex valued function $\mathcal{F} : A_+ \rightarrow \mathbb{C}$, e.g., the Möbius μ function, Euler totient φ function, divisor function d , in fact almost all the classical arithmetic functions. We define the *unit* function u as $u(m) = 1$ for all $m \in A_+$. The *identity* function is the map \mathbb{I} defined by $1 \mapsto 1$ and $m \mapsto 0$ for all $m \neq 1$. We define the Möbius function to be

$$\mu(m) = \begin{cases} (-1)^s, & m \text{ is square free with } s \text{ distinct prime factors,} \\ 0, & m \text{ has a square factor.} \end{cases}$$

We prove a few properties of these functions that will be important in the later theory.

Proposition 1.2.1. For any $m \in A_+$, $\sum_{D|m} \mu(D) = \mathbb{I}(m)$.

²Taking $k = \mathbb{F}_q(T)$ is not canonical since $k' = \mathbb{F}_q(\frac{aT+b}{cT+d})$, with $ad - bc \neq 0, a, b, c, d \in \mathbb{F}_q$ can also work well.

³ $K = k$ plus all limits of Cauchy sequences with respect to the absolute value of ∞ in k .

⁴A topologist, analyst or a geometer may need to do more and obtain a spherically complete field.

Proof. Let $1 \neq m = P_1^{\alpha_1} \cdots P_s^{\alpha_s}$ be the unique factorization of m as a product of prime powers. Let $N = P_1 \cdots P_s$. Then $\sum_{D|m} \mu(D) = \sum_{D|N} \mu(D)$ since the Möbius function vanishes on non squarefree polynomials. Any divisor of N corresponds to a subset of $\{P_1, \dots, P_s\}$. Therefore, for $m \neq 1$, $\sum_{D|N} \mu(D) = \sum_{i=0}^s \binom{s}{i} (-1)^i = (1-1)^s = 0$. The result is clear if $m = 1$. \square

If \mathcal{F}, \mathcal{G} are arithmetical functions on A_+ , we define their Dirichlet product $\mathcal{F} * \mathcal{G}$ to be the arithmetical function \mathcal{H} given by $\mathcal{H}(m) = \sum_{D|m} \mathcal{F}(D) \mathcal{G}(\frac{m}{D})$ for any $m \in A_+$. So we can rewrite $\sum_{D|m} \mu(D) = \mathbb{I}(m)$ as $\mu * u = \mathbb{I}$, so μ and u are Dirichlet inverses of each other.

Proposition 1.2.2 ([2], Theorem 2.6). *Dirichlet multiplication $*$ is commutative and associative.*

Proposition 1.2.3 (Möbius Inversion Formula). *Let $m \in A_+$, \mathcal{F}, \mathcal{G} be arithmetic functions. Then*

$$\mathcal{F}(m) = \sum_{D|m} \mathcal{G}(D) \text{ if and only if } \mathcal{G}(m) = \sum_{D|m} \mathcal{F}(D) \mu\left(\frac{m}{D}\right).$$

Proof. $\mathcal{F}(m) = \sum_{D|m} \mathcal{G}(D)$ means $\mathcal{F} = \mathcal{G} * u$, where $*$ is the Dirichlet product. Taking the Dirichlet product by μ on both sides gives $\mathcal{F} * \mu = (\mathcal{G} * u) * \mu = \mathcal{G}$ since $*$ is associative, so $\mathcal{G}(m) = \sum_{D|m} \mathcal{F}(D) \mu\left(\frac{m}{D}\right)$. Conversely, $\mathcal{F} = \mathcal{F} * \mathbb{I} = \mathcal{F} * (\mu * u) = (\mathcal{F} * \mu) * u = \mathcal{G} * u$. \square

The multiplicative version of this result asserts that, for any $m \in A_+$,

$$\mathcal{F}(m) = \prod_{D|m} \mathcal{G}(D) \text{ if and only if } \mathcal{G}(m) = \prod_{D|m} \mathcal{F}(D)^{\mu\left(\frac{m}{D}\right)}.$$

Proposition 1.2.4. *For any $m \in A_+$,*

$$|m| = \sum_{D|m} \varphi(D) \text{ and } \varphi(m) = \sum_{D|m} \mu(D) \left| \frac{m}{D} \right|.$$

Proof. We shall count the residue classes modulo m in two different ways. On the one hand, there are $|m|$ residue classes. Each residue class representative a can be written as Dm_0 , where $D = (a, m)$. Therefore, $(m_0, \frac{m}{D}) = 1$. Therefore, we can partition the residue classes $a \pmod{m}$ according to the value of the GCD (a, m) . The number of classes corresponding to a given $D|m$ is precisely $\varphi(\frac{m}{D})$. Therefore $|m| = \sum_{D|m} \varphi(\frac{m}{D}) = \sum_{D|m} \varphi(D)$ as desired. The second identity follows by from the Möbius Inversion Formula, Proposition 1.2.3. \square

Like L. Carlitz, we shall define more general absolute functions from A_+ to \mathbb{C}_∞ . In our case, there is a special absolute function that will be useful in the study of the coefficients of cyclotomic polynomials and computation of values of cyclotomic polynomials at special points. Let $\exp_A(\cdot)$, and $\text{Log}_A(\cdot)$ be \mathbb{C}_∞ valued *exponential* and *logarithm* (polynomial) functions with the following properties. For any $f, g \in A$, (i), $\exp_A(f + g) = \exp_A(f) \cdot \exp_A(g)$, (ii), $\exp_A(\text{Log}_A(f)) = f$, (iii), $\text{Log}_A(\exp_A(f)) = f$ and (iv), $\text{Log}_A(fg) = \text{Log}_A(f) + \text{Log}_A(g)$.

These serve more as notations than functions. This gives rise to two von Mangoldt functions,

$$\Lambda_0(m) = \begin{cases} \deg(P), & \text{if } m = P^s, \\ 0, & \text{otherwise,} \end{cases}, \quad \text{and} \quad \Lambda_1(m) = \begin{cases} \text{Log}_A(P), & \text{if } m = P^s, \\ 0, & \text{otherwise.} \end{cases} \quad (1.3)$$

These two von Mangoldt functions satisfy the following identities.

Proposition 1.2.5. *Let $m \in A_+$, then*

$$\begin{cases} \deg(m) = \sum_{D|m} \Lambda_0(D), \\ \text{Log}_A(m) = \sum_{D|m} \Lambda_1(D), \end{cases} \quad \text{and} \quad \begin{cases} \Lambda_0(m) = \sum_{D|m} \mu\left(\frac{m}{D}\right) \deg(D), \\ \Lambda_1(m) = \sum_{D|m} \mu\left(\frac{m}{D}\right) \text{Log}_A(D). \end{cases}$$

Proof. Take $m = P_1^{e_1} \cdots P_s^{e_s}$ to be the prime factorisation of m . Then,

$$\begin{aligned} \sum_{D|m} \Lambda_0(D) &= \sum_{i=1}^s \sum_{j=1}^{e_i} \Lambda_0(P_i^j) = \sum_{i=1}^s e_i \cdot \deg(P_i) = \sum_{i=1}^s \deg(P_i^{e_i}) = \deg(m), \text{ and} \\ \sum_{D|m} \Lambda_1(D) &= \sum_{i=1}^s \sum_{j=1}^{e_i} \Lambda_1(P_i^j) = \sum_{i=1}^s e_i \cdot \text{Log}_A(P_i) = \sum_{i=1}^s \text{Log}_A(P_i^{e_i}) = \text{Log}_A(m). \end{aligned}$$

The second set of equations follows by the Möbius Inversion Formula, Proposition 1.2.3. \square

Let $\phi_* : A_+ \rightarrow A$ be an absolute function defined by $\phi_*(m) = \sum_{D \in A_m} (D, m)$.

Proposition 1.2.6. *ϕ_* is a multiplicative function.*

Proof. By grouping the terms according to gcd, $\phi_*(m) = \sum_{a \in A_m} (a, m) = \sum_{D|m} \varphi\left(\frac{m}{D}\right)(D, m)$. Multiplicativity of ϕ_* follows from that of the GCD function and φ , since $\phi_* = \varphi * \text{gcd}(\cdot)$. \square

By grouping the terms of $\phi_*(m)$ according to the divisors of m , with the help of $\varphi(\cdot)$, we have $\phi_*(1) = 1$, $\phi_*(P^s) = P^{s-1}(P-1)$ and $\phi_*(m_1 m_2) = \phi_*(m_1)\phi_*(m_2)$ if m_1 and m_2 are coprime.

Proposition 1.2.7. *Let $m \in A_+$. Then*

$$m = \sum_{D|m} \phi_*(D), \text{ and } \phi_*(m) = \sum_{D|m} D \mu\left(\frac{m}{D}\right).$$

Proof. This is because \mathbb{I} is completely multiplicative. \square

Although the properties of ϕ_* are identical to those of φ , ϕ_* is the analogue of the gcd sum, (also known as (the analogue of) of the Pillai arithmetical function). We introduced this function, because, it often occurs in the determination of special values of $\Phi_m(x)$ over $\mathbb{F}_2[T]$.

Proposition 1.2.8. For any $m \in A_+$,

$$\phi_*(m) = m \prod_{P|m} \left(1 - \frac{1}{P}\right).$$

Proof. Follows from the fact that $\phi_*(P^s) = P^{s-1}(P - 1)$ and multiplicativity of ϕ_* . \square

In the same vein, $\sigma_s(m) = \sum_{D|m} D^s$ - is the sum s^{th} powers of divisors of m . Its special values are $\sigma_0(m) = 2^t$, where t is the number of prime divisors of m , and $\sigma_1(m) = m \prod_{P|m} (1 + \frac{1}{P})$.

The list can further be extended and analogues of other arithmetic and absolute arithmetic functions exist, like the divisor, Jordan totient, Liouville, Ramanujan sums e.t.c. However the aforementioned functions will suffice for our study. For details, see [12], [29] and [22].

Lastly, take $\pi_A(n) := \#\{P \in A : P \text{ a prime of degree } n\}$ to be the prime polynomial counting function (we shall also use the notation $\pi_{\mathbb{F}_q[T]}(n)$). Notice that we only count *monics*. This is because we conventionally defined a prime to be monic and secondly to obtain an analogy with only counting positive primes. This is why we segregate irreducibles by degree.

Theorem 1.2.9 (Gauss' Prime Polynomial Theorem).

$$\pi_A(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

This formula (in the case $q = p$) appears in an unpublished section 8 of the *Disquisitiones Arithmeticae*. There are several proofs of Gauss's Prime Polynomial Theorem available. Perhaps the most insightful (and important for the development of the theory) is the proof via zeta functions, mimicking Riemann's approach to the classical Prime Number Theorem, see ([22], Chapter 2) for details. If we want an asymptotic result, we can isolate the main (largest) term, corresponding to $d = n$, i.e., $\pi_A(n) \sim \frac{q^n}{n}$. If we set $x = q^n$, then $\pi_A(x) \sim \frac{x}{\log_q(x)}$.

In summary, A is a Euclidean domain hence a PID and UFD, its residue class rings of non zero ideals are finite. It has infinitely many primes and finitely many units. The monics and monic irreducibles in A correspond to positive integers and prime numbers in \mathbb{Z} resp. The size of a polynomial depends on the degree of the polynomial. The analogues of the Euler, Fermat and Wilson Theorems are true. We also pointed out some non analogies that arise from the complicated structure of the group of units of its factor rings. We described an analytic construction of field extensions and completions of k , studied some arithmetic functions. A proper mastering of this chapter will be very helpful in chapters 2 and 3.

Chapter 2

Carlitz cyclotomic polynomials

The aim of this chapter is to algebraically construct Carlitz cyclotomic polynomials from the Carlitz module ρ , the sign normalised rank one Drinfeld module. To do this we shall imitate the standard construction for classical cyclotomic polynomials. Again our underlying philosophy is to “replace \mathbb{Z} by $\mathbb{F}_q[T]$ almost everywhere”. For example, in this chapter and onwards, the notion of abelian groups (\mathbb{Z} - modules) will be replaced by $\mathbb{F}_q[T]$ - modules. In particular, \mathbb{G}_m - the multiplicative group scheme over \mathbb{Q} viewed as a \mathbb{Z} - module using the standard \mathbb{Z} - action will be replaced by the Carlitz module \mathcal{C} , which is essentially a special $\mathbb{F}_q[T]$ - module structure on the additive group scheme $\mathbb{G}_a := (\mathbb{C}_\infty, +)$ over k . In addition, we shall prove several factorisation and composition identities of Carlitz cyclotomic polynomials.

2.1 Carlitz polynomials and Carlitz cyclotomic polynomials

We shall maintain our notation as used previously in chapter 1. In addition, let τ be the q th power Frobenius element defined by $\tau(x) = x^q$, $x \in \mathbb{C}_\infty$. We denote by $k\{\tau\}$, the ‘twisted polynomial ring’ with a commutation relation $\tau w = w^q \tau$ for all $w \in k$. Each element of $k\{\tau\}$ is an \mathbb{F}_q - linear endomorphism of \mathbb{G}_a , the additive group scheme over k . To see this, take $\alpha \in \mathbb{G}_a$ and $f(\tau) = \sum a_i \tau^i \in k\{\tau\}$, then $f(\alpha) = f(\tau)(\alpha) = (\sum a_i \tau^i)(\alpha) = \sum a_i \alpha^{q^i} \in \mathbb{G}_a$. In this way, $k\{\tau\}$ is isomorphic to the ring of polynomials of the form $\sum_{i=1}^n a_i x^{q^i} \in k[x]$, where addition is defined as usual and multiplication is defined by composition of polynomials.

Let $\rho : A \rightarrow k\{\tau\}$ be a ring homomorphism (in fact it is an \mathbb{F}_q - algebra homomorphism) characterised by $T \mapsto \tau + T\tau^0$, obviously ρ fixes \mathbb{F}_q element-wise. This gives \mathbb{G}_a a new A - module structure with the module multiplication defined as follows, to each $m \in A$ and $x \in \mathbb{G}_a$, we set $m * x = \rho_m(x)$. We took \mathcal{C} to be the abelian group \mathbb{G}_a together with the associated ring homomorphism $\rho : A \rightarrow k\{\tau\}$ and called it the Carlitz module, $\mathcal{C} := (\mathbb{G}_a, \rho)$.

Although \mathcal{C} is the true Carlitz module, we shall often simply take the new A module homomorphism ρ to mean the Carlitz module, \mathcal{C} . If x is an indeterminate, then $\rho_m(x)$ is called the *Carlitz m - polynomial*. A moments reflection shows that $\rho_m(x)$ is an additive and separable polynomial over \mathbb{C}_∞ , (since $\rho'_m(x) = m$). These properties follow from the definition of the Carlitz module. Later on in section 2.2, we shall give recursive formula for computing $\rho_m(x)$.

There exists an analytic construction of these modules through the exponential functions associated with lattices in \mathbb{C}_∞ . This was first given by L. Carlitz in his seminal paper of 1938, [8]. This was the first and a special case of a more general construction for *elliptic modules* introduced by V. Drinfeld in 1974, [10]. These elliptic modules (a.k.a., *Drinfeld modules*) are in many respects similar to elliptic curves or in general, abelian varieties over algebraically closed fields. Moreover, these modules can be described analytically through lattices over some algebraically closed field of characteristic p by some sort of Weierstrass uniformisation, or algebraically as a module structure of the additive group scheme G_a of k . The interplay between these two view points results in a rich theory of modular schemes and modular forms, a deep area of mathematics. Below is a simple example of this analytic construction.

Let Λ be a rank one A lattice, i.e., a *strongly discrete abelian*¹ subgroup of \mathbb{C}_∞ of the form $\Lambda = \zeta A$, $\zeta \neq 0$. The exponential function associated to this A - lattice is given by

$$e_\Lambda(z) = z \prod_{\lambda \in \Lambda - \{0\}} \left(1 - \frac{z}{\lambda}\right).$$

This product has a (convergent) power series expansion of the form

$$e_\Lambda(z) = \sum_{i=0}^{\infty} a_i z^q,$$

(where $\lim_{i \rightarrow \infty} (|a_i|_\infty) = 0$). These types of exponentials have the following properties: they are \mathbb{C}_∞ valued functions, \mathbb{F}_q - linear, ζ - periodic, entire and therefore surjective as a functions on \mathbb{C}_∞ [22]. For $i \in \mathbb{Z}_+$, define $[i] := T^{q^i} - T$, the product of monic primes of degree dividing i . By definition $[0] = 1$, (the empty product). In particular, if we set

$$\bar{\zeta} = \bar{\pi} := (-[1])^{\frac{1}{q-1}} \prod_{i=0}^{\infty} \left(1 - \frac{[i]}{[i+1]}\right) \in K,$$

the Carlitz period, then $\Lambda_C := \bar{\pi}A$ gives rise to a special exponential function $e_C(z)$, called the Carlitz exponential. Note the ambiguity in \mathbb{F}_q^* arising in the $q - 1$ th root is similar to the sign ambiguity in trying to extract $2\pi i$ from $2\pi i\mathbb{Z}$. This was discovered by L. Carlitz [8] but working in a reverse direction, i.e., begun with the exponential $e_C(z)$ and then constructed

¹The term strongly discrete means that, the intersection of Λ with each ball in \mathbb{C}_∞ of finite radius is finite.

the A lattice Λ_C . Explicitly, it has a power series expansion (convergent for all $z \in \mathbb{C}_\infty$)

$$e_C(z) := \sum_{i=0}^{\infty} \frac{z^{q^i}}{D_i} \in k[[z]],$$

where $D_0 = 1$ and $D_i = [i][i-1] \cdots [1]$. $e_C(z)$ is also a \mathbb{C}_∞ -valued function, \mathbb{F}_q -linear, $\bar{\pi}$ -periodic, entire and therefore surjective as a function on \mathbb{C}_∞ , [12]. The element $\bar{\pi}$ is called the Carlitz period, and was shown to be transcendental over k by L. Wade, [31].

Consider the sequence of abelian groups below,

$$0 \longrightarrow \Lambda_C \longrightarrow \mathbb{C}_\infty \xrightarrow{e_C(z)} \mathbb{C}_\infty \longrightarrow 0. \quad (2.1)$$

Since Λ_C is the set of zeros of $e_C(z)$, (2.1) is a short exact sequence. So for any $0 \neq m$ in A , the diagram below commutes, ($m : \mathbb{C}_\infty/\Lambda_C \rightarrow \mathbb{C}_\infty/\Lambda_C$ is the usual multiplication in A).

$$\begin{array}{ccc} \mathbb{C}_\infty/\Lambda_C & \xrightarrow[e_C(z)]{\cong} & \mathbb{C}_\infty \\ m \downarrow & & \downarrow \rho_m \\ \mathbb{C}_\infty/\Lambda_C & \xrightarrow[e_C(z)]{\cong} & \mathbb{C}_\infty \end{array}$$

This is just a restatement of the functional equation $e_C(mz) = \rho_m(e_C(z))$. This gives a new A module homomorphism ρ that sends multiplication by m to a *new multiplication* denoted by ρ_m . This A module homomorphism is what we call(ed) the Carlitz module homomorphism.

To each $m \neq 0$ in A , the Carlitz module ρ associates an additive and separable polynomial $\rho_m(x)$. We define Λ_m to be the set of zeros of $\rho_m(x)$. As a subset of \mathbb{C}_∞ , Λ_m has a structure of a finitely generated rank one k -submodule of Λ_C . Moreover, we can realise Λ_m as follows,

$$\Lambda_m = \text{Ker}(\rho_m : \mathbb{C}_\infty \rightarrow \mathbb{C}_\infty) \cong \text{Ker}(m : \mathbb{C}_\infty/\Lambda_C \rightarrow \mathbb{C}_\infty) \cong (\frac{1}{m}\Lambda_C)/\Lambda_C \cong A/mA.$$

Therefore, with taking of A_m as the set of representatives of (A/mA) , we have

$$\Lambda_m = \{\lambda \in \mathbb{C}_\infty : \rho_m(\lambda) = 0\} = \{e_C(b\frac{\bar{\pi}}{m}) \in \mathbb{C}_\infty : b \in A_m\}.$$

An element $\lambda \in \Lambda_m$ is a *primitive Carlitz torsion point* of m if and only if it generates Λ_m as an A -module. Adjoining any primitive m -torsion λ or Λ_m to k yields a Galois k -extension $K_m := k(\Lambda_m)$, called the *Carlitz m -cyclotomic function field*. Its Galois group $\text{Gal}(K_m/k)$ is isomorphic to $(A/mA)^*$. For more details on Carlitz cyclotomic function fields, refer to the texts [23] and [22]. We use the name Carlitz as an adjective to cyclotomic function field in order to distinguish it from the constant field extension got by adjoining roots of unity to k .

Definition 2.1.1. Let $m \in A_+$ and Λ_m^* be the set of primitive Carlitz m -torsion points. We define

the Carlitz m - cyclotomic polynomial over k to be

$$\Phi_m(x) := \prod_{\lambda \in \Lambda_m^*} (x - \lambda) = \prod_{b \in A_m^*} (x - e_C(b \frac{\pi}{m})), \quad (2.2)$$

and the Carlitz m - inverse cyclotomic polynomial over k to be,

$$\psi_m(x) := \prod_{\lambda \in \Lambda_m \setminus \Lambda_m^*} (x - \lambda) = \prod_{b \in A_m \setminus A_m^*} (x - e_C(b \frac{\pi}{m})). \quad (2.3)$$

The emphasis on the name Carlitz m - cyclotomic polynomial to distinguish it from $\Phi_n(x)$, the classical n th - cyclotomic polynomial. $\Phi_m(x)$ satisfies nice relations that are well known for $\Phi_n(x)$. It is these that we explore in the next section, see [3] for additional material.

2.2 Elementary properties of Carlitz cyclotomic polynomials

We begin with a recursive formula for computing coefficients of $\rho_m(x)$. This will be very important in designing algorithms for computing both $\rho_m(x)$ and $\Phi_m(x)$, (see Appendix A).

Lemma 2.2.1 ([12], Proposition 3.3.10). *let $m \in A_+$. Then $\rho_m(x) = \sum_{i=0}^{\deg(m)} a_{m,i} x^i$ where,*

$$a_{m,0} = m, \quad a_{m,i} = \frac{a_{m,i-1}^q - a_{m,i-1}}{T^{q^i} - T}, \quad i = 1, \dots, \deg(m).$$

Proof. Let $n = \deg(m)$ and write $\rho_m = m\tau^0 + \chi_m$, where $\chi_m = \sum_{j=1}^n a_{m,j} \tau^j \in A\{\tau\}$. So $a_{m,0} = m$. Since $\rho_T = T\tau^0 + \tau$, we have $\chi_T = \tau$, and since ρ is a ring homomorphism, we get

$$\begin{aligned} \rho_m \circ \rho_T &= \rho_T \circ \rho_m & (2.4) \\ (m\tau^0 + \chi_m)(T\tau^0 + \tau) &= (T\tau^0 + \tau)(m\tau^0 + \chi_m) \\ mT\tau^0 + m\tau + \sum_{j=1}^n T^{q^j} a_{m,j} \tau^j + \sum_{j=1}^n a_{m,j} \tau^{j+1} &= Tm\tau^0 + \sum_{j=1}^n Ta_{m,j} \tau^j + m^q \tau + \sum_{j=1}^n a_{m,j}^q \tau^{j+1} \\ \sum_{j=1}^n (T^{q^j} - T) a_{m,j} \tau^j &= \sum_{j=1}^{n+1} (a_{m,j-1}^q - a_{m,j-1}) \tau^j. & (2.5) \end{aligned}$$

The result follows upon equating the coefficients of τ^j for $j = 1, \dots, n$ on both sides of Equation (2.5). For $j = n + 1$, we have $a_{m,n}^q - a_{m,n} = 0$ hence $a_{m,n} \in \mathbb{F}_q$. Which by $j = n$ implies that $(T^{q^n} - T)a_{m,n} = a_{m,n-1}^q - a_{m,n-1}$ which is realised as the leading coefficient of m . \square

Since any polynomial is determined by its coefficients, Lemma 2.2.1 gives a recursion for computing $\rho_m(x)$. If $m = P$, a prime, then $\rho_m(\tau) \in k\{\tau\}$ and as a polynomial in τ is Eisenstein at the prime P . Apart from Lemma 2.2.1, there are other ways of computing $a_{m,i}$. For

example: (i) Since T generates A over \mathbb{F}_q as an algebra, and ρ is a ring homomorphism, we get recursive formulas for $a_{m,i}$ from $\rho_{\sum_j a_j T^j} = \sum_j a_j \rho_{T^j}$, where $\rho_{T^j} = \rho_{T^{j-1}}(\rho_T) = \rho_{T^{j-1}}(T + \tau)$. (ii) Another way to get the $a_{m,i}$ directly is to use $\text{Log}_C(z)$, the additive local inverse of the Carlitz exponential $e_C(z)$, this is also referred to as the Carlitz logarithm, see [29] for details.

As an example, we compute $\rho_{T^2+1}(x)$ in A using technique (i) and then Lemma 2.2.1.

1. Technique (i). Given $m = T^2 + 1$. By definition $\rho_1(x) = x$ and $\rho_T(x) = x^q + Tx$. Also $\rho_{T^2}(x) = \rho_T(\rho_T(x))$, since ρ is a ring homomorphism. We compute $\rho_{T^2}(x)$ as follows.

$$\rho_{T^2}(x) = \rho_T(x^q + Tx) = (x^q + Tx)^q + T(x^q + Tx) = x^{q^2} + (T^q + T)x^q + T^2x.$$

Since ρ is a homomorphism, $\rho_{T^2+1}(x) = \rho_{T^2}(x) + \rho_1(x) = x^{q^2} + (T^q + T)x^q + (T^2 + 1)x$.

2. Using Lemma 2.2.1. Given $m = T^2 + 1$, we have $a_{m,0} = T^2 + 1$ and $a_{m,2} = 1$. Lastly,

$$a_{m,1} = \frac{a_{m,0}^q - a_{m,0}}{T^q - T} = \frac{(T^2 + 1)^q - (T^2 + 1)}{T^q - T} = \frac{T^{2q} - T^2}{T^q - T} = \frac{(T^q - T)(T^q + T)}{T^q - T} = T^q + T.$$

So $\rho_{T^2}(x) = a_{m,2}x^{q^2} + a_{m,1}x^q + a_{m,0}x = x^{q^2} + (T^q + T)x^q + (T^2 + 1)x$.

Proposition 2.2.2 (Fundamental Factorisation Identity). *Let $m \in A_+$. Then*

$$\rho_m(x) = \prod_{D|m} \Phi_D(x), \quad (2.6)$$

and

$$\Phi_m(x) = \prod_{D|m} \rho_D(x)^{\mu(\frac{m}{D})}, \quad (2.7)$$

where μ is the $\mathbb{F}_q[T]$ analogue of the Möbius function and D runs over monic divisors of m .

Proof. Since $\rho_m(x)$ is separable, the roots of $\rho_m(x)$ are exactly the Carlitz m -torsion points. On the other hand, if λ_D is an m -torsion point of Carlitz order D , then λ_D is a primitive D -torsion point, hence a root of $\Phi_D(x)$. But D also divides m , hence λ_D is also a root to the R.H.S. So the polynomials on L.H.S. and R.H.S. have the same roots. Equality of both polynomials on the L.H.S. and R.H.S. follows from the fact the both polynomials are monic and separable over \mathbb{C}_∞ . The next formula follows by the Möbius Inversion Formula. \square

By separability of $\rho_m(x)$, $\Phi_m(x)$ and $\psi_m(x)$, we have $\psi_m(x)\Phi_m(x) = \rho_m(x)$. Proposition 2.2.2 is used to study properties of $\Phi_m(x)$. For example, for any prime P and $s \geq 1$, $\Phi_{P^s}(x)$ is an Eisenstein polynomial for the prime P with coefficients in A . We have the following result.

Theorem 2.2.3. *Let $m \in A_+$, $\Phi_m(x) \in A[x]$ is a monic and irreducible polynomial over k .²*

²In other words, $\Phi_m(x)$ is the minimum polynomial over k of the primitive Carlitz m -torsion points.

There are many proofs for the classical version of this result. So to obtain a proof for the function field case, one carefully mimics any of them. We mimic ([15], Theorem 1, page 195).

Proof. We first prove that $\Phi_m(x) \in A[x]$.

The field extension K_m of k is the splitting field of the separable polynomial $\rho_m(x) \in A[x]$, since this polynomial splits over K_m and K_m is generated as an algebra by a single/primitive root of the polynomial $\rho_m(x)$. Since splitting fields are normal, the extension K_m/k is Galois. Any element of the Galois group $\text{Gal}(K_m/k)$, being a field automorphism, must map λ_m to another Λ_m -generator. Therefore, since the Galois group permutes the roots of $\Phi_m(x)$, it must fix the coefficients of $\Phi_m(x)$, so by Galois theory, these coefficients are in k . Since the coefficients are also integral over k , they must as well be in A as A is integrally closed in k .

Let f be the minimum polynomial of λ_m in $k[x]$. f is monic and has integral coefficients as well, since λ_m is integral over A . We shall prove that $f = \Phi_m(x)$ by showing that $\Phi_m(x)$ and f have the same roots. We achieve this via establishing the following claim,

Claim: For any prime $P \nmid m$, and any Λ_m -generator λ_m , if $f(\lambda_m) = 0$, then $f(\rho_P(\lambda_m)) = 0$.

This is because, if $(a, m) = 1$, $a \in A_+$, then $\rho_a(\lambda_m)$ is also Λ_m -generator. So, if $P \nmid m$, there exists $a_1, a_2 \in A_+$ such that $a_1P + a_2m = 1$. So $\rho_P(\rho_{a_1}(\lambda_m)) = \rho_{a_1P+a_2m}(\lambda_m) = \lambda_m$. Since λ_m and $\rho_{a_1}(\lambda_m)$ are Λ_m -generators, this means that any other Λ_m -generator can be obtained by successively taking the P -Carlitz action on λ_m a finite number of times.

To prove this claim, consider the factorisation $\rho_m(x) = f(x)g(x)$, $g(x) \in A[x]$ as occurring over K_m . Writing \mathcal{O}_m for the ring of integers of K_m , we treat the factorisation as taking place in $\mathcal{O}_m[x]$ and proceed to mod out both sides of the factorisation by any prime \mathfrak{P} of \mathcal{O}_m lying above the ideal PA . $\rho_m(x)$ has no repeated roots modulo \mathfrak{P} . This is because $\rho'_m(x) = m \neq 0$ is coprime to $\rho_m(x)$. So, if $f(\lambda_m) \equiv 0 \pmod{\mathfrak{P}}$, then $g(\lambda_m) \not\equiv 0 \pmod{\mathfrak{P}}$. Now we have

$$g(\rho_P(\lambda_m)) \equiv g(\lambda_m^{q^{\deg(P)}}) \equiv g(\lambda_m)^{q^{\deg(P)}} \not\equiv 0 \pmod{\mathfrak{P}}.$$

So $g(\rho_P(\lambda_m)) \neq 0$, because it does not even equal 0 modulo \mathfrak{P} . We know, $\rho_P(\lambda_m)$ is a root of $\rho_m(x)$, so if it is not a root of $g(x)$, it must be a root of $f(x)$. So $f(\rho_P(\lambda_m)) = 0$, as desired. $\Phi_m(x)$ is irreducible over A , and consequently over k , since k is the quotient field of A . \square

The following facts are standard. We have included their proofs for two reasons: (i) we shall need similar ideas in later chapters, and (ii) failure to find proper references for their proofs. In all the results presented from now and onwards, we shall consider $m \in A_+$ and $s \in \mathbb{Z}_+$.

Proposition 2.2.4 ([3], Proposition 1.1 (d)). *Let $s \in \mathbb{Z}_+$, $m \in A_+$ and P be a prime in A . Then*

$$\Phi_{mP^s}(x) = \begin{cases} \Phi_m(\rho_{P^s}(x)), & (m, P) \neq 1 \\ \Phi_{mP}(\rho_{P^{s-1}}(x)), & (m, P) = 1. \end{cases}$$

Proof. Suppose $(m, P) \neq 1$, this means P divides m . Then by Equation (2.7), we have

$$\begin{aligned}\Phi_{mP^s}(x) &= \prod_{D|mP^s} \left(\rho_{\frac{mP^s}{D}}(x)\right)^{\mu(D)} = \prod_{D|m} \left(\rho_{\frac{mP^s}{D}}(x)\right)^{\mu(D)} \prod_{D|mP^s, D \nmid m} \left(\rho_{\frac{mP^s}{D}}(x)\right)^{\mu(D)} \\ &= \Phi_m(\rho_{P^s}(x)) \prod_{D|mP^s, D \nmid m} \left(\rho_{\frac{mP^s}{D}}(x)\right)^{\mu(D)} = \Phi_m(\rho_{P^s}(x)),\end{aligned}$$

and the last equality follows from the fact that $D | mP^s$ and $D \nmid m$ implies $P^2 | D$, therefore $\mu(D) = 0$. Now suppose $P \nmid m$, then by Equation (2.7), we have

$$\Phi_{mP^s}(x) = \prod_{D|mP^s} \left(\rho_{\frac{mP^s}{D}}(x)\right)^{\mu(D)} = \Phi_{mP}(\rho_{P^{s-1}}(x)) \prod_{D|mP^s, D \nmid mP} \left(\rho_{\frac{mP^s}{D}}(x)\right)^{\mu(D)} = \Phi_{mP}(\rho_{P^{s-1}}(x)),$$

again $D | mP^s$ and $D \nmid mP$ implies $P^2 | D$, therefore $\mu(D) = 0$. The result follows. \square

Corollary 2.2.5.

$$\Phi_{mP^s}(x) = \begin{cases} \Phi_m(\rho_{P^s}(x)), & (m, P) \neq 1 \\ \frac{\Phi_m(\rho_{P^s}(x))}{\Phi_m(\rho_{P^{s-1}}(x))}, & (m, P) = 1. \end{cases}$$

Proof. It is enough to consider the case $(m, P) = 1$. By Proposition 2.2.4, we have

$$\begin{aligned}\Phi_{mP^s}(x) &= \Phi_{mP}(\rho_{P^{s-1}}(x)) = \prod_{D|mP} \rho_{D^{P^{s-1}}}(x)^{\mu\left(\frac{mP}{D}\right)} \\ &= \prod_{D|m} \rho_{D^{P^{s-1}}}(x)^{\mu\left(\frac{mP}{D}\right)} \prod_{D|m} \rho_{D^{P^s}}(x)^{\mu\left(\frac{mP}{DP}\right)} = \frac{\prod_{D|m} \rho_D(\rho_{P^s}(x))^{\mu\left(\frac{m}{D}\right)}}{\prod_{D|m} \rho_D(\rho_{P^{s-1}}(x))^{\mu\left(\frac{m}{D}\right)}} = \frac{\Phi_m(\rho_{P^s}(x))}{\Phi_m(\rho_{P^{s-1}}(x))}.\end{aligned}$$

\square

It is easy to show that,

$$\Phi_{mP^s}(x) \equiv \begin{cases} \Phi_m(x)^{|P^s|} \pmod{P}, & (m, P) \neq 1 \\ \Phi_m(x)^{\varphi(P^s)} \pmod{P}, & (m, P) = 1. \end{cases}$$

Theorem 2.2.6. Let m_0 be the ‘largest’ (in degree) squarefree factor of m , then $\Phi_m(x) = \Phi_{m_0}\left(\rho_{\frac{m}{m_0}}(x)\right)$.

Proof. Using the formula in Equation (2.7) and the definition of μ , we have

$$\Phi_m(x) = \prod_{D|m} \rho_{\frac{m}{D}}(x)^{\mu(D)} = \prod_{D|m, D|m_0} \rho_{\frac{m}{D}}(x)^{\mu(D)} = \prod_{D|m_0} \rho_{\frac{m_0}{D}}\left(\rho_{\frac{m}{m_0}}(x)\right)^{\mu(D)} = \Phi_{m_0}\left(\rho_{\frac{m}{m_0}}(x)\right).$$

\square

Theorem 2.2.6 will play a crucial role in the establishment of Theorem 3.2.3.

Theorem 2.2.7 ([3], Corollary 1.2 (b)). Let $s \in \mathbb{Z}_+$, $m \in A_+$,

$$\Phi_m(0) = \begin{cases} 1, & \text{if } m \text{ is not a power of a prime,} \\ P, & m = P^s. \end{cases}$$

Proof. We have

$$\Phi_m(x) = \prod_{D|m} \rho_D(x)^{\mu(\frac{m}{D})} = x^{\sum_{D|m} \mu(\frac{m}{D})} \prod_{D|m} x^{-\mu(\frac{m}{D})} \rho_D(x)^{\mu(\frac{m}{D})} = \prod_{D|m} (x^{-1} \rho_D(x))^{\mu(\frac{m}{D})}.$$

By Proposition 1.2.5, we have $\Lambda_1(m) = \sum_{D|m} \mu(\frac{m}{D}) \text{Log}_A(D)$. So

$$\Phi_m(0) = \prod_{D|m} D^{\mu(\frac{m}{D})} = \exp_A \left(\text{Log}_A \left(\prod_{D|m} D^{\mu(\frac{m}{D})} \right) \right) = \exp_A(\Lambda_1(m)) = \begin{cases} P, & \text{if } m = P^s, \\ 1, & \text{otherwise,} \end{cases}$$

and the result follows immediately. □

Theorem 2.2.8 ([4], Theorem 5.3.14). Let $\alpha \in \mathbb{F}_q$, $f \in A$, and η_α be the function $\eta_\alpha : k \rightarrow k$ defined by $f \mapsto f(T + \alpha)$. Then η_α is a k -automorphism. Moreover, for any $m \in A$

$$\Phi_{\eta_\alpha(m)}(x) = \eta_\alpha(\Phi_m(x)).$$

Example 2.2.9. If we take $m_1 = T^3 + T + 1 \in \mathbb{F}_2[T]$, we have $\Phi_{m_1}(x) = x^7 + (T^4 + T^2 + T)x^3 + (T^4 + T^3 + T^2 + 1)x + T^3 + T + 1$. There exists another prime in $\mathbb{F}_2[T]$ of degree 3 given by $m_2 = T^3 + T^2 + 1$. A straight forward computation shows that, $m_2 = \eta_1(m_1)$ and so we get;

$$\eta_1(\Phi_{m_1}(x)) = x^7 + (T^4 + T^2 + T + 1)x^3 + (T^4 + T^3 + T)x + T^3 + T^2 + 1 = \Phi_{m_2}(x).$$

The elementary properties from Lemma 2.2.1 to Theorem 2.2.8 are by far the most important in the theory of Carlitz cyclotomic polynomials. Evidence of this will be seen in chapters 3 and 4. For now, let us discuss the analogues of resultant and discriminant of $\Phi_m(x)$.

Let $f(x) = \sum_{i=0}^s \alpha_i x^i$ and $g(x) = \sum_{i=0}^t \beta_i x^i$ be elements of $A[x]$ of degrees s and t respectively. The Sylvester matrix ([20], pp. 20-22) of f and g is the $(s + t)$ -square matrix $M(f, g)$, where

$$M(f, g) := \begin{pmatrix} \alpha_s & \alpha_{s-1} & \cdots & \alpha_0 & & & & & & \\ & \alpha_s & \alpha_{s-1} & \cdots & \alpha_0 & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & \alpha_s & \alpha_{s-1} & \cdots & \alpha_0 \\ \beta_t & \beta_{t-1} & \cdots & \beta_0 & & & & & & \\ & \beta_t & \beta_{t-1} & \cdots & \beta_0 & & & & & \\ & & & & & \ddots & & & & \\ & & & & & & \beta_t & \beta_{t-1} & \cdots & \beta_0 \end{pmatrix}. \quad (2.8)$$

This is formed by filling the matrix beginning with the upper left corner with the coefficients of f , then shifting down one row and one column to the right and filling in the coefficients starting there until they hit the right side. The process is then repeated for the coefficients of g . The determinant of $M(f, g)$ is called the resultant of f and g and is denoted by $\mathcal{R}(f, g)$.

Theorem 2.2.10 (Resultant). *Let $f(x) = \alpha \prod_{i=1}^s (x - A_i)$ and $g(x) = \beta \prod_{j=1}^t (x - B_j)$, then*

1. $\mathcal{R}(f, g) = \alpha^t \beta^s \prod_{i=1}^s \prod_{j=1}^t (A_i - B_j) = (-1)^{st} \mathcal{R}(g, f)$
2. $\mathcal{R}(f, g) = \beta^s \prod_{j=1}^t f(B_j) = \alpha^t \prod_{i=1}^s g(A_i)$
3. $\mathcal{R}(f, gh) = \mathcal{R}(f, g)\mathcal{R}(f, h)$
4. $\mathcal{R}(f, g) = 0$ if and only if f and g have a common root.
5. if $f \equiv R \pmod{g}$, then $\mathcal{R}(f, g) = \beta^{s-t} \mathcal{R}(R, g)$.
6. $\mathcal{R}(f(x^l), g(x^l)) = \mathcal{R}(f, g)^l$.

Proof. For properties 1 to 5, refer to any standard text book on polynomials, e.g., [20]. We prove the last one which seems unfamiliar. Let $f(x) = \sum_{i=0}^s \alpha_i x^i$ and $g(x) = \sum_{i=0}^t \beta_i x^i$, then by definition $\mathcal{R}(f, g) = \det(M(f, g))$. From Definition 2.8, we see that $\mathcal{R}(f, g)$ has s rows of coefficients of f and t rows (not shown) of coefficients of g . Now considering the polynomials $f(x^l)$ and $g(x^l)$, we realize that these $f(x^l)$ and $g(x^l)$ have the same coefficients as $f(x)$ and $g(x)$ but separated by $l - 1$ zeros. This implies the following,

$$\begin{aligned} \mathcal{R}(f(x^l), g(x^l)) &= \begin{vmatrix} \alpha_s & 0 & \cdots & 0 & \alpha_{s-1} & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \alpha_s & \cdots & 0 & 0 & \alpha_{s-1} & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \alpha_s & 0 & 0 & \cdots & \alpha_{s-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ \beta_t & 0 & \cdots & 0 & \beta_{t-1} & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \beta_t & \cdots & 0 & 0 & \beta_{t-1} & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \alpha_s & 0 & 0 & \cdots & \beta_{t-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & \beta_0 \end{vmatrix} \\ &= \begin{vmatrix} \alpha_s \mathbb{I}_l & \alpha_{s-1} \mathbb{I}_l & \cdots & \alpha_0 \mathbb{I}_l & & & & & & \\ & \alpha_s \mathbb{I}_l & \alpha_{s-1} \mathbb{I}_l & \cdots & \alpha_0 \mathbb{I}_l & & & & & \\ & & \ddots & & & & & & & \\ \beta_t \mathbb{I}_l & \beta_{t-1} \mathbb{I}_l & \cdots & \beta_0 \mathbb{I}_l & \alpha_s \mathbb{I}_l & \alpha_{s-1} \mathbb{I}_l & \cdots & \alpha_0 \mathbb{I}_l & & \\ & \beta_t \mathbb{I}_l & \beta_{t-1} \mathbb{I}_l & \cdots & \beta_0 \mathbb{I}_l & & & & & \\ & & \ddots & & & & & & & \\ & & & & \beta_t \mathbb{I}_l & \beta_{t-1} \mathbb{I}_l & \cdots & \beta_0 \mathbb{I}_l & & \end{vmatrix} = \text{Det}(\mathcal{R}(f, g) \otimes \mathbb{I}_l), \end{aligned}$$

where \mathbb{I}_l is the $l \times l$ identity matrix and \otimes represents the tensor product of two matrices. We think of $\mathcal{R}(f(x^l), g(x^l))$ as the determinant of a block matrix where the individual entries, or blocks, are multiples of \mathbb{I}_l . Since the determinant of a block matrix equals the determinant of the original matrix, and a moment's thought leads us to the following calculation,

$$R(f(x^l), g(x^l)) = \text{Det}(\mathcal{R}(f, g) \otimes \mathbb{I}_l) = \text{Det}(\mathcal{R}(f, g))^l \text{Det}(\mathbb{I}_l)^{s+t} = \mathcal{R}(f, g)^l.$$

□

By properties 2 and 3 of Theorem 2.2.10, we observe that $\mathcal{R}(\Phi_1(x), \Phi_m(x)) = \Phi_m(0)$ and $\mathcal{R}(\Phi_{m_1}(x), \Phi_{m_2}(x)) = \mathcal{R}(\Phi_{m_2}(x), \Phi_{m_1}(x))$, whenever $m_1 \neq m_2$, since for $q > 2$, $\deg(\Phi_m(x))$ is even and for $q = 2$, $-1 \equiv 1 \pmod{2}$. The following result *with its proof* is due to S. Bae,

Theorem 2.2.11 (S. Bae [3], Theorem 2.2). *Let v, γ be elements in the extension of k , then*

$$\mathcal{R}(\Phi_m(x + v), \Phi_N(x + \gamma)) = \prod_{D|N} \Phi_{\frac{m}{(m,D)}}(\rho_D(v - \gamma))^{\mu\left(\frac{N}{D}\right) \frac{\varphi(m)}{\varphi\left(\frac{m}{(m,D)}\right)}}.$$

Corollary 2.2.12. *Let m, N be elements in A , such that $\deg(m) \geq \deg(N) \geq 0$, then*

$$\mathcal{R}(\Phi_m(x), \Phi_N(x)) = \begin{cases} 0, & \text{if } m = N, \\ P^{\varphi(N)}, & \text{if } m = NP^s, \\ 1, & \text{if } m \neq NP^s. \end{cases}$$

Proof. Set $v = \gamma = 0$, then substitute in Theorem 2.2.11, and use Theorem 2.2.7. □

The resultant $\mathcal{R}(f, g)$ has many applications, e.g., in elimination theory. We consider $P(x, z)$, $Q(y, z)$ as polynomials in z (so x, y are taken as constants), the vanishing of the resultant of these two polynomials is exactly the required relation $R(x, y) = 0$ (elimination of the variable z in the polynomial system $P(x, z) = 0 = Q(y, z)$). In algebraic geometry, it allows one to reduce a system of algebraic equations in order to search for roots of polynomials.

Definition 2.2.13. *Let $f \in k[x]$ be of degree $n \geq 1$. Let K_1 be an extension of k where f splits, and v_i be the roots of f in K_1 (taken with multiplicities). Then the (normalized) discriminant of f is*

$$\mathcal{D}_0(f) = \prod_{1 \leq i < j \leq n} (v_i - v_j)^2.$$

Such a field K_1 exists, for example the algebraic closure of k will do, and $\mathcal{D}_0(f) \in k$ does not depend on the choice of K_1 . (This also follows from the fact that $\mathcal{D}_0(f)$ is a symmetric polynomial in the variables v_1, \dots, v_n). Furthermore, $\mathcal{D}_0(\alpha f) = \mathcal{D}_0(f)$ for any constant $\alpha \neq 0$. However, while the definition of \mathcal{D}_0 is simple and natural, \mathcal{D}_0 is particularly useful for monic polynomials. Let $f = \alpha_n x^n + \dots + \alpha_0$ be a polynomial of degree $n \geq 1$ with coefficients in

an arbitrary ring A . The (standard) discriminant of f is given by,

$$\mathcal{D}(f) = \alpha_n^{2n-2} \prod_{1 \leq i < j \leq n} (v_i - v_j)^2 = \alpha_n^{2n-2} \mathcal{D}_0(f),$$

where v_i 's are the roots of f in some algebraic extension of k . Although Definition 2.2.13 is nice, it is sometimes hard to use for computations. We instead prove Lemma 2.2.14 that relates the discriminant and the resultant of a polynomial f with its derivative f' .

Lemma 2.2.14. *Let $f \in A[x]$ be (separable) of degree $n \geq 1$ with leading coefficient α , then*

$$\mathcal{R}(f, f') = (-1)^{\frac{n(n-1)}{2}} \alpha^{2-n} \mathcal{D}(f) = (-1)^{\frac{n(n-1)}{2}} \alpha^n \mathcal{D}_0(f).$$

Proof. Let v_1, \dots, v_n be roots of f in L/k . Since f is separable over L , $f(x) = \alpha \prod_{i=1}^n (x - v_i)$ and its derivative is $f'(x) = \sum_{j=1}^n \prod_{i \neq j} (x - v_i)$, so $f'(v_j) = \prod_{i \neq j} (v_j - v_i)$. Consequently,

$$\begin{aligned} \mathcal{R}(f, f') &= \alpha^n \prod_{i=1}^n f'(v_i) = \alpha^n \prod_{i=1}^n \prod_{j \neq i} (v_j - v_i) = \alpha^n \prod_{1 \leq i < j \leq n} (v_i - v_j)(v_j - v_i) \\ &= (-1)^{\frac{n(n-1)}{2}} \alpha^n \prod_{1 \leq i < j \leq n} (v_i - v_j)^2 = (-1)^{\frac{n(n-1)}{2}} \alpha^n \mathcal{D}_0(f) = (-1)^{\frac{n(n-1)}{2}} \alpha^{2-n} \mathcal{D}(f). \end{aligned}$$

□

Proposition 2.2.15 (Discriminant of $\Phi_m(x)$). *Let $m \in A_+$. Then*

$$\mathcal{D}(\Phi_m(x)) = m^{\varphi(m)} \prod_{P|m} P^{-\frac{\varphi(m)}{\varphi(P)}}.$$

Proof. We adapt the proof of ([20], Section 3.3.5). We have

$$\Phi_m(x) = \prod_{D|m} \rho_D(x)^{\mu(\frac{m}{D})} = \rho_m(x) \prod_{D|m, D \neq m} \rho_D(x)^{\mu(\frac{m}{D})}, \text{ and, } \Phi'_m(\lambda) = m \prod_{D|m, D \neq m} \rho_D(\lambda)^{\mu(\frac{m}{D})}.$$

If λ is a root to $\Phi_m(x)$, then $\rho_D(\lambda)$ is a root of $\Phi_{\frac{m}{D}}(x)$, and therefore

$$\begin{aligned} \prod_{\lambda \in \Lambda^*} \Phi'_m(\lambda) &= m^{\varphi(m)} \prod_{D|m, D \neq m} \left(\prod_{\lambda \in \Lambda^*} \rho_D(\lambda) \right)^{\mu(\frac{m}{D})} \\ &= m^{\varphi(m)} \prod_{D|m, D \neq m} \left(\Phi_{\frac{m}{D}}(0)^{\frac{\varphi(m)}{\varphi(\frac{m}{D})}} \right)^{\mu(\frac{m}{D})} = m^{\varphi(m)} \prod_{P|m} P^{-\frac{\varphi(m)}{\varphi(P)}}. \end{aligned}$$

This follows from the fact the value of $\Phi_{\frac{m}{D}}(0)$ is distinct from 1 if and only if $\frac{m}{D}$ is a prime power, on the other hand $\mu(\frac{m}{D})$ is distinct from zero if and only if $\frac{m}{D}$ is not divisible by a

square of a prime. Hence there remain values of D for which $\frac{m}{D}$ is a prime. Therefore,

$$\mathcal{D}(\Phi_m(x)) = (-1)^{\frac{\varphi(m)(\varphi(m)-1)}{2}} \mathcal{R}(\Phi_m(x), \Phi'_m(x)) = \prod_{\lambda} \Phi'_m(\lambda) = m^{\varphi(m)} \prod_{P|m} P^{-\frac{\varphi(m)}{\varphi(P)}}.$$

□

Proposition 2.2.16 ([23], Proposition 12.5.11). *Let $m \in A_+$. If m is not a prime power, then $\Phi_m(x) \equiv 1 + ax^{(q-1)} \pmod{x^{2(q-1)}}$, where $a \in A$ and $\deg(a) = (-1 + \deg(m))(q-1) - 1$.*

As a corollary, we give an alternative proof to the second part of ([22], Proposition 12.6).

Corollary 2.2.17. *If $m \neq P^s$. Then any primitive Carlitz m torsion λ is a unit in \mathcal{O}_m .*

Proof. $0 = \Phi_m(\lambda) \equiv 1 + a\lambda^{(q-1)} \pmod{\lambda^{2(q-1)}}$, therefore, $1 = \lambda(-a\lambda^{q-2} + \alpha\lambda^{2q-3})$, for some α an algebraic integer in K_m . Therefore, λ is a unit in \mathcal{O}_m , the ring of integers of K_m . □

In section 2.1, we introduced the Carlitz module and used it to construct Carlitz polynomials, and their cyclotomic factors. In section 2.2, we discussed several elementary properties of these polynomials analogous to those of classical cyclotomic polynomials. From our discussion, we realised that the analogy is not truly perfectly symmetric. There are some results true in A with no known analogues in \mathbb{Z} and vice versa, e.g., Theorem 2.2.8 is true in A but not in \mathbb{Z} , and the palindrome property is true for \mathbb{Z} but not in A . The above properties form the foundation for the theory developed in chapters 3, 4 and Appendix A. We computed the resultant of $\Phi_m(x)$ and $\Phi'_m(x)$ and used them to calculate the discriminant of $\Phi_m(x)$. As indicated in the statements or their proofs, most of these results can be found in the literature.

Chapter 3

Coefficients

In this chapter, we shall prove a number of results concerning coefficients of $\Phi_m(x)$. In particular, we shall define the order, prime height, absolute height and give explicit formula for prime height of $\Phi_{p^s}(x)$ and absolute height of $\Phi_m(x)$. Over $\mathbb{F}_2[T]$, we shall compute the coefficient of x in $\Phi_m(x)$. Lastly, we shall state and prove an analogue of Suzuki's Theorem. *Part of this work has been accepted for publication in peer reviewed journals, for example, see [6].*

3.1 On the coefficients of Carlitz cyclotomic polynomials

In this section, we investigate three properties of coefficients of cyclotomic polynomials. Firstly, divisibility of coefficients with respect to some prime P , then their size with respect to the absolute value that comes from the place at infinity and lastly, the values of these polynomials at special points. Part of this work appears in [4] but not in this revised form.

Let $m \in A$, we define the *order* of $\Phi_m(x)$, denoted by $\text{ord}_A(m)$ to be the number of distinct prime factors of m . If m has only one prime factor P , then we can define the P -*prime height* of $\Phi_m(x)$, denoted by either $\mathcal{A}_P(\Phi_m(x))$ or $\mathcal{A}_P(m)$ as the maximum valuation with respect to P of the non zero coefficients of $\Phi_m(x)$. This can also be extended to Carlitz polynomials and the inverse cyclotomic polynomials corresponding to the same m , and one similarly defines $\mathcal{A}_P(\rho_m(x))$ and $\mathcal{A}_P(\psi_m(x))$ respectively. We define $\mathcal{A}_P(m)$ as above because the order one Carlitz cyclotomic polynomials are already Eisenstein at the prime P . This can be deduced from Lemma 2.2.1 and Proposition 2.2.4. See ([22], Corollary - 12.6) for a rigorous proof.

Theorem 3.1.1 ([4], Theorem 5.3.12). *For any prime $P \in A_+$, we have $\mathcal{A}_P(P) = 1$.*

Proof. Suppose $\deg(P) = 1$, then $\Phi_P(x) = x^{q-1} + P$, clearly its valuation set is $V_P = \{0, 1\}$, (we only take the valuation of the non zero terms) therefore $\mathcal{A}_P(P) = 1$. Let $\deg(P) = n > 1$,

by Proposition 2.2.1, $\Phi_P(x) = a_{P,0} + a_{P,1}x^{q-1} + \dots + a_{P,n}x^{q^n-1}$, where the coefficients are

$$a_{P,0} = P, a_{P,1} = \frac{a_{P,0}^q - a_{P,0}}{T^q - T}, a_{P,2} = \frac{a_{P,1}^q - a_{P,1}}{T^{q^2} - T}, \dots, a_{P,n-1} = \frac{a_{P,n-2}^q - a_{P,n-2}}{T^{q^{n-1}} - T}, a_{P,n} = 1.$$

So $v_P(a_{P,0}) = 1$ and $v_P(a_{P,n}) = 0$. Now, $v_P(a_{P,0}^q - a_{P,0}) = v_P(P^q - P) = 1$ since $P \nmid (P^{q-1} - 1)$ and $v_P(T^q - T) = 0$ since $\deg(P) > 1$ and $T^q - T$ splits over \mathbb{F}_q , so $v_P(a_{P,1}) = 1$. Similarly, $v_P(a_{P,2}) = v(a_{P,1}^q - a_{P,1}) - v_P(T^{q^2} - T) = 1$. This is done upto $a_{P,n-1}$, since a prime P divides $T^{q^n} - T$ if and only its degree divides n . $v_P(a_{P,n}) = v_P(a_{P,n-1}^q - a_{P,n-1}) - v_P(T^{q^n} - T) = 0$, because at this point, at-least one of the factors of $T^{q^n} - T$ is P . Therefore, the $V_P = \{0, 1\}$. \square

Theorem 3.1.2 ([4], Theorem 5.3.16). *Let $s \in \mathbb{Z}_{\geq 2}$, then $\mathcal{A}_P(P^s) = (q^{\deg(P)} - 1)(s - 1)$.*

Proof. We proceed by induction on powers s of P , set $n = \deg(P)$. Trivially, $\Phi_1(x) = x$ and $\Phi_P(x) = x^{q^n-1} + c_{P,1}x^{q(q^{n-1}-1)} + \dots + c_{P,q(q^{n-1}-1)}x^{q-1} + P$, where by Theorem 3.1.1, we have $\mathcal{A}_P(P) = 1$. In particular $v_P(c_{P,q(q^{n-1}-1)}) = 1$. Since both $\rho_P(x)$ and $\Phi_P(x)$ have the same non zero coefficients (all divisible by P but not P^2), and $q^n - 1 > q^{n-1}$ for all q and $n \in \mathbb{Z}_+$, $(\rho_P(x))^{q^n-1}$ contains the term with the highest valuation with respect to P in the expression:

$$\Phi_{P^2}(x) = \Phi_P(\rho_P(x)) = (\rho_P(x))^{q^n-1} + \dots + P = x^{q^n-1} \left(\Phi_P(x)^{q^n-1} \right) + \dots + P.$$

The coefficient of x^{q^n-1} in $\Phi_{P^2}(x)$ is given by $\Phi_P(0)^{q^n-1} = P^{q^n-1}$. Therefore, when $s = 2$, we have $\mathcal{A}_P(P^2) = q^n - 1 = (q^n - 1)(2 - 1)$, and so the formula true for $s = 2$. Suppose it is true for $s = n'$, that is to say $\mathcal{A}_P(P^{n'}) = (q^n - 1)(n' - 1)$ and the coefficient attaining this valuation is x^{q^n-1} . We now compute $\Phi_{P^{n'+1}}(x)$. Now using Theorem 2.2.4, we obtain

$$\Phi_{P^{n'+1}}(x) = \Phi_P(\rho_{P^{n'}}(x)) = \rho_{P^{n'}}(x)^{q^n-1} + \dots + P = x^{q^n-1} \left(\prod_{t=1}^{n'} \Phi_{P^t}(x)^{q^n-1} \right) + \dots + P,$$

with the position having maximum P -adic valuation at x^{q^n-1} . To obtain the coefficient of x^{q^n-1} , consider the constant terms of $\Phi_{P^t}(x)$. So the coefficient of x^{q^n-1} in $\Phi_{P^{n'+1}}(x)$ is

$$c_{P^t, q^n-1} = \prod_{t=1}^{n'} \Phi_{P^t}(0)^{q^n-1} = P^{n'(q^n-1)},$$

so $\mathcal{A}_P(P^{n'+1}) = (q^n - 1)(n' + 1 - 1)$. \square

So we obtain $\mathcal{A}_P(P^s) \propto s - 1$. This parallels the classical results where $\mathcal{A}_p(p^s) \propto s$.

Example 3.1.3. *Suppose $A = \mathbb{F}_3[T]$, and $P = T \in A$. Computations using **SAGE** reveal that $\Phi_{T^4}(x) = x^{54} + (2T^9 + 2T^3 + 2T)x^{36} + (2T^6 + 2T^4 + 2T^2)x^{30} + 2T^3x^{28} + (T^{18} + 2T^{12} + 2T^{10} + T^6 + 2T^4 + T^2)x^{18} + (2T^{15} + 2T^{13} + 2T^{11} + 2T^9 + T^7 + T^5 + 2T^3)x^{12} + (2T^{12} + 2T^6 + 2T^4)x^{10} + (T^{12} + 2T^{10} + 2T^6 + T^4)x^6 + (2T^9 + 2T^7 + 2T^5)x^4 + T^6x^2 + T$. The coefficient with highest valuation with respect to the prime T is T^6 and so $\mathcal{A}_T(T^4) = 6 = (3^1 - 1)(4 - 1)$.*

We define *absolute height* of a polynomial $f \in A[x]$ denoted by $\mathcal{H}(f)$ to be the maximum absolute value¹ of the coefficients of f , e.g., given $f = x^{q^2-1} + (T^q + T)x^{q-1} + T$, then $\mathcal{H}(f) = q^q$. Since this absolute value is non archimedean, the height function $\mathcal{H}(\cdot)$ is multiplicative. Since $\rho_m(x), \Phi_m(x) \in A[x]$, their absolute heights are powers of q .

Theorem 3.1.4 ([4], Theorem 5.3.5). *Let $m \in A_+$, then $\log_q(\mathcal{H}(\rho_m(x))) = q^{\deg(m)-1}$.*

The last part of this section focuses on supplying explicit formulas for evaluation of $\Phi_m(x)$ and its first derivative at 0. Firstly, recall from Theorem 2.2.7 that

$$\Phi_m(0) = \exp_A(\Lambda_1(m)) = \begin{cases} 1, & \text{if } m \text{ is not a power of a prime,} \\ P, & m = P^s. \end{cases}$$

This is analogous to the following result due to V. Lebesgue [17]

$$\Phi_n(1) = e^{\Lambda(n)} = \begin{cases} 1, & \text{if } n \text{ is not a power of a prime,} \\ p, & n = p^s, \end{cases}$$

with 0 replaced by 1 and $\Lambda_1(m)$ by the von Mangoldt function. With the help of this, D. Lehmer [17] showed that the geometric mean of $\{\Phi_{n_0}(0) : n \in \mathbb{Z}_+, n_0 \leq n\}$ tends to the Euler number $e \approx 2.7182$ as $n \rightarrow \infty$. The following theorem is an analogue to this result.

Theorem 3.1.5. *The geometric mean of $\{\Phi_m(0) : m \in A_+, \deg(m) \leq n\} \rightarrow [1]_q^{\frac{1}{q}}$ as $n \rightarrow \infty$.*

Proof. Let E_n be the geometric mean of $\{\Phi_m(0) : m \in A_+, \deg(m) \leq n\}$. By Theorem 2.2.7,

$$E_n = \left(\prod_{m \in A_+, 1 \leq \deg(m) \leq n} \Phi_m(0) \right)^{\frac{q-1}{q^{n+1}-q}} = \left(\prod_{1 \leq \deg(P^s) \leq n} P \right)^{\frac{q-1}{q^{n+1}-q}} = (L_n)^{\frac{q-1}{q^{n+1}-q}},$$

where $L_n = [n][n-1] \cdots [2][1]$, $[i] = T^{q^i} - T$. It is clear that the product $\prod_{1 \leq \deg(P^s) \leq n} P$ is the least common multiple of the non zero monics in A with degree less than or equal to n . By ([12], Proposition 3.1.6), this product is equal to L_n which has degree $\frac{q^n-1}{q-1}$. Define $\bar{\pi}_n$ as

$$\bar{\pi}_n = \prod_{j=1}^{n-1} \left(1 - \frac{[j]}{[j+1]} \right) = \frac{[1]_q^{\frac{q^n-1}{q-1}}}{L_n}, n \geq 1.$$

Since $v_\infty(\bar{\pi}_n) = 0$ for all $n \in \mathbb{Z}_+$, it is clear, the sequence $\{\bar{\pi}_n\}$ has a limit $\bar{\pi}$ in K . So

¹The absolute value coming from the place at ∞ of k .

$$\begin{aligned}\bar{\pi} &= \lim_{n \rightarrow \infty} \prod_{j=1}^{n-1} \left(1 - \frac{[j]}{[j+1]}\right) = \lim_{n \rightarrow \infty} \frac{[1]_{\frac{q^n-1}{q-1}}}{L_n}, \text{ hence,} \\ \lim_{n \rightarrow \infty} E_n &= \lim_{n \rightarrow \infty} (L_n)^{\frac{q-1}{q^{n+1}-q}} = \lim_{n \rightarrow \infty} \left(\frac{[1]_{\frac{q^n-1}{q-1}}}{\bar{\pi}_n} \right)^{\frac{q-1}{q^{n+1}-q}} = \frac{\lim_{n \rightarrow \infty} \left([1]_{\frac{1}{q-1}} \right)^{\frac{(q^n-1)(q-1)}{q^{n+1}-q}}}{\lim_{n \rightarrow \infty} \bar{\pi}_n^{\frac{1}{q^{n+1}-q}}} = \alpha [1]_{\frac{1}{q}},\end{aligned}$$

where $\alpha = (1)_{\frac{1}{q}} \in \overline{\mathbb{F}_q}$. Since $\alpha^q = 1$, its order is 1 and so $\alpha = 1$ which completes the proof. \square

In [17], D. Lehmer showed that $\Phi'_n(0) = \mu(n)$, $\Phi''_n(0) = 1 - \mu(n)$. In general, we have a closed formula for $\Phi_n^{(s)}(0)$. This is $\Phi_n^{(s)}(0) = s!c_{n,s}$, where $c_{n,s}$ is the coefficient of x^s in $\Phi_n(x)$. The explicit formula for $c_{n,s}$ was given by A. Grytczuk and B. Tropicak in [13]. Unfortunately, there is no analogous construction in the $\mathbb{F}_q[T]$ case. This is because $\Phi_m^{(s)}(0) = 0$ for all $s \geq p$. However, we have a few results, e.g., ([3], Corollary 1.2 (a)) tells us that the coefficient of x^s in $\Phi_m(x)$ is 0 whenever $s \not\equiv 0 \pmod{q-1}$ except when $q = 2$. So for the coefficient of x , it suffices to study this exception. It was O. Hölder who first proved that $\Phi'_n(1) = \frac{1}{2}\varphi(n)e^{\Lambda(n)}$, [17]. Continuing our philosophy, Theorem 3.1.6 is an analogue of Hölder's result.

Theorem 3.1.6. *Let $q = 2$, then we have $\Phi'_1(0) = 1$, and if $\deg(m) \geq 1$ then,*

$$\Phi'_m(0) = \frac{\Phi_m(0)\phi_*(m)}{T(T+1)},$$

where $\phi_*(m)$ is the analogue of the Pillai arithmetical function.

Proof. It is trivial, when $m = 1$, as $\Phi_m(x) = x$ and so $\Phi'_m(0) = 1$. Let $m \in A_+$, $\deg(m) \geq 1$,

$$\Phi_m(x) = \prod_{D|m} \rho_D(x)^{\mu\left(\frac{m}{D}\right)} = \prod_{D|m} \rho_D^+(x)^{\mu\left(\frac{m}{D}\right)},$$

where $\rho_D^+(x) = \frac{\rho_D(x)}{x}$, so $\rho_D^+(0) = D$. Taking logarithmic derivatives on both sides,

$$\frac{\Phi'_m(x)}{\Phi_m(x)} = \sum_{D|m} \mu\left(\frac{m}{D}\right) \frac{(\rho_D^+(x))'}{\rho_D^+(x)},$$

so we have

$$\begin{aligned}\Phi'_m(0) &= \left(\Phi_m(x) \sum_{D|m} \mu\left(\frac{m}{D}\right) \frac{(\rho_D^+(x))'}{\rho_D^+(x)} \right) \Big|_{x=0} = \sum_{D|m} \mu\left(\frac{m}{D}\right) \left\{ \Phi_m(x) \frac{(\rho_D^+(x))'}{\rho_D^+(x)} \right\} \Big|_{x=0} \\ &= \sum_{D|m} \mu\left(\frac{m}{D}\right) \Phi_m(0) \left\{ \frac{\frac{D^2-D}{T^2-T}}{D} \right\} = \Phi_m(0) \sum_{D|m} \mu\left(\frac{m}{D}\right) \frac{D-1}{T^2-T} \\ &= \frac{\Phi_m(0)}{T(T+1)} \sum_{D|m} \mu\left(\frac{m}{D}\right) (D-1) = \frac{\Phi_m(0)}{T(T+1)} \sum_{D|m} D \mu\left(\frac{m}{D}\right) = \frac{\Phi_m(0)\phi_*(m)}{T(T+1)},\end{aligned}$$

where $\phi_*(m)$ by Proposition 1.2.6 is the analogue of Pillai arithmetical function. \square

Remark 3.1.7. Theorem 3.1.6 is close to Hölder's result in the sense that 2 is replaced by $T(T+1)$, a condition that may be interpreted as being 'even' in $\mathbb{F}_2[T]$. We also saw that $e^{\Lambda(n)}$ is an analogue of $\Phi_m(0)$, whereas $\varphi(n)$ and $\phi_*(m)$ share many properties in their respective rings.

We now describe a technique for extracting coefficients of $\Phi_m(x)$ using i th derivatives.

Proposition 3.1.8. Let $f(x) = \sum_{i=0}^n a_i x^i$ be of degree n , and $0 \leq s \leq q-1$, we have for any $i \geq s$,

$$s!a_i = \left(x^{-(i-s)} f(x) \text{MOD}(x^{-1}) \right)^{(s)}(0), \quad (3.1)$$

where $\text{MOD}(x^{-1})$ means throwing away any negative powers of x .

Proof. Let $0 \leq i \leq p-1$, where p is the characteristic of \mathbb{F}_q . By Taylor's expansion we have $i!a_i = f^{(i)}(0)$. Otherwise, let $0 \leq s \leq q-1 < i$ and compute $\left(x^{-(i-s)} f(x) (\text{MOD}(x^{-1})) \right)^{(s)}(0)$, where $\text{MOD}(x^{-1})$ means throwing away any negative powers of x .

$$\left(x^{-(i-s)} f(x) \right) \text{MOD}(x^{-1}) = \left(\sum_{j=0}^{\varphi(m)} a_j x^{j-i+s} \right) \text{MOD}(x^{-1}) = \sum_{j=i-s}^{\varphi(m)} a_j x^{j-i+s} (\text{MOD}(x^{-1})).$$

We now evaluate the s th derivative of $\left(x^{-(i-s)} f(x) \right) \text{MOD}(x^{-1})$ at 0 as follows,

$$\left(x^{-(i-s)} f(x) (\text{MOD}(x^{-1})) \right)^{(s)}(0) = \left(\sum_{j=i-s}^{\varphi(m)} \frac{(j-i+s)!}{(j-i)!} a_j x^{j-i} (\text{MOD}(x^{-1})) \right)(0) = s!a_i.$$

\square

Corollary 3.1.9. Let $\Phi_m(x) = \sum_{i=0}^{\varphi(m)} c_{m,i} x^i$, then

$$c_{m,i} = \left(x^{-(i-1)} \Phi_m(x) (\text{MOD}(x^{-1})) \right)^{(1)}(0) = - \left(x^{-(i-(q-1))} \Phi_m(x) (\text{MOD}(x^{-1})) \right)^{(q-1)}(0).$$

Proof. Take $s = 1$ and $s = q-1$ respectively. \square

Although we know a lot about $\Phi_m(x)$, some properties of its coefficients are still imperfectly understood and are still a mystery. In the following theorem, we study some of these properties over $\mathbb{F}_2[T]$ and obtain an analogue of result due to D. Lehmer [17].

Theorem 3.1.10. Let $q = 2$ and P be a prime, then $\Phi_1(1) = 1$, $\Phi_T(1) = T+1$, $\Phi_{T+1}(1) = T$ and

$$\Phi_m(1) = \begin{cases} 0, & m = T(T+1) \\ P, & m = T(T+1)P^s, s \geq 1 \\ 1, & \text{otherwise.} \end{cases}$$

Proof. To prove this result, we first show that,

$$\rho_m(1) = \begin{cases} 0, & m \equiv 0 \pmod{T(T+1)} \\ T, & m \equiv 0 \pmod{T+1} \text{ and } m \equiv 1 \pmod{T} \\ T+1, & m \equiv 1 \pmod{T+1} \text{ and } m \equiv 0 \pmod{T} \\ 1, & \text{otherwise.} \end{cases}$$

Let us first show that $\rho_{T^n}(1) = 1 + T$ for each $n \in \mathbb{Z}_+$. We prove this by induction on n . Let S_n be the statement that $\rho_{T^n}(1) = 1 + T$ for $n \in \mathbb{Z}_+$. Since $\rho_T(x) = x^T + Tx$, we have $\rho_T(1) = 1 + T$ and so S_1 is true. Assume that S_l is true, i.e., $\rho_{T^l}(1) = 1 + T$, where $l \in \mathbb{Z}_+$. We are left to check that S_{l+1} is also true. In this case, we have $\rho_{T^{l+1}}(1) = \rho_T(\rho_{T^l}(1)) = \rho_T(1 + T) = (1 + T)^2 + T(1 + T) = 1 + T$. So S_n is a true statement. Applying Theorem 2.2.8, we get $\rho_{(T+1)^n}(1) = T$. Moreover, $\rho_{T(T+1)}(1) = 1^4 + (T^2 + T + 1)(1)^2 + (T^2 + T)(1) = 0$ and so if $m \equiv 0 \pmod{T(T+1)}$, then $\rho_m(1) = \rho_{m_0}(\rho_{T(T+1)}(1)) = 0$. Suppose m is a prime in $\mathbb{F}_2[T]$ of degree strictly greater than 1, then it consists of an odd number of terms of which the constant term is 1. So $\rho_P(1) = (\text{even number of terms})(T + 1) + \rho_1(1) = \rho_1(1) = 1$. If m is a product of primes of degree greater than 1, then $\rho_m(1) = 1$. Lastly, we have,

1. $m \equiv 0 \pmod{T+1}$ and $m \equiv 1 \pmod{T}$. Suppose $m = (T+1)^s m_0$, where $(T+1)^s \parallel m$, $m_0 \equiv 1 \pmod{T}$ and $m_0 \equiv 1 \pmod{T+1}$ imply either m_0 is prime or a product of higher degree primes. So $\rho_{m_0}(1) = 1$ and $\rho_m(1) = \rho_{(T+1)^s}(\rho_{m_0}(1)) = \rho_{(T+1)^s}(1) = T$.
2. $m \equiv 1 \pmod{T+1}$ and $m \equiv 0 \pmod{T}$. Suppose $m = T^s m_1$, where $T^s \parallel m$. Now $m_1 \equiv 1 \pmod{T+1}$ and $m_1 \equiv 1 \pmod{T}$ imply either m_1 is prime or a product of higher degree primes. So $\rho_{m_1}(1) = 1$ and $\rho_m(1) = \rho_{T^s}(\rho_{m_1}(1)) = \rho_{T^s}(1) = T + 1$.

We now compute $\Phi_m(1)$, we shall do this in 4 steps, the first cases being trivial.

1. $m = T(T+1)$, we have $\Phi_m(1) = 0$ since $\Phi_{T(T+1)}(x) = x + 1$.
2. $m \equiv 0 \pmod{T+1}$ and $m \equiv 1 \pmod{T}$, take $m = (T+1)^s m_0$, where $(T+1)^s \parallel m$. So,

$$\Phi_m(1) = \frac{\Phi_{m_0}(\rho_{(T+1)^s}(1))}{\Phi_{m_0}(\rho_{(T+1)^{s-1}}(1))} = \begin{cases} \frac{\Phi_{m_0}(T)}{\Phi_{m_0}(T)} = 1, & s \geq 2 \\ \frac{\Phi_{m_0}(T)}{\Phi_{m_0}(1)} = 1, & s = 1, m_0 \neq 1. \end{cases}$$

This follows from $\rho_1(T) = T$, $\rho_T(T) = T^2 + T^2 = 0$ hence $\rho_{T^n}(T) = 0$ for all $n \geq 1$. This means that $\rho_{m_0}(T) = T$ since $m_0 \equiv 1 \pmod{T}$ and so are all its divisors D , $\rho_D(T) = T$. Using the fundamental identity, $\Phi_{m_0}(T) = \prod_{D|m_0} \rho_D(T)^{\mu(\frac{m_0}{D})}$ we obtain $\Phi_{m_0}(T) = 1$. By the same arguments, we have $\rho_{m_0}(1) = 1$ and so $\Phi_{m_0}(1) = 1$.

3. $m \equiv 1 \pmod{T+1}$ and $m \equiv 0 \pmod{T}$, take $m = T^s m_1$, where $T^s \parallel m$. So,

$$\Phi_m(1) = \frac{\Phi_{m_1}(\rho_{T^s}(1))}{\Phi_{m_1}(\rho_{T^{s-1}}(1))} = \begin{cases} \frac{\Phi_{m_1}(T+1)}{\Phi_{m_1}(T+1)} = 1, & s \geq 2 \\ \frac{\Phi_{m_1}(T+1)}{\Phi_{m_1}(1)} = 1, & s = 1, m_0 \neq 1. \end{cases}$$

4. $m \equiv 0 \pmod{T(T+1)}$ and $T^i(T+1)^j \parallel m$, then $m = T^i(T+1)^j m_2$ or $m = T^i(T+1)^j P^l$, where m_2 is coprime to T and $T+1$ and $i, j, l \geq 1$ and has at least two distinct prime factors (of course different from T and $T+1$). In this case first assume $i = j = s$, so

$$\Phi_m(1) = \frac{\Phi_{m_2}(\rho_{(T(T+1))^s}(1))}{\Phi_{m_2}(\rho_{(T(T+1))^{s-1}}(1))} = \begin{cases} \frac{\Phi_{m_2}(0)}{\Phi_{m_2}(0)} = 1, & s \geq 2 \\ \frac{\Phi_{m_2}(0)}{\Phi_{m_2}(1)} = 1, & s = 1, \end{cases}$$

where $\Phi_{m_0}(1) = \Phi_{m_1}(1) = \Phi_{m_2}(1) = 1$, because all the prime divisors of m_2 have degree ≥ 2 and so its value follows from the identity $\Phi_{m_2}(1) = \prod_{D|m_2} \rho_D(1)^{\mu(\frac{m_2}{D})}$, with $\rho_D(1) = 1$. Otherwise, we have two cases left and that is firstly when $m = T(T+1)P^l$. Since $\Phi_{T(T+1)}(\rho_{P^l}(1)) = 0$, we have a case of $\frac{0}{0}$, and so we apply l' Hopital's rule,

$$\Phi_m(1) = \left(\frac{\Phi_{T(T+1)}(\rho_{P^l}(x))}{\Phi_{T(T+1)}(\rho_{P^{l-1}}(x))} \right) \Big|_{x=1} = \left(\frac{(\rho_{P^l}(x) + 1)'}{(\rho_{P^{l-1}}(x) + 1)'} \right) \Big|_{x=1} = P.$$

The case $i \neq j$, (assume $i > j$), then

$$\rho_{T^i(T+1)^j}(1) = \rho_{T^j(T+1)^j}(\rho_{T^{i-j}}(1)) = \rho_{T^j(T+1)^j}(1+T) = \rho_{T^j(T+1)^j}(T) = 0.$$

$$\Phi_m(1) = \frac{\Phi_{m_2}(\rho_{(T(T+1))^j}(T))}{\Phi_{m_2}(\rho_{(T(T+1))^{j-1}}(T))} = \begin{cases} \frac{\Phi_{m_2}(0)}{\Phi_{m_2}(0)} = 1, & j \geq 2 \\ \frac{\Phi_{m_2}(0)}{\Phi_{m_2}(1)} = 1, & j = 1. \end{cases}$$

We have one case left, i.e., $m = T^i(T+1)^j P^l$, i, j such that $i \neq 1$ and $j = 1$ simultaneously. So $\Phi_{T^i(T+1)^j P^l}(1) = \Phi_{T(T+1)P}(\rho_{T^{i-1}(T+1)^{j-1} P^{l-1}}(1)) = \Phi_{T(T+1)P}(0) = 1$.

□

3.2 Statement and proof of an analogue to Suzuki's Theorem

In chapter 2, we explored elementary properties of $\Phi_m(x)$. We saw that, corresponding to each polynomial m in A , is an additive polynomial $\rho_m(x) = \alpha x^{q^n} + \dots + a_1 x^q + a_0 x$, where $\alpha = \text{LC}(m)$, the leading coefficient of m and $a_0 = m$. The statement $a_0 = m$ explicitly implies, A is the set of coefficients of Carlitz polynomials (since m is allowed to run through A). Also for any monic irreducible P in A and any $s \in \mathbb{Z}_+$, Theorem 2.2.7 shows that the constant term of $\Phi_P(x)$ is P . So every prime P in A is a coefficient in some cyclotomic polynomial. The first argument is less informative about the coefficients of cyclotomic polynomials, however the second one assures us that the set of coefficients is larger than the set of primes in A .

We defined our Carlitz polynomial only for monics so that the resulting polynomials are also monic, however the theory still holds if we set m to run over all elements A . This is

because all the elements of A , can be made monic through multiplication by a suitable scalar $\alpha \in \mathbb{F}_q^*$ and $\rho_{\alpha m}(x) = \alpha \rho_m(x)$ for any m in A_+ , plus by definition, cyclotomic polynomials are meant to be monic and irreducible factors of $\rho_m(x)$. Without loss of generality, it is enough to consider only monics in A . Let m be a non zero monic polynomial of degree n , and let

$$\rho_m(x) = \sum_{i=0}^{|m|} a_{m,i} x^i, \quad \Phi_m(x) = \sum_{i=0}^{\varphi(m)} c_{m,i} x^i,$$

set $S(m) = \{a_{m',i} : m' \in mA, i \in \mathbb{Z}_{\geq 0}\}$ and $T(m) = \{c_{m',i} : m' \in mA, i \in \mathbb{Z}_{\geq 0}\}$.

Proposition 3.2.1. $S(1) = A$.

Proof. For each $m \in A$, the coefficient of x in $\rho_m(x)$ is m , implying $m \in S(1)$ and so $A \subseteq S(1)$. Also, we know $\rho_m(x) \in A[x]$ and so we have $S(1) \subseteq A$ implying $S(1) = A$ as sets. \square

Proposition 3.2.2. Set $s(A) = \{\text{all prime polynomials in } A\}$. Then $s(A) \subseteq T(1) \subseteq S(1)$.

Proof. Since A is a PID, all polynomials are characterised by primes in A . For any $P \in s(A)$, by Theorem 2.2.7, the constant coefficient of $\Phi_P(x)$ is $P \in S(1)$ implying that $s(A) \subseteq T(1)$. The upper inclusion is trivial from the fact that $\Phi_m(x) \in A[x]$ and Proposition 3.2.1. \square

In 1987, J. Suzuki [26] showed that every integer is a coefficient in some cyclotomic polynomial. An analogue to Suzuki's Theorem would require the second inclusion in Proposition 3.2.2 to be an equality. It turns out to be true, however, to prove this is not straight forward. In stead, we prove Theorem 3.2.4, an analogue of a result due to C. Ji, W. Li and P. Moree [16] on coefficients of cyclotomic polynomials, to which Theorem 3.2.3 is a corollary. Ji. et al., showed that Suzuki's Theorem holds when the parametrising set is replaced by $n\mathbb{Z}_+$, n fixed.

Theorem 3.2.3 (Analogue of Suzuki's Theorem, ([26], Theorem)). $T(1) = A$, i.e., for any $a \in A$, there exists an $m \in A$ and a non negative integer i such that $c_{m,i} = a$.

Theorem 3.2.4. Let $m^* \in A_+$, and \mathfrak{a} be the principal ideal generated by $m_1 := \frac{m^*}{m_0^*}$, then $\mathfrak{a} \subseteq T(m^*)$.

To prove Theorem 3.2.3, we shall first prove Theorem 3.2.4, but this requires Lemma 3.2.5.

Lemma 3.2.5. Let $m \in A$ be of degree $d > 0$, m_0 be the squarefree part of m , $w_m(x) = \sum_{i=0}^d w_{m,i} x^{q^i}$, $w_{m,i} \neq 0$ for $1 < i \leq d$, be a monic additive polynomial in $k[x]$. Let $0 \leq j \leq s := \varphi(m_0)$, if $x^{q^d(s-1)+1}$ occurs in $x^j w_m(x)^{s-j}$ then either $j = 0$ and $w_{m,0} \neq 0$ or $j = 1$ and $w_{m,1} \neq 0$.

Proof. Let $w_m(x) = \sum_{i=0}^d w_{m,i} x^{q^i}$, where $d := \deg(m) > 0$, using the Multinomial Theorem,

$$\begin{aligned} x^j w_m(x)^{s-j} &= x^j \left(\sum_{i=0}^d w_{m,i} x^{q^i} \right)^{s-j} = x^j \sum_{t_0 + \dots + t_d = s-j} \prod_{i=1}^d (w_{m,i} x^{q^i})^{t_i} \\ &= x^j \sum_{t_0 + \dots + t_d = s-j} (\text{coefficient}) x^{\sum_{i=0}^d q^i t_i}. \end{aligned} \quad (3.2)$$

To get non zero terms of the form $bx^{q^d(s-1)+1}$, $b \in A$, we solve Equations (3.3) and (3.4),

$$j + \sum_{i=0}^d q^i t_i = q^d(s-1) + 1 \quad (3.3)$$

$$t_0 + \cdots + t_d = s - j, \quad (3.4)$$

simultaneously. Using Equation (3.4), eliminate s from Equation (3.3), to get

$$j + \sum_{i=0}^d q^i t_i = q^d(j + \sum_{i=0}^d q^i t_i - 1) + 1.$$

Expressing j in terms of t_i 's yields the following relation,

$$j = 1 - \frac{1}{q^d - 1} \sum_{i=0}^d (q^d - q^i) t_i.$$

Since $q^d - q^i, t_i \geq 0$ for $0 \leq i \leq d$ and $j \in \mathbb{Z}_{\geq 0}$, we have two possible values of j , i.e, $j = 0$ or 1 . Since m_0 is a squarefree non constant polynomial, $0 < s \leq \varphi(m_0) \leq q^d$ and $t_i \geq 0$. So,

1. Case 1, when $j = 0$. We have $\sum_{i=0}^d (q^d - q^i) t_i = q^d - 1$, but this is true if and only if $t_0 = 1$, $t_i = 0$ for $0 < i < d$ and $t_d = s - 1$. Otherwise, suppose $0 < u < d$ is the least index such that $t_u \neq 0$, then $q^{d-u} - q^j > 0$ for all $0 \leq j < d - u$, and $\sum_{i=0}^d (q^d - q^i) t_i = q^u (\sum_{i=0}^{d-u} (q^{d-u} - q^i) t_{u+i}) = q^{ul}$ for some $l \in \mathbb{Z}_+$. But this implies q divides $q^d - 1$, which is impossible. In addition, since $w_m(x)$ has degree q^d , it easy to see from the third part of Equation (3.2) that the term $bx^{q^d(s-1)+1} \neq 0$ only if $w_{m,0} \neq 0$.
2. Case 2, when $j = 1$. This means $\frac{1}{q^d - 1} \sum_{i=0}^d (q^d - q^i) t_i = 0$ which is equivalent to solving the following equation $\sum_{i=0}^d (q^d - q^i) t_i = 0$. This is true if and only if $t_i = 0$ for $0 \leq i < d$ and $t_d = s - 1$. Similarly, we have $bx^{q^d(s-1)+1} \neq 0$ if $w_{m,1} \neq 0$.

This completes the proof of Lemma 3.2.5. □

Proof of Theorem 3.2.4. Let $m^* \in A_+$ and m_0^* be its squarefree part, so $m_1 := \frac{m^*}{m_0^*}$, $\mathfrak{a} = m_1 A$ and $T(m^*) = \{c_{m^* m', i} : m' \in A, i \in \mathbb{Z}_{\geq 0}\}$. We shall show that $\mathfrak{a} \subseteq T(m^*)$. To do this, let $0 \neq m \in \mathfrak{a}$, so $m = m_1 N$ for some $N \in A$. Take $M := m m_0^* f_0$, where f_0 is the product of prime factors of N coprime to m^* . By Theorem 2.2.6 $\Phi_M(x) = \Phi_{m_0^* f_0}(\rho_m(x))$. It suffices to show that m is a coefficient in $\Phi_M(x)$, so $m \in T(m^*)$. Since m is arbitrary, $m \in T(m^*) \Rightarrow \mathfrak{a} \subseteq T(m^*)$.

Given a non zero polynomial $m \in \mathfrak{a}$, set $m_0 := m_0^* f_0$ to be its squarefree part. Then we have $\varphi(m_0) \equiv (-1)^t \equiv \mu(m_0) \pmod{q}$, where t is the number of distinct prime factors of m_0 . We shall show that $\mu(m_0)m$ is a coefficient in $\Phi_M(x)$. By Theorem 2.2.6, $\Phi_M(x) = \Phi_{m_0}(\rho_m(x))$ so we can write $\Phi_{m_0}(x) = x^{\varphi(m_0)} + g_{m_0}(x)$, where $g_{m_0}(x)$ is an integer polynomial in A in lower degree terms. It is enough to just search the coefficient of $x^{|m|(\varphi(m_0)-1)+1}$ in

$$\Phi_M(x) = \Phi_{m_0}(\rho_m(x)) = (\rho_m(x))^{\varphi(m_0)} + g_{m_0}(\rho_m(x)).$$

The degree of $g_{m_0}(\rho_m(x))$ is at most $|m|(\varphi(m_0) - 1) < |m|(\varphi(m_0) - 1) + 1$, so no term in $g_{m_0}(\rho_m(x))$, contributes to the coefficient of $x^{|m|(\varphi(m_0)-1)+1}$. We concentrate on the first term, and split it into two terms as follows, $\rho_m(x) = mx + h_m(x)$, where $h_m(x)$ is a polynomial in higher degree terms. Expanding $(mx + h_m(x))^{\varphi(m_0)}$ using the Binomial Theorem, we get

$$\begin{aligned}\Phi_M(x) &= (h_m(x) + mx)^{\varphi(m_0)} + g_{m_0}(\rho_m(x)) \\ &= \sum_{j=0}^{\varphi(m_0)} \binom{\varphi(m_0)}{j} (mx)^j h_m(x)^{\varphi(m_0)-j} + g_{m_0}(\rho_m(x)) \\ &= \left[h_m(x)^{\varphi(m_0)} + \mu(m_0)mxh_m(x)^{\varphi(m_0)-1} + \dots + (mx)^{\varphi(m_0)} \right] + g_{m_0}(\rho_m(x))\end{aligned}$$

By Lemma 3.2.5, there is no term of the form $bx^{|m|(\varphi(m_0)-1)+1}$ in $(mx)^j h_m(x)^{\varphi(m_0)-j}$ except possibly when $j = 0$ or 1 . Since $h_m(x)$ has no term in x , by Lemma 3.2.5, the case when $j = 0$ is excluded. So we concentrate on $\mu(m_0)mxh_m(x)^{\varphi(m_0)-1}$ and write $h_m(x) := x^{|m|} + i_m(x)$, where $i_m(x)$ is a polynomial in lower degree terms, but with the lowest term $a_{m,1}x^q \neq 0$.

$$\begin{aligned}\Phi_M(x) &= h_m(x)^{\varphi(m_0)} + \mu(m_0)mx(x^{|m|} + i_m(x))^{\varphi(m_0)-1} + \dots + (mx)^{\varphi(m_0)} + g_{m_0}(\rho_m(x)) \\ &= h_m(x)^{\varphi(m_0)} + \left[\mu(m_0)mx^{|m|(\varphi(m_0)-1)+1} + \dots \right] + \dots + (mx)^{\varphi(m_0)} + g_{m_0}(\rho_m(x)).\end{aligned}$$

To have the coefficient as m , for any $m \in A$, set $M = \mu(m_0)m_0m$, and $\Phi_{\alpha m}(x) = \alpha\Phi_m(x)$. \square

Remark 3.2.6. Theorem 3.2.4 is weaker analogue of the result due to C. Ji et al. in the sense that, $T(m) \supseteq \frac{m}{m_0}A$, where m_0 is the squarefree part of m . It is still an open question whether $T(m) = A$?

Corollary 3.2.7. If m^* is a squarefree polynomial, then $T(m^*) = A$.

Proof. m^* - squarefree $\Rightarrow m_1 = \frac{m^*}{m_0^*} = 1$, so $a = A$. By Theorem 3.2.4, $A \subseteq T(m^*) \subseteq A$. \square

In particular, Theorem 3.2.3 is proved. It is worth mentioning, Theorem 3.2.3 was conjectured and proved after a series of experiments done with the SAGE computer algebra system [25]. Like the classical theorem of Suzuki, our construction gives a procedure to locate a given m as coefficient in some Carlitz cyclotomic polynomial. The examples below illustrate this.

Example 3.2.8. Take $q = 2$ and $m = T^5 + T^4 + T^2 + T = T(T+1)^2(T^2+T+1)$. Then the squarefree part of m is $m_0 = T(T+1)(T^2+T+1)$, so $M = mm_0 = T^2(T+1)^3(T^2+T+1)^2$, and $M_0 = m_0$. Clearly $\mu(M_0) = -1 = 1$, $s = \varphi(M_0) = 3$ and $l = |m|(\varphi(M_0) - 1) + 1 = 65$. Using SAGE software, we search $c_{\mu(M_0)M,l}$, the coefficient of x^l in $\Phi_{\mu(M_0)M}(x)$. It turns out that the coefficient of x^l in $\Phi_{\mu(M_0)M}(x)$ is $T^5 + T^4 + T^2 + T$. Below are a few terms of $\Phi_{\mu(M_0)M}(x)$,

$$\begin{aligned}\Phi_{\mu(M_0)M}(x) &= x^{96} + (T^{16} + T^8 + T^4 + T^2 + T + 1)x^{80} + (T^{16} + T^{12} + T^{10} + T^9 + T^6 + \\ &\quad T^5 + T^3 + T)x^{72} + (T^{12} + T^{10} + T^9 + T^7 + T^6 + T^2 + 1)x^{68} + (T^8 + T^7 + \\ &\quad T^3 + T^2 + T + 1)x^{66} + (T^5 + T^4 + T^2 + T)x^{65} + (T^{32} + T^{16} + T^8 + T^4 + \\ &\quad T^2)x^{64} + \dots + (T^{15} + T^{14} + T^{13} + T^{11} + T^{10} + T^8 + T^7 + T^5 + T^4 + T^3)x^3 + \\ &\quad (T^5 + T^4 + T^2 + T)x^2 + (T^7 + T^5 + T^4 + T^2)x + 1.\end{aligned}$$

Example 3.2.9. Take $q = 3$ and $m = T^4 + 2T^3 + 2T^2 + 2T + 1 = (T + 1)^2(T^2 + 1)$. Then the squarefree part of m is $m_0 = (T + 1)(T^2 + 1)$, so $M = mm_0 = (T + 1)^3(T^2 + 1)^2$, and $M_0 = m_0$. Clearly $\mu(M_0) = 1$, $s = \varphi(M_0) = 16$ and $l = |m|(\varphi(M_0) - 1) + 1 = 1216$. Using SAGE software, we search $c_{\mu(M_0)M,l}$, the coefficient of x^l in $\Phi_{\mu(M_0)M}(x)$. It turns out that the coefficient of x^l in $\Phi_{\mu(M_0)M}(x)$ is $T^4 + 2T^3 + 2T^2 + 2T + 1$. Below are a few terms of $\Phi_{\mu(M_0)M}(x)$,

$$\begin{aligned} \Phi_{\mu(M_0)M}(x) = & x^{1296} + (T^{27} + T^9 + T^3 + T + 2)x^{1242} + (T^{18} + T^{12} + T^{10} + 2T^9 + T^6 + T^4 + \\ & 2T^3 + T^2 + 2T + 2)x^{1224} + (T^9 + T^7 + 2T^6 + T^5 + 2T^4 + 2T^2 + 2T + 2)x^{1218} + \\ & (T^4 + 2T^3 + 2T^2 + 2T + 1)x^{1216} + (2T^{81} + 2T^{27} + 2T^9 + 2T^3 + 2T)x^{1134} + \\ & (2T^{108} + 2T^{90} + 2T^{84} + 2T^{82} + T^{81} + T^{54} + T^{27} + T^{18} + T^9 + T^6 + T^3 + T^2 + \\ & T + 2)x^{1080} + \dots + (2T^{20} + 2T^{19} + 2T^{18} + T^{17} + 2T^{12} + 2T^{11} + T^{10} + 2T^9 + \\ & T^8 + 2T^7 + 2T^6 + 2T^5 + 2T^4 + T^3 + 2T^2 + 2T)x^4 + (T^{11} + T^9 + T^8 + 2T^7 + \\ & T^6 + 2T^5 + 2T^4 + 2T^2)x^2 + 1. \end{aligned}$$

Remark 3.2.10. The above procedure is sufficient to guarantee existence of such a polynomial, we are not claiming that it is unique or optimal. For example, if m is a prime, the above procedure requires us to compute $\Phi_{-p^2}(x)$ to check for the existence of P . However, we can also use $\Phi_P(x)$.

In summary,

–	Classical cyclotomic polynomials $\Phi_n(x)$	Carlitz cyclotomic polynomials $\Phi_m(x)$
1	$s, n \in \mathbb{Z}_+, p$ a prime	$m \in A_+, P \in A$ monic irreducible
2	$\mathcal{A}_p(p^s) = s$	$\mathcal{A}_P(P) = 1, \mathcal{A}_P(P^s) = (s - 1)(q^{\deg(P)} - 1)$
3	–	$\mathcal{H}(m) = \sum_{D m} \mu\left(\frac{m}{D}\right)q^{\deg(D)}$
4	Lebesque’s Result ([17])	see Theorem 2.2.7
5	Lehmer’s Theorem ([17], Theorem 1)	see Theorem 3.1.5
6	Holder’s Result ([17])	see Theorem 3.1.6
7	Ji., etal’s Result ([16], Theorem 1)	see Theorem 3.2.4 (Weaker form)
8	Suzuki’s Theorem ([26], Theorem)	see Theorem 3.2.3
9	⋮	⋮

Table 3.1. Analogy between classical and Carlitz cyclotomic polynomials.

We stated some results on prime and absolute heights of $\Phi_m(x)$. In $\mathbb{F}_2[T]$, we computed the values of $\Phi_m(x)$ and $\Phi'_m(x)$ at some special torsions giving analogues of O. Hölder and D. Lehmer’s results in these cases. Lastly, we proved an $\mathbb{F}_q[T]$ analogue of Suzuki’s Theorem.

Chapter 4

The Carlitz Bang Zsigmondy Theorem and Carlitz Wieferich primes (Part I)

In this chapter, we shall discuss a few applications of the theory of Carlitz (cyclotomic) polynomial developed so far. We shall study the factors of the homogeneous form of $\rho_m(x)$, the Carlitzian A analogues of Zsigmondy primes, Fermat pseudoprimes and Wieferich primes. Our proofs of results on Carlitz Wieferich primes are quantitative rather than qualitative. *Part of this work has been submitted for publication in peer reviewed journals, e.g., see [5].*

4.1 Zsigmondy and non Zsigmondy primes in $\mathbb{F}_q[T]$

Recall from elementary number theory that, if a, n are integers greater than 1, then a prime p is called a Zsigmondy prime for the pair $\langle a, n \rangle$ if $p \nmid a$ and the order of a modulo p is n . The order of a modulo p is the smallest positive integer s such that $a^s \equiv 1 \pmod{p}$. The simplest class of Zsigmondy primes is the sequence $Z(n, 2, 1)$, i.e., the Zsigmondy primes of $\langle 2, n \rangle$, where $n \in \mathbb{Z}_+$. $Z(n, 2, 1) = 3, 7, 5, 31, (1), 127, 17, 73, 11, \dots$ (SLOANE'S **A064078**, OEIS). (1) means there is no Zsigmondy prime for $n = 6$. We shall say more on this in the Bang - Zsigmondy Theorem. If p is a Zsigmondy prime for the pair $\langle a, n \rangle$, then n divides $p - 1$ and so $p \geq n + 1$. A Zsigmondy prime for the pair $\langle a, n \rangle$ is called large if $p > n + 1$ or $a^n \equiv 1 \pmod{p^2}$. This implies that all Wieferich primes to the base a are also large Zsigmondy primes. We shall explore more about Wieferich primes in section 4.3. Lastly, p is a non Zsigmondy prime for the pair $\langle a, n \rangle$ if $p \nmid a$ and the order of a modulo p is less than n .

The above construction can be understood as taking place in the abelian group $(\mathbb{Z}/p\mathbb{Z})^*$, a \mathbb{Z} module. To characterise the Carlitzian A analogue of Zsigmondy and non Zsigmondy factors of the pair $\langle f, N \rangle$, where f, N are non constant polynomials in A , we replace the

standard \mathbb{Z} action on $(\mathbb{Z}/p\mathbb{Z})^*$ by the Carlitz module action on the abelian group (A/PA) .

Proposition 4.1.1 (Carlitz (additive) Analogue of Fermat's Little Theorem). *Let P be a prime in A . Then for any $a \in A$, we have $\rho_{P-1}(a) \equiv 0 \pmod{P}$.*

Proof. We have $\rho_{P-1}(a) = \rho_P(a) - a \equiv a^{q^{\deg(P)}} - a = a(a^{q^{\deg(P)-1} - 1}) \equiv 0 \pmod{P}$. The first congruence follows by Theorem 3.1.1 whereas the last one follows from Corollary 4.3.5. \square

Let $m \in A_+$ and $\mathcal{C} = (\mathbb{G}_a, \rho)$ be the Carlitz A -module. Then reduction of \mathcal{C} modulo mA turns A/mA into a finite A module denoted by $\mathcal{C}(A/mA)$ with multiplication by elements of A given by the Carlitz module ρ . Let $f \in A$, we define the annihilator ideal of f modulo m to be the ideal $\text{Ann}_m(f) := \{a \in A : \rho_a(f) \equiv 0 \pmod{m}\}$. Since A is a PID, there exists an $l \in A_+$ such that $\text{Ann}_m(f) = lA$, i.e., monic polynomial of least degree such that $\rho_l(f) \equiv 0 \pmod{m}$. We call this generator of $\text{Ann}_m(f)$, the Carlitz order of f modulo m .

Definition 4.1.2. *Let f, N be non constants in A .*

1. P is a Carlitz Zsigmondy prime (or a c -Zsigmondy prime) for the pair $\langle f, N \rangle$ if
 - (i) $P \nmid f$,
 - (ii) N is the Carlitz order of f modulo P .
2. P is a large c -Zsigmondy prime for the pair $\langle f, N \rangle$ if P is a c -Zsigmondy prime for $\langle f, N \rangle$ and either $\deg(P) > \deg(N)$ or $\rho_N(f) \equiv 0 \pmod{P^2}$.
3. Q is a non c -Zsigmondy prime for $\langle f, N \rangle$ if Q is not a c -Zsigmondy prime for $\langle f, N \rangle$.

The requirement $P \nmid f$ excludes the trivial case. This is because, if $P \mid f$, then $\text{Ann}_P(f) = A$, and so its generator as an A -ideal is 1. So the Carlitz order N of f modulo P is 1, which contradicts the assumption that N is non constant. If P is a c -Zsigmondy prime for the pair $\langle f, N \rangle$, then $\Phi_N(f) \equiv 0 \pmod{P}$. The following two propositions characterise the c -Zsigmondy prime factors of $\rho_N(f)$. We shall need the following lemma on Carlitz orders.

Lemma 4.1.3. *If a prime factor P of $\Phi_N(f)$ is coprime to N , then P is a c -Zsigmondy prime.*

Proof. Given $P \mid \Phi_N(f)$, assume P is not a c -Zsigmondy prime for $\langle f, N \rangle$. Then there exists a prime factor Q of N such that $\rho_{\frac{N}{Q}}(f) \equiv 0 \pmod{P}$. Since $\Phi_N(x)$ divides $\rho_N(x)$ but not $\rho_{\frac{N}{Q}}(x)$, we have $\Phi_N(x)$ divides $\Phi_Q(\rho_{\frac{N}{Q}}(x))$. Since P is a prime factor of $\Phi_N(f)$, we have P divides $\Phi_Q(\rho_{\frac{N}{Q}}(f)) \equiv \Phi_Q(0) \equiv Q \pmod{P}$, (since $\rho_{\frac{N}{Q}}(f) \equiv 0 \pmod{P}$) implying $Q = P$ and so P divides N . This means if $P \nmid N$, then P is a c -Zsigmondy prime for $\Phi_N(f)$. \square

Proposition 4.1.4. *A prime factor P of $\Phi_N(f)$ is c -Zsigmondy for $\langle f, N \rangle$ if and only if $P \nmid N$.*

Proof. (\Rightarrow) Given that $P \mid \Phi_N(f)$ and so $\rho_N(f) \equiv 0 \pmod{P}$. Suppose that $P \mid N$. Then $\rho_N(f) \equiv \rho_P(\rho_{\frac{N}{P}}(f)) \equiv \rho_{\frac{N}{P}}(f)^{|P|} \equiv \rho_{\frac{N}{P}}(f) \equiv 0 \pmod{P}$, so P is not a Zsigmondy prime for $\langle f, N \rangle$. Therefore, if P is a (c - Zsigmondy) prime factor of $\Phi_N(f)$, then P does not divide N .

(\Leftarrow) See Lemma 4.1.3. □

Corollary 4.1.5. *A prime factor P of $\Phi_N(f)$ is non c - Zsigmondy for $\langle f, N \rangle$ if and only if $P \mid N$.*

Lemma 4.1.6. *Let $f, N \in A_+$, $(f, N) = 1$ and P be a non c - Zsigmondy prime factor of $\Phi_N(f)$. The Carlitz order of f modulo P is NP^{-s} , where s is such that $P^s \parallel N$.*

Proof. Corollary 4.1.5 asserts that if P is a non c - Zsigmondy prime factor of $\Phi_N(f)$, then $\rho_{\frac{N}{P}}(f) \equiv 0 \pmod{P}$. So $\rho_{\frac{N}{P_1}}(f) \not\equiv 0 \pmod{P}$ for any prime factor P_1 of N different from P , so the Carlitz order of f modulo P is of the form $\frac{N}{P^t}$ for some $t \geq 1$. To see this, let $N = mP^s$, where $P^s \parallel N$, since $\rho_N(f) \equiv 0 \pmod{P}$, we have $\rho_P(\rho_{mP^{s-1}}(f)) \equiv (\rho_{mP^{s-1}}(f))^{|P|} \equiv 0 \pmod{P}$ implying $\rho_{mP^{s-1}}(f) \equiv 0 \pmod{P}$, and this goes on until $\rho_m(f) \equiv 0 \pmod{P}$. We can not go further because $P \nmid m$. Since P divides $\rho_m(f)$ but not m and f , it must divide $\Phi_m(f)$, and so P is a primitive factor of $\rho_m(f)$. In other words, $m = \frac{N}{P^t}$ is the Carlitz order of f modulo P . □

Theorem 4.1.7. *Let $f, N \in A_+$, $(f, N) = 1$. Then $\Phi_N(f)$ has at most two non c - Zsigmondy prime factors. If it has one, then it is the largest prime $P \mid N$. If it has two, then they differ by ± 1 .*

Proof. Given $f, N \in A_+$, $(f, N) = 1$ and a non c - Zsigmondy prime P for $\Phi_N(f)$. Lemma 4.1.6 says that the Carlitz order of f modulo P is of the form $\frac{N}{P^s}$ where $P^s \parallel N$. Suppose that $N_1 = \frac{N}{P^s}$ is the Carlitz order of f modulo P , then N_1 divides $P - 1$, since $\rho_{P-1}(f) \equiv 0 \pmod{P}$. Therefore, P is one of the largest (in degree) prime factors of N .

The second largest (in degree) prime factor of N would be $P_1 = \frac{N}{P^s}$. But this can only occur if $P - P_1 = \pm 1$, since P_1 is a prime that must divide $P - 1$, and $\deg(P_1) = \deg(P - 1)$. □

Theorem 4.1.8. *Let P be a prime, $f, N \in A$, $N = mP^s$, $s \in \mathbb{N}$, $P \nmid m, f$. The Carlitz order of f mod P is m if and only if $P \mid \Phi_N(f)$. The other prime factors Q of $\Phi_N(f)$ are c - Zsigmondy for $\langle f, N \rangle$.*

To prove Theorem 4.1.8, we shall need Lemma 4.1.9 below.

Lemma 4.1.9. *Suppose P is a prime and g is a non zero polynomial divisible by P , then*

1. $g^{-1}\rho_P(g) \equiv 0 \pmod{P}$.
2. $\rho_P(g) \equiv 0 \pmod{P^2}$.
3. $g^{-1}\rho_P(g) \equiv P \pmod{P^2}$ for $q \geq 2$, except when $q = 2$, $\deg(P) = 1$ and $g \equiv P \pmod{P^2}$.

Proof. Given $g \equiv 0 \pmod{P}$, then $g^{-1}\rho_P(g) = P + a_{P,1}g^{q-1} + \dots + g^{q^{\deg(P)}-1} \equiv 0 \pmod{P}$. It is clear that (1) \Rightarrow (2). To prove (3), there are two cases involved.

1. Case 1. $q \geq 2, \deg(P) \neq 1$. Since $q \geq 2$ and $\deg(P) > 1$, we have $q^{\deg(P)} > 2$ and

$$g^{-1}\rho_P(g) = P + a_{P,1}g^{q-1} + \dots + g^{q^{\deg(P)}-1}.$$

By Theorem 3.1.1, $a_{P,i} \equiv 0 \pmod{P}$ for $i \leq q^{\deg(P)} - 1$, so $g^{-1}\rho_P(g) \equiv P \pmod{P^2}$.

2. $q = 2$ and $\deg(P) = 1$. We have $g^{-1}\rho_P(g) = P + g \equiv P + g \pmod{P^2}$, where $g = Pa$ and $a \equiv 0$ or $1 \pmod{P}$. In this case, if $a \equiv 1 \pmod{P}$, then $g^{-1}\rho_P(g) \equiv 0 \pmod{P^2}$.

□

Proof of Theorem 4.1.8. Let $q = 2$ and $N = T(T+1)$. A little computation shows that Theorem 4.1.8 is true in this case. Let \mathcal{D} be the set of monic divisors D of m with $\mu(\frac{m}{D}) \neq 0$. The monic divisors D of N with $\mu(\frac{m}{D}) \neq 0$ are DP^s and DP^{s-1} for $D \in \mathcal{D}$. Now $(m, P) = 1$, so $m \mid DP^t$ if and only if $D = m$. Hence if $\deg(D) < \deg(m)$, $\rho_{DP}(f) \equiv (\rho_D(f^{|P|})) \equiv \rho_D(f) \not\equiv 0 \pmod{P}$, since f is coprime to P , and the Carlitz order of f modulo P is taken to be m . So

$$\Phi_N(f) = \frac{\rho_{mP^s}(f)}{\rho_{mP^{s-1}}(f)} \prod_{D \in \mathcal{D}, \deg(D) < \deg(m)} \frac{F_D(f)}{G_D(f)} = \frac{\rho_P(\rho_{mP^{s-1}}(f))}{\rho_{mP^{s-1}}(f)} \prod_{D \in \mathcal{D}, \deg(D) < \deg(m)} \frac{F_D(f)}{G_D(f)},$$

and the terms $F_D(f), G_D(f)$ are not multiples of P . $\rho_{mP^s}(f) \equiv \rho_P(\rho_{mP^{s-1}}(f)) \equiv 0 \pmod{P}$, so by part 1 of Lemma 4.1.9, $\frac{\rho_P(\rho_{mP^{s-1}}(f))}{\rho_{mP^{s-1}}(f)}$ is a multiple of P , which implies P divides $\Phi_N(f)$. By part 3 of Lemma 4.1.9, P^2 does not divide $\frac{\rho_P(\rho_{mP^{s-1}}(f))}{\rho_{mP^{s-1}}(f)}$, so P^2 does not divide $\Phi_N(f)$.

To show that all the other prime factors of $\Phi_N(f)$ are c -Zsigmondy prime, we let Q be a prime factor of $\Phi_N(f)$ and the Carlitz order of f modulo Q be S . Then $\rho_N(f) \equiv 0 \pmod{Q}$, so S divides N and also by Proposition 4.1.1, S divides $Q - 1$. Let R be a prime factor of $\frac{N}{S}$, and set $J = \frac{N}{R}$. Then S divides J , so $\rho_J(f) \equiv 0 \pmod{Q}$ and this implies that $\Phi_N(f)$ divides $\frac{\rho_N(f)}{\rho_J(f)} \equiv \frac{\rho_R(\rho_J(f))}{\rho_J(f)} \equiv R \pmod{Q}$ since $\rho_J(f) \equiv 0 \pmod{Q}$. But R is a prime, so $R = Q$. So Q is a prime factor of $\frac{N}{S}$, hence N is of the form SQ^t for some $t \geq 1$. Since S divides $Q - 1$, Q must be the largest prime factor of N , so $Q = P$ and $S = m$. So P is a non c -Zsigmondy factor of $\Phi_N(f)$, and if it is unique, then Carlitz order of f is $S = m$. We saw in Theorem 4.1.7, that if $N \neq (Q - 1)Q$, where $Q, Q - 1$ are twin primes, or N does not have a unique largest prime factor, then we do not have any non c -Zsigmondy primes of $\Phi_N(f)$. □

We now establish a very striking fact, i.e., non c -Zsigmondy prime factors of $\Phi_N(f)$ only occur in the way described in Theorems 4.1.7 and 4.1.8 above. For a given N , there is at most one such factor, *the largest (in degree) prime factor of N* . Let $N = P$ and Q be a non c -Zsigmondy prime factor of $\Phi_N(f)$, (for $\langle f, N \rangle$). Then $\rho_P(f) \equiv 0 \pmod{Q}$, so Carlitz order of f modulo Q divides P . By assumption, the Carlitz order of f modulo Q is not P , so it is 1, hence $f \equiv 0 \pmod{Q}$. Hence $\Phi_P(f) = P + a_{P,1}f^{q-1} + \dots + f^{q^{\deg(P)}-1} \equiv P \pmod{Q}$. Since $\Phi_P(f)$ is a multiple of Q , then $Q = P$, the only possible non Zsigmondy factor of $\Phi_P(f)$ is P itself, and it is a factor when $f \equiv 0 \pmod{P}$, contradicting the hypothesis that $(f, P) = 1$.

We now compute an upper bound for the number of c -Zsigmondy primes for $\langle f, N \rangle$.

Theorem 4.1.10. *Let f, N be as above, $\mathcal{Z}(f, N)$ be the number of Zsigmondy primes of $\langle f, N \rangle$, then*

$$\mathcal{Z}(f, N) \leq \frac{(1 + \varphi(N)) \deg(f)}{\deg(N)}.$$

Proof. Let P_1, \dots, P_s be the set of Zsigmondy primes for $\langle f, N \rangle$, then $\deg(P_i) \geq \deg(N)$ for each i and $\deg(P_1 \cdots P_s) \leq \deg(\Phi_N(f))$. But $\deg(\Phi_N(f)) \leq \deg(f^{\varphi(N)+1})$, and so $\deg(N^s) \leq \deg(f^{\varphi(N)+1})$, hence $s \deg(N) \leq (1 + \varphi(N)) \deg(f)$, and the result follows. \square

4.2 Primitive and non primitive factors of $\mathcal{P}_N(x, y)$

In this section, our main goal is to prove the Carlitzian analogue of the Bang - Zsigmondy Theorem. To achieve this, we shall closely follow S. Bae's work [3] on the $\mathbb{F}_q[T]$ analogue of $x^n - y^n$. At many places, we shall give detailed proofs so as to have a complete description. To each unoriginal proof given or rewritten, a pointer to the original proof will be indicated.

Let $N \in A_+$ with $\deg(N) = n$, we define

$$\mathcal{P}_N(x, y) = y^{q^n} \rho_N \left(\frac{x}{y} \right) \quad (4.1)$$

$$\mathcal{Q}_N(x, y) = x^{-1} \mathcal{P}_N(x, y) \quad (4.2)$$

$$\mathcal{F}_N(x, y) = y^{\varphi(N)} \Phi_N \left(\frac{x}{y} \right). \quad (4.3)$$

As an action on \mathbb{G}_a , ρ_N is analogous to x^n as an action on \mathbb{G}_n . However, when we think of a polynomial whose roots are precisely the N torsion points in \mathbb{G}_a , then it is clear that $\rho_N(x)$ is the right Carlitzian analogue to the unital polynomial $x^n - 1$, polynomial whose roots are the n torsion points. Since $x^n - y^n = y^n \left(\left(\frac{x}{y} \right)^n - 1 \right)$, $\mathcal{P}_N(x, y)$, (and $\mathcal{Q}_N(x, y)$ resp.) can be thought as the Carlitzian analogues to the homogeneous polynomials $x^n - y^n$, (and $\frac{x^n - y^n}{(x-y)}$ resp.). Replacing y by 1 in the above formulas, we recover all results in chapter 2. In addition, replacing $\Phi_N(x)$ by $\mathcal{F}_N(x, y)$, and $\rho_N(x)$ by $\mathcal{P}_N(x, y)$, we obtain Proposition 4.2.1.

Proposition 4.2.1 ([3], Remark 1 (a)). *For any $N \in A_+$, we have*

$$\mathcal{P}_N(x, y) = \prod_{D|N} \mathcal{F}_D(x, y). \quad (4.4)$$

Proof. By definition,

$$\mathcal{P}_N(x, y) = y^{q^n} \rho_N \left(\frac{x}{y} \right) \stackrel{\text{Prop. 2.2.2}}{=} y^{q^n} \prod_{D|N} \Phi_D \left(\frac{x}{y} \right) \stackrel{\text{Prop. 1.2.4}}{=} \prod_{D|N} y^{\varphi(D)} \Phi_D \left(\frac{x}{y} \right) = \prod_{D|N} \mathcal{F}_D(x, y).$$

□

Applying the Möbius Inversion Formula to Equation (4.4) yields

$$\mathcal{F}_N(x, y) = \prod_{D|N} \mathcal{P}_D(x, y)^{\mu\left(\frac{N}{D}\right)}.$$

Proposition 4.2.2 ([3], Proposition 4.1). *Let $N_1, N_2 \in A_+$ be of degrees n_1, n_2 respectively, then*

(a)

$$\begin{aligned} \mathcal{P}_{N_1 N_2}(x, y) &= \mathcal{P}_{N_1}(\mathcal{P}_{N_2}(x, y), y^{q^{n_2}}) = \mathcal{P}_{N_2}(\mathcal{P}_{N_1}(x, y), y^{q^{n_1}}), \\ \mathcal{Q}_{N_1 N_2}(x, y) &= \mathcal{Q}_{N_1}(x \mathcal{Q}_{N_2}(x, y), y^{q^{n_2}}) \mathcal{Q}_{N_2}(x, y) = \mathcal{Q}_{N_2}(x \mathcal{Q}_{N_1}(x, y), y^{q^{n_1}}) \mathcal{Q}_{N_1}(x, y), \end{aligned} \quad (4.5)$$

therefore, $\mathcal{P}_{N_1}(x, y), \mathcal{P}_{N_2}(x, y) \mid \mathcal{P}_{N_1 N_2}(x, y)$ and $\mathcal{Q}_{N_1}(x, y), \mathcal{Q}_{N_2}(x, y) \mid \mathcal{Q}_{N_1 N_2}(x, y)$.

(b) If $n_1 > n_2$, then

$$\begin{aligned} \mathcal{P}_{N_1+N_2}(x, y) &= \mathcal{P}_{N_1}(x, y) + y^{q^{n_1}-q^{n_2}} \mathcal{P}_{N_2}(x, y), \\ \mathcal{Q}_{N_1+N_2}(x, y) &= \mathcal{Q}_{N_1}(x, y) + y^{q^{n_1}-q^{n_2}} \mathcal{Q}_{N_2}(x, y). \end{aligned}$$

(c)

$$\begin{aligned} \prod_{c \in \mathbb{F}_q} \mathcal{P}_{NT+c}(x, y) &= \mathcal{P}_{NT}^q(x, y) - y^{(q^{n+1}-1)(q-1)} x^{q-1} \mathcal{P}_{NT}(x, y), \\ \prod_{c \in \mathbb{F}_q} \mathcal{Q}_{NT+c}(x, y) &= \mathcal{Q}_{NT}^q(x, y) - y^{(q^{n+1}-1)(q-1)} x^{q-1} \mathcal{Q}_{NT}(x, y). \end{aligned}$$

(d) $\mathcal{P}_N(x, y)$ is \mathbb{F}_q -linear in the first variable.

Proof. We only prove item (d) which does not appear in the original statement of [3], Proposition 4.1. \mathbb{F}_q -linearity in the first coordinate follows from the following calculation,

$$\mathcal{P}_N(\alpha x + \beta z, y) = y^{q^n} \rho_N\left(\frac{\alpha x + \beta z}{y}\right) = \left(\alpha y^{q^n} \rho_N\left(\frac{x}{y}\right) + \beta \rho_N\left(\frac{z}{y}\right)\right) = \alpha \mathcal{P}_N(x, y) + \beta \mathcal{P}_N(z, y).$$

□

The following two results will be useful in the proof of Theorem 4.2.10. Although they are implicitly used in [3], we failed to find their proofs in that paper, so we supplied our own.

Proposition 4.2.3 (Analogue of Proposition 2.2.4).

$$\mathcal{F}_{mP^s}(x, y) = \begin{cases} \mathcal{F}_m(\mathcal{P}_{P^s}(x, y), y^{q^{s \deg(P)}}), & (m, P) \neq 1 \\ \mathcal{F}_{mP}(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}}), & (m, P) = 1. \end{cases}$$

Proof. Firstly, suppose $(m, P) \neq 1$, i.e., $P \mid m$.

$$\begin{aligned} \mathcal{F}_{mP^s}(x, y) &= \prod_{D \mid mP^s} \left(\mathcal{P}_{\frac{mP^s}{D}}(x, y) \right)^{\mu(D)} = \prod_{D \mid m} \left(\mathcal{P}_{\frac{mP^s}{D}}(x, y) \right)^{\mu(D)} \prod_{D \mid mP^s, D \nmid m} \left(\mathcal{P}_{\frac{mP^s}{D}}(x, y) \right)^{\mu(D)} \\ &= \prod_{D \mid m} \left(\mathcal{P}_{\frac{m}{D}} \left(\mathcal{P}_{P^s}(x, y), y^{q^s \deg(P)} \right) \right)^{\mu(D)} = \mathcal{F}_m \left(\mathcal{P}_{P^s}(x, y), y^{q^s \deg(P)} \right), \end{aligned}$$

since $D \mid mP^s$ and $D \nmid m$ implies $P^2 \mid D$, therefore $\mu(D) = 0$. Secondly, suppose $P \nmid m$,

$$\begin{aligned} \mathcal{F}_{mP^s}(x, y) &= \prod_{D \mid mP^s} \left(\mathcal{P}_{\frac{mP^s}{D}}(x, y) \right)^{\mu(D)} = \prod_{D \mid mP} \left(\mathcal{P}_{\frac{mP^s}{D}}(x, y) \right)^{\mu(D)} \prod_{D \mid mP^s, D \nmid mP} \left(\mathcal{P}_{\frac{mP^s}{D}}(x, y) \right)^{\mu(D)} \\ &= \prod_{D \mid mP} \left(\mathcal{P}_{\frac{m}{D}} \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right) \right)^{\mu(D)} = \mathcal{F}_{mP} \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right), \end{aligned}$$

again $D \mid mP^s$ and $D \nmid mP$ implies $P^2 \mid D$, therefore $\mu(D) = 0$ and the result follows. \square

Corollary 4.2.4 (Analogue of Corollary 2.2.5).

$$\mathcal{F}_{mP^s}(x, y) = \begin{cases} \mathcal{F}_m \left(\mathcal{P}_{P^s}(x, y), y^{q^s \deg(P)} \right), & (m, P) \neq 1 \\ \frac{\mathcal{F}_m \left(\mathcal{P}_{P^s}(x, y), y^{q^s \deg(P)} \right)}{\mathcal{F}_m \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right)}, & (m, P) = 1. \end{cases}$$

Proof. If $(m, P) \neq 1$, the result follows from Proposition 4.2.3. Otherwise, we have

$$\begin{aligned} \mathcal{F}_{mP} \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right) &= \prod_{D \mid mP} \left(\mathcal{P}_D \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right) \right)^{\mu\left(\frac{m}{D}\right)} \\ &= \prod_{D \mid m} \left(\mathcal{P}_D \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right) \right)^{\mu\left(\frac{mP}{D}\right)} \\ &\quad \cdot \prod_{D \mid m} \left(\mathcal{P}_{DP} \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right) \right)^{\mu\left(\frac{mP}{DP}\right)} \\ &= \frac{\prod_{D \mid m} \left(\mathcal{P}_{DP} \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right) \right)^{\mu\left(\frac{m}{D}\right)}}{\prod_{D \mid m} \left(\mathcal{P}_D \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right) \right)^{\mu\left(\frac{m}{D}\right)}} \\ &= \frac{\prod_{D \mid m} \left(\mathcal{P}_D \left(\mathcal{P}_{P^s}(x, y), y^{q^s \deg(P)} \right) \right)^{\mu\left(\frac{m}{D}\right)}}{\prod_{D \mid m} \left(\mathcal{P}_D \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right) \right)^{\mu\left(\frac{m}{D}\right)}} \\ &= \frac{\mathcal{F}_m \left(\mathcal{P}_{P^s}(x, y), y^{q^s \deg(P)} \right)}{\mathcal{F}_m \left(\mathcal{P}_{P^{s-1}}(x, y), y^{q^{(s-1) \deg(P)}} \right)}. \end{aligned}$$

\square

In the remaining part of this section, we shall prove an analogue of the Bang - Zsigmondy Theorem. To do this, let us first make a detour to the analogy with the integers. We begin like this, over \mathbb{Z} , the integer $x^n - y^n$ factors as $x^n - y^n = p_1^{e_1} \cdots p_t^{e_t}$, where p_i 's are distinct primes. If $\{p_i\}_{i=1}^s$ is the set of primitive¹ prime factors of $x^n - y^n$, then the factor $q_n(x, y) = p_1^{e_1} \cdots p_s^{e_s}$ is called the *arithmetic factor* of $x^n - y^n$. By the fundamental factorisation property of classical cyclotomic polynomials (see Proposition 2.2.2), and with abuse of notation, we set

$$\mathcal{P}_n(x, y) := x^n - y^n = y^n \left(\left(\frac{x}{y} \right)^n - 1 \right) = y^n \prod_{d|n} \Phi_d \left(\frac{x}{y} \right) = \prod_{d|n} y^{\varphi(d)} \Phi_d \left(\frac{x}{y} \right) =: \prod_{d|n} \mathcal{F}_d(x, y).$$

Applying the Möbius Inversion Formula, we obtain

$$\mathcal{F}_n(x, y) = \prod_{d|n} \mathcal{P}_d(x, y)^{\mu \left(\frac{n}{d} \right)}.$$

We refer to $\mathcal{F}_n(x, y)$ as the *algebraic factor* of $x^n - y^n$.

As an example, take $x = 2, y = 1, n = 6$, we have $\mathcal{P}_6(2, 1) = 3^2 \cdot 7$. Since 3 divides $\mathcal{P}_2(2, 1)$ and 7 divides $\mathcal{P}_3(2, 1)$, we have no primitive prime factors for $\mathcal{P}_6(2, 1)$, so $q_6(2, 1) = 1$. A simple calculation shows that $\mathcal{F}_6(2, 1) = \Phi_6(2) = 3$, a non primitive factor for $\mathcal{P}_6(2, 1)$. In other words, not all the prime factors of $\mathcal{F}_n(x, y)$ are necessarily primitive factors of $\mathcal{P}_n(x, y)$. There is a wonderful classical result firstly due to S. Bang and secondly K. Zsigmondy that guarantees existence of primitive prime factors of $x^n - y^n$, except for a few cases.

Theorem 4.2.5 (Bang - Zsigmondy Theorem). *Let $x, y \in \mathbb{Z}_+$ be coprime such that if $1 \leq y < x$, then $x^n - y^n$ has at least one primitive prime factor with the following two possible exceptions,*

1. $n = 6, x = 2$ and $y = 1$.
2. $n = 2$ and $x + y$ is a power of 2.

Similarly, $x^n + y^n$ has at least one primitive prime factor with the exception $2^3 + 1^3$.

There are several proofs in the literature for Theorem 4.2.5 due to K. Zsigmondy (1890), D. Birkhoff and H. Vandiver (1904), L. Dickson (1905), E. Artin (1955), C. Hering (1974) and H. Lüneburg (1981). All these proofs have one thing in common, they use properties of cyclotomic polynomials. It is no surprise that the proof of its Carlitzian analogue uses properties of (Carlitz) cyclotomic polynomials. We follow Birkhoff and Vandiver's approach [7] to prove this analogue. With this strategy in mind, we go back to the ring A .

Having introduced an analogue of $x^n - y^n$ and some of its properties, we now explore the notion of its *primitive factors* in analogy to the classical primitive factors of $x^n - y^n$. Let f, g

¹A primitive prime factor of $x^n - y^n$ is a prime p dividing $x^n - y^n$ but not $x^d - y^d$ for any divisor $d \neq n$ of n .

be (coprime monics) in A , $N \in A$ and $\deg(N) = n$. A prime factor P of $\mathcal{P}_N(f, g)$ coprime to $\mathcal{P}_M(f, g)$ for all proper divisors $M, (\neq N)$ of N , is called a *primitive prime factor* of $\mathcal{P}_N(f, g)$.

Proposition 4.2.6 ([3], Proposition 4.4). *Let $f, g \in A_+$ and $N \in A$, the following are equivalent,*

- (a) P is a primitive factor of $\mathcal{P}_N(f, g)$.
- (b) P divides $\mathcal{F}_N(f, g)$ and $P \equiv 1 \pmod{N}$.
- (c) P divides $\mathcal{F}_N(f, g)$ and $P \nmid N$.

In this proof, we give details intentionally left out in S. Bae's proof of ([3], Proposition 4.4).

Proof. We proceed as follows.

1. We prove (a) implies (b). Let P be a primitive factor of $\mathcal{P}_N(f, g)$, then $P \nmid \mathcal{P}_1(f, g) = f$, hence $P \nmid g$. This is because, if $P \mid \mathcal{P}_N(f, g)$, and g , then $0 \equiv \mathcal{P}_N(f, g) \equiv f^{q^n} \pmod{P}$, so $P \mid f$. To check divisibility with respect to P , we shall work modulo P , so without loss of generality, we can assume $\deg(f) < \deg(P)$. We also know $\rho_{P-1}(f) \equiv 0 \pmod{P}$. Let N be the generator of the annihilator ideal $\text{Ann}_P(f)$ of f , i.e., this is the monic polynomial of minimum degree for which $\rho_N(f) \equiv 0 \pmod{P}$. Viewing A/PA as an A -module via ρ , the Carlitz order of f modulo P is N , thence N must divide $P - 1$.
2. It is clear that (b) implies (c).
3. To prove (c) implies (a), we proceed as follows. Firstly P divides $\mathcal{F}_N(f, g)$ implies that P divides $\mathcal{P}_N(f, g)$. We now show that $P \nmid N$ implies that $P \nmid \mathcal{F}_D(f, g), \mathcal{P}_D(f, g)$ for any proper divisor D of N . Assume $\mathcal{P}_D(f, g) \equiv 0 \pmod{P}$ for some proper divisor $D, (\neq N)$ of N , then $\mathcal{F}_D(f, g) \equiv 0 \pmod{P}$,

$$\mathcal{P}_N(f, g) = \mathcal{F}_N(f, g)\mathcal{F}_D(f, g)(\text{ other factors }) \equiv 0 \pmod{P^2}.$$

Since $\mathcal{F}_N(f + P, g) \equiv \mathcal{F}_N(f, g) \equiv 0 \pmod{P}$, $\mathcal{F}_D(f + P, g) \equiv \mathcal{F}_D(f, g) \equiv 0 \pmod{P}$, we have $\mathcal{P}_N(f + P, g) \equiv 0 \pmod{P^2}$. So

$$0 \equiv \mathcal{P}_N(f + P, g) \equiv \mathcal{P}_N(f, g) + \mathcal{P}_N(P, g) = NPg^{q^n-1} \pmod{P^2}.$$

This is impossible since $P \nmid N$ and $P \nmid g$. We must have $D = N$, hence (c) implies (a).

□

Proposition 4.2.7. *Let f, N be as above, the following are equivalent,*

1. P is a primitive prime factor of $\rho_N(f)$.
2. P divides $\Phi_N(f)$ and $P \equiv 1 \pmod{N}$.
3. P divides $\Phi_N(f)$ and $P \nmid N$.

Proof. For the proof of this result, see the proof of Proposition 4.2.6 with $g = 1$. \square

Remark 4.2.8. Part (3) of Proposition 4.2.7 is the statement of Proposition 4.1.4. This suggests that the so called c -Zsigmondy primes of $\rho_N(f)$ are precisely the primitive prime factors of $\rho_N(f)$.

Let $f, g, N \in A_+$, $\mathcal{P}_N(f, g) = P_1^{\alpha_1} \cdots P_t^{\alpha_t}$ be the prime factorisation of $\mathcal{P}_N(f, g)$, with $\{P_i\}_{i=1}^s$ as the distinct primitive prime factors of $\mathcal{P}_N(f, g)$, i.e., $\{P_i\}_{i=s+1}^t$ - are non primitive. Put

$$q_N(f, g) = \prod_{i=1}^s P_i^{\alpha_i},$$

and call $q_N(f, g)$, the arithmetic factor of $\mathcal{P}_N(f, g)$. We also have

$$\mathcal{P}_N(f, g) = \prod_{D|N} \mathcal{F}_D(f, g),$$

and so by the Möbius Inversion Formula,

$$\mathcal{F}_N(f, g) = \prod_{D|N} \mathcal{P}_D(f, g)^{\mu\left(\frac{N}{D}\right)}.$$

We call $\mathcal{F}_N(f, g)$ - the algebraic factor of $\mathcal{P}_N(f, g)$. Like in the classical case, some factors of $\mathcal{F}_N(f, g)$ may not necessarily be primitive factors of $\mathcal{P}_N(f, g)$. Let $\omega_N(f, g) := \frac{\mathcal{F}_N(f, g)}{q_N(f, g)}$. In 1998, S. Bae [3] proved that, there are not many non primitive prime factors in $\mathcal{F}_N(f, g)$.

Theorem 4.2.9 ([3], Theorem 4.5). *Let $f, g, N \in A$. If $\deg(N) > 0$, then $\omega_N(f, g) = 1$, unless $q_N(f, g) \equiv 0 \pmod{P}$, where $N = P^s N_1$ and $P \nmid N_1$. In the latter case,*

$$\omega_N(f, g) = \begin{cases} PQ, & \text{if } q \text{ is even and } (g, N) = 1, \text{ where } Q = P - 1 \text{ is a prime,} \\ P, & \text{if } q \text{ is odd.} \end{cases}$$

We now state and prove the long awaited Carlitzian analogue of Theorem 4.2.5. Our demonstration is slightly different from that presented by S. Bae [3], but we both mimic (at least very closely) the classical ideas in the proof constructed by D. Birkhoff and H. Vandiver, [7].

Theorem 4.2.10 ((Carlitz) - Bang - Zsigmondy Theorem, ([3], Theorem 4.10)). *Suppose $q > 2$ and $\deg(N) > 0$. Then $\mathcal{P}_N(f, g)$ possesses at least one primitive prime factor, except when $q = 3$, $N = (T + \alpha)(T + \alpha + 1)$, $\alpha \in \mathbb{F}_3$ and $f = \pm 1 = g$. In this case, we have the equations*

$$\begin{aligned} \mathcal{P}_{(T+\alpha)}(\pm 1, \pm 1) &= \pm(T + \alpha + 1), \\ \mathcal{P}_{T+\alpha+1}(\pm 1, \pm 1) &= \pm(T + \alpha - 1), \\ \mathcal{P}_{(T+\alpha)(T+\alpha+1)}(\pm 1, \pm 1) &= \pm(T + \alpha + 1)^2(T + \alpha - 1). \end{aligned}$$

Proof. To prove this theorem, it suffices to show that $\deg(q_N(f, g)) > 0$. Firstly, we consider the case $q_N(f, g) \equiv 0 \pmod{P}$, where $f, g \in A_+$. By Theorem 4.2.9, $N = N_1 P^\beta$ for some $\beta \in \mathbb{Z}_+$, $P \equiv 1 \pmod{N_1}$ and $\mathcal{F}_{N_1}(f, g) \equiv 0 \pmod{P}$. Now $f, g \in A_+$ implies $\mathcal{F}_{N_1}(f, g) \neq 0$

and so $\deg(\mathcal{F}_{N_1}(f, g)) \geq \deg(P)$ hence $\deg(\varrho_N(f, g)) = \deg\left(\frac{\mathcal{F}_N(f, g)}{P}\right) \geq \deg\left(\frac{\mathcal{F}_N(f, g)}{\mathcal{F}_{N_1}(f, g)}\right)$. Suppose $N_1 \neq 1$, since f and g are monics, we have $\deg(\mathcal{P}_D(f, g)) \geq \deg(f^{|D|-1})$. Also

$$\mathcal{F}_N(f, g) = \prod_{D|N} (\mathcal{P}_D(f, g))^{\mu\left(\frac{N}{D}\right)} = \frac{\prod_{D_+|N} (\mathcal{P}_{D_+}(f, g))}{\prod_{D_-|N} (\mathcal{P}_{D_-}(f, g))}, \quad (4.6)$$

where D_+ and D_- are the monic divisors of N such that $\mu\left(\frac{N}{D_+}\right) = 1$ and $\mu\left(\frac{N}{D_-}\right) = -1$ respectively. So we obtain $\deg\left(\prod_{D_+|N} \mathcal{P}_{D_+}(f, g)\right) \geq \deg\left(\prod_{D_+|N} f^{|D_+|-1}\right)$ and

$$\deg\left(\prod_{D_+|N} \mathcal{P}_{D_+}(f, g)\right) \geq \deg\left(\prod_{D_+|N} f^{|D_+|-1}\right) = \deg(f^{\sum_{D_+|N} |D_+|-1}) = \deg(f^{-2^{s-1} + \sum_{D_+|N} |D_+|}),$$

where s is the number of distinct prime factors in N . The -2^{s-1} in exponent comes from the following calculation $\sum_{D_+|N} -1 = -\frac{1}{2} \sum_{D|N} |\mu(D)| = -\frac{1}{2} \sum_{i=0}^s \binom{s}{i} = -\frac{1}{2} (1+1)^s = -2^{s-1}$. For the denominator of $\mathcal{F}_N(f, g)$, since for any $f, g \in A_+$, with say $\deg(f) \geq \deg(g)$, we have $\deg(\mathcal{P}_D(f, g)) < \deg(f^{|D|+1})$, we get

$$\deg\left(\prod_{D_-|N} \mathcal{P}_{D_-}(f, g)\right) \leq \deg\left(\prod_{D_-|N} f^{|D_-|+1}\right) = \deg(f^{2^{s-1} + \sum_{D_-|N} |D_-|}).$$

Dividing the inequalities for numerator and denominator of $\mathcal{F}_N(f, g)$ in Equation (4.6), yields $\deg(\mathcal{F}_N(f, g)) > \deg(f^{\varphi(N)-2^s})$. Since by assumption $\deg(N_1) > 0$, using the inequality $\deg(\mathcal{P}_D(f, g)) < \deg(f^{|D|+1})$ in the numerator and $\deg(\mathcal{P}_D(f, g)) > \deg(f^{|D|-1})$ in the denominator of $\mathcal{F}_{N_1}(f, g)$, we obtain $\deg(\mathcal{F}_{N_1}(f, g)) > \deg(f^{\varphi(N_1)-2^{s-1}})$. So

$$\deg\left(\frac{\mathcal{F}_N(f, g)}{\mathcal{F}_{N_1}(f, g)}\right) > \deg(f^{\varphi(N) - \varphi(N_1) - 2^{s-1}}).$$

Now let us consider the exponent $\varphi(N) - \varphi(N_1) - 2^{s-1}$ more closely. Since $\deg(N_1) > 0$, we have $\varphi(N_1) \geq (q-1)^{s-1} \geq 2^{s-1}$. Also $\varphi(P^\beta) \geq 3$, except when $q = 3, \beta = 1$ and $\deg(P) = 1$, noting that $q > 2$. So, $\varphi(N) = \varphi(N_1)\varphi(P^\beta) \geq 3\varphi(N_1) \geq 3 \cdot 2^{s-1}$, except when $q = 3, \beta = 1$ and $\deg(P) = 1$. Clearly, $\varphi(N) - \varphi(N_1) - 2^{s-1} \geq 2\varphi(N_1) - 2^{s-1} \geq 2^{s-1}$ with the exception of $q = 3, \beta = 1$ and $\deg(P) = 1$. The exception implies that $\deg(N) = 2$. So

$$\deg(\varrho_N(f, g)) = \deg\left(\frac{\mathcal{F}_N(f, g)}{P}\right) \geq \deg\left(\frac{\mathcal{F}_N(f, g)}{\mathcal{F}_{N_1}(f, g)}\right) > \deg(f^{\varphi(N) - \varphi(N_1) - 2^{s-1}}) > 0,$$

except when $q = 3$ and $\deg(N) = 2$. We compute $\rho_{(T+\alpha)(T+\alpha+1)}(x)$ where $\alpha = 0, 1, 2$, and get

$$\begin{aligned} \rho_{(T+\alpha)(T+\alpha+1)}(x) &= \eta_\alpha(\rho_{T(T+1)}(x)) = \eta_\alpha(x^9 + (T^3 + T + 1)x^3 + (T^2 + T)x) \\ &= x^9 + (T^3 + T + 2\alpha + 1)x^3 + (T^2 + (2\alpha + 1)T + \alpha^2 + \alpha)x. \end{aligned}$$

Using $\rho_{T+\alpha}(x) = x^3 + (T + \alpha)x$, we have

$$\begin{aligned} \mathcal{F}_{T(T+1)}(x, y) &= \frac{\mathcal{P}_1(x, y)\mathcal{P}_{T(T+1)}(x, y)}{\mathcal{P}_T(x, y)\mathcal{P}_{T+1}(x, y)} = \frac{x(x^9 + (T^3 + T + 1)x^3y^6 + (T^2 + T)xy^8)}{(x^3 + Txy^2)(x^3 + (T + 1)xy^2)} \\ &= x^4 + (T + 2)xy^3 + y^4, \end{aligned}$$

and so $\mathcal{F}_{(T+\alpha)(T+\alpha+1)}(x, y) = \eta_\alpha(\mathcal{F}_{T(T+1)}(x, y)) = x^4 + (T + \alpha + 2)xy^3 + y^4$. Hence

$$\mathcal{F}_{(T+\alpha)(T+\alpha+1)}(f, g) = f^4 + (T + \alpha + 2)fg^3 + g^4,$$

which is greater than 3 in absolute value except for $f = \pm 1 = g$. In this case, we have the following $\mathcal{F}_{(T+\alpha)(T+\alpha+1)}(\pm 1, \pm 1) = \pm(T + \alpha + 2) + 2 = T + \alpha + 1$ or $-(T + \alpha)$. Since $\mathcal{F}_{(T+\alpha)}(\pm 1, \pm 1) = T + \alpha + 1$, as α runs over \mathbb{F}_3 , no primitive divisor of $\mathcal{F}_{(T+\alpha)(T+\alpha+1)}(\pm 1, \pm 1)$ other than 1 exists and so $\varrho_{(T+\alpha)(T+\alpha+1)}(\pm 1, \pm 1) = 1$. When $N_1 = 1$, then $N = P^\beta$ and from

$$\mathcal{F}_N(f, g) = \frac{\mathcal{P}_N(f, g)}{\mathcal{P}_{\frac{N}{P}}(f, g)} = \frac{\mathcal{P}_P(\mathcal{P}_{P^{\beta-1}}(f, g), g^{q^{(\beta-1)\deg(P)}})}{\mathcal{P}_{P^{\beta-1}}(f, g)},$$

an expression greater than P in degrees, since the expanded forms contain P and positive integral terms some of which are greater than unity. Hence $\deg(\varrho_{P^\alpha}(f, g)) > 0$. The case $\omega = 1$ remains to be disposed of. We have $\deg(\mathcal{F}_N(f, g)) > \deg(f^{\varphi(N)-0-2^{s-1}})$. Obviously $\varphi(N) \geq 2^{s-1}$, hence $\deg(\mathcal{F}_N(f, g)) > 0$ and so $\deg(\varrho_N(f, g)) > 0$ completing the proof. \square

Remark 4.2.11. *The above method fails in general for the case $q = 2$ because of the indeterminacy...*

Corollary 4.2.12. *With the exception of $N = (T + \alpha)(T + \alpha + 1) \in \mathbb{F}_3[T]$, $\alpha \in \mathbb{F}_3$, $\mathcal{P}_N(f, g)$ possesses at least one prime factor congruent to $1 \pmod{N}$.*

Theorem 4.2.13. *There are infinitely many primes of the form $P \equiv 1 \pmod{N}$.*

Proof. Consider the sequence $\varrho_{m_1N}(f, g), \varrho_{m_2N}(f, g), \dots$ with m_1, m_2, \dots distinct. The polynomials represented are all coprime to each other. By Theorem 4.2.10 and Proposition 4.2.6 (b), each contains at least one primitive prime factor congruent to $1 \pmod{N}$. Consequently, the sequence furnishes infinitely many primes congruent to $1 \pmod{N}$. \square

Remark 4.2.14. *This is a special case of Dirichlet Theorem for primes in arithmetic progressions.*

Proposition 4.2.15 (Analogue of [7], Application 2). *Let $f \in A_+$, then $\mathcal{F}_P(f, 1)$ is a prime in A .*

Proof. Suppose $\mathcal{F}_P(f, 1)$ is reducible then

$$\mathcal{F}_P(f, 1) = \frac{\mathcal{P}_P(f, 1)}{\mathcal{P}_1(f, 1)} = f_1(f)f_2(f)$$

where $f_1(f)$ and $f_2(f)$ are polynomials in f with integral coefficients. In the above identity, let f take on the elements of $\{a \in A : \deg(a) < \deg(P)\} - \{0\}$. For any of these values, $\mathcal{F}_P(f, 1) = \varrho_P(f, 1)$ and also $f_1(f) \equiv 1 \pmod{P}$ since it is a divisor of $\varrho_P(f, 1)$. Consequently, the congruence $f_1(f) \equiv 1 \pmod{P}$ admits $|P| - 1$ roots which is impossible, since P is a prime and the degree of $f_1(f)$ is less than $|P| - 1$. $\mathcal{F}_P(f, 1)$ is thus irreducible in A . \square

4.3 Fermat pseudoprimes in $\mathbb{F}_q[T]$ and Wieferich primes in $\mathbb{F}_p[T]$

A pseudoprime may be defined as any composite integer that shares a property common to all prime numbers. A pseudoprime is classified according to which property of primes it satisfies, e.g. Fermat's Little Theorem, Euler's Theorem, Catalan's congruence, e.t.c. In our study, we shall only consider the so called Fermat pseudoprimes, i.e., composite integers satisfying Fermat's Little Theorem. Fix $a \in \mathbb{Z}_{\geq 2}$, a Fermat pseudoprime to base a is any composite integer n coprime to a and satisfying $a^{n-1} \equiv 1 \pmod{n}$. For $a = 2$, we found the $n = 341, 561, 645, \dots$. In the case when $a = 3$, we have $n = 91, 286, 671, 703, 949, \dots$. An integer n that is a Fermat pseudoprime to all values of a coprime to it is called a Carmichael number. For example, the smallest such a number is 561, and in fact in 1992, W. Alford, A. Granville and C. Pomerance [1] proved that there are infinitely many such numbers.

Let us fix $a \in A - \{0\}$ and define $\mathcal{F}(a) := \{m \in A : \rho_{m-1}(a) \equiv 0 \pmod{m}\}$. Therefore, the set $\mathcal{F}(a)$ includes all primes coprime to a . Any composite member of $\mathcal{F}(a)$ is called a Carlitz - Fermat a - pseudoprime. We denote by $\text{PS}(a)$, the set of Carlitz - Fermat a - pseudoprimes. In this section, we shall write $\Phi_N^*(a)$ to denote $\Phi_N(a)$ without any non c - Zsigmondy factors.

Theorem 4.3.1. *Let $a, N \in A_+$, we have $\Phi_N^*(a) \in \mathcal{F}(a)$.*

Proof. Let $a, N \in A$. If $m \in A$ is such that $m \mid \rho_N(a)$ and $m \equiv 1 \pmod{N}$, then $m \in \mathcal{F}(a)$. This is because $\rho_{m-1}(a) = \rho_b(\rho_N(a)) \equiv 0 \pmod{m}$, where $b \in A$, and $Nb = m - 1$. By Proposition 4.2.7, these conditions are met by the primes of $\Phi_N^*(a)$, so $\Phi_N^*(a) \in \mathcal{F}(a)$. \square

Examples of Carlitz Fermat T pseudoprimes in $\mathbb{F}_3[T]$ include $\Phi_{T+1}(T) = T^2 + T + 1, T^3 + T^2 + 2T, T^5 + 2T^3 + 2T^2 + T, T^5 + T^4 + 1, T^5 + 2T^4 + T^3 + 1, T^6 + 2T^3 + T, T^6 + T^4 + T^2 + 1, T^6 + T^5 + 2T^4 + T^3 + T^2 + 2T + 1, \Phi_{T^2+2T+1}(T) = T^6 + 2T^5 + 2T^3 + T^2 + T + 1$, e.t.c.

Remark 4.3.2. *Moreover, if the same argument is applied to any composite divisor of $\Phi_N^*(a)$,*

1. *and if in addition P is a prime such that $P \nmid a$, then $\Phi_P^*(a) = \Phi_P(a)$, and $\Phi_P(a) \in \mathcal{F}(a)$.*
2. *then we obtain an infinitude of Carlitz a - pseudoprimes for each $0 \neq a \in A$.*

With the above in mind, a polynomial $N \in A_+$ is called a Carlitz - Carmichael polynomial if N is a Carlitz - Fermat pseudoprime for all polynomials in A coprime to N . In 1998, C. Hsu [14] proved an analogue of Korselt's result that characterises such polynomials. In the same paper, he used this criterion to establish infinitude of Carlitz - Carmichael polynomials in A .

Lastly, like in the classical case, we can not fail to point out the close connections that exist between the analogues of the unital polynomials, classical cyclotomic polynomials and Fermat's Last Theorem. Firstly, we shall give a brief history of the development of the analogue

of Fermat's Last Theorem and demonstrate how this is related to the definition for Carlitz Wieferich primes coined by D. Thakur, [28]. Secondly, we shall use Thakur's congruence definition to derive a necessary and sufficient condition for a prime P in A to be Carlitz Wieferich. From here, we shall give a few consequences of this criterion including construction of an algorithm to sieve Carlitz Wieferich primes. We further use the criterion to give some kind of horizontal existence theorem for Carlitz Wieferich primes. The examples of Carlitz Wieferich primes obtained from these algorithms motivate our study of fixed polynomials, (switch from q to p), relationship with Artin Schreier primes and Carlitz Wieferich primes. From this theory of fixed polynomials, we derive a vertical existence theorem and a new algorithm for computing Carlitz Wieferich primes in $\mathbb{F}_p[T]$. We wind up the section with two heuristic arguments on the number of Carlitz Wieferich primes in $\mathbb{F}_p[T]$. Before we address any of the above mentioned items, let us first make a detour to the classical realm.

Fermat's Last Theorem (FLT) is the assertion that for $n \geq 3$, the equation $x^n + y^n = z^n$ has no integer solutions $(x, y, z) \in \mathbb{Z}^3$ with $xyz \neq 0$ (as proved by A. Wiles and completed in a joint paper with R. Taylor). It was proven by P. Fermat for $n = 4$ and L. Euler for $n = 3$. Historically, this puzzle of Fermat was attacked by dividing it into two cases depending on whether $p \nmid xyz$ or $p \mid xyz$, i.e., first and second cases respectively. The first case asserts that, for any odd prime p , there are no integers x, y, z such that $p \nmid xyz$ and $x^p + y^p = z^p$, [21, page 192]. In 1909, while working on the first case of FLT, A. Wieferich stumbled on primes that satisfied a special congruence. In [32], Wieferich proved the following result.

Theorem 4.3.3. *If the first case of FLT is false for the odd prime p , then $2^{p-1} \equiv 1 \pmod{p^2}$.*

In other words, if a prime p satisfies $2^{p-1} \not\equiv 1 \pmod{p^2}$, then the first case of Fermat's Last Theorem is true for p . Theorem 4.3.3 is a strong condition that is now taken as the definition of classical Wieferich primes. Existence of such primes does not in any way invalidate FLT.

Definition 4.3.4. *A Wieferich prime (to base 2) is a prime number p satisfying $2^{p-1} \equiv 1 \pmod{p^2}$.*

In 1910, D. Mirimanoff showed that, one can replace the base 2 in $2^{p-1} \equiv 1 \pmod{p^2}$ by 3. Several authors [21, page 221] have done this trick of replacing 2 by another a , and called the corresponding primes p such that $a^{p-1} \equiv 1 \pmod{p^2}$, Wieferich primes to base a . The current record is that one can replace the base 2 by any prime $a \leq 113$, (the range [90, 113] was established by J. Suzuki [27]). At this point, A. Wiles and R. Taylor had proven FLT in general, so the motivation for going further disappeared. Despite a number of extensive searches, the only Wieferich primes known to date (2014) are 1093 and 3511 (SLOANE's A001220 on OEIS). Today November 10, 2014, we neither know whether there are finitely nor infinitely many Wieferich primes. However, there is a heuristic that indicates the number of Wieferich primes $\leq x$ to be asymptotically $\log(\log(x))$, [21, page 226]. The disadvantage of this slow growth (almost a constant) is that it is difficult to verify it computationally.

Owing to the recent development of the arithmetic of function fields, the discovery of Carlitz cyclotomic extensions, which are almost identical and excellent analogues for the classical cyclotomic extensions led D. Goss [12] to construct Fermat's equations in this new setting. The procedure for constructing Fermat's equations is quite natural, first one recalls the classical Fermat equation $x^n + y^n = z^n$, which can be rewritten in the preferred form $x^n - y^n = z^n$ or equivalently $y^n \left(\left(\frac{x}{y} \right)^n - 1 \right) = z^n$. In this construction, the connection with the complex roots of $w^n - 1$ is made transparent. Following this procedure, we are led to the equation $\mathcal{P}_N(x, y, z) = 0$ parametrised by the element $N \in A$ of positive degree n . Here

$$\mathcal{P}_N(x, y, z) = \mathcal{P}_N(x, y) - z^{q^n} = y^{q^n} \rho_N \left(\frac{x}{y} \right) - z^{q^n}. \quad (4.7)$$

Equation (4.7) is clearly homogeneous. The inhomogeneous version of Equation (4.7) is

$$\mathcal{P}_N^{\text{in}}(x, y, z) = y^{q^n} \rho_N \left(\frac{x}{y} \right) - z^p, \quad (4.8)$$

where p is the characteristic of k . It is these Fermat equations that we call *geometric Fermat equations* because of their evident connection with the analogues classical cyclotomic polynomials. Any triple $(a, b, c) \in k^3$ such that $\mathcal{P}_N(a, b, c) = 0$ is a rational solution to $\mathcal{P}_N(x, y, z) = 0$. If in addition $(a, b, c) \in A^3$, then (a, b, c) is an integer solution. An integer solution (x, y, z) to any the above two equations is said to be *non trivial* if $xyz \neq 0$. In 1994, L. Denis [9] proved an analogue of Fermat's Last Theorem for the Equations (4.7) and (4.8).

Theorem 4.3.5 (Fermat - Goss - Denis Theorem, ([9], Theorems 1,2,3 and 4)). *Let $N \in A_+$ and $n = \deg(N)$, and p be the characteristic of A . Let*

1. $q \neq 2$ and $n > 1$, (or $n > 2$ and $q = 2$). Then both $\mathcal{P}_N(x, y, z) = 0$ and $\mathcal{P}_N^{\text{in}}(x, y, z) = 0$ have only a finite number of rational solutions with $(x, y) = (y, z) = 1$.
2. $q \geq 3$ and $n \geq 2$. Then $\mathcal{P}_N(x, y, z) = 0$ has no rational solutions with $xyz \neq 0$.
3. $q \geq 3$, $p > 2$ and $n \geq 2$. Then $\mathcal{P}_N^{\text{in}}(x, y, z) = 0$ has no rational solutions with $xyz \neq 0$.

Statement 4.3.6 (Fermat Goss Theorem (Case I)). *Let $q > 2$. Then for any $(x, y, z) \in A^3$ with $Q \nmid xyz$, where Q is a prime with $\deg(Q) > 1$, $\mathcal{P}_Q(x, y, z) \neq 0$. (and for $q = 2$, $\deg(Q) > 2$).*

Statement 4.3.6 is true because of Theorem 4.3.5. We expect that, assuming a non trivial solution to $\mathcal{P}_N(x, y, z) = 0$ yields Carlitz Wieferich primes. Theorem 4.3.7 shows that this is indeed the case. Note, existence of such primes does not invalidate Theorem 4.3.5.

Theorem 4.3.7. *If Statement 4.3.6 is false, then there exists an $a \in A$ and a prime P such that*

$$\rho_P(a) \equiv a^{|P|} \pmod{P^2}.$$

Proof. If Statement 4.3.6 is false for a prime P , then there exists a triple $(x, y, z) \in A^3$ with $P \nmid xyz$ and $\mathcal{P}_P(x, y, z) = 0$. Let $x_1 = z^{-1}x$ and $y_1 = z^{-1}y$, then

$$\begin{aligned} 0 &= z^{-q^{\deg(P)}} \mathcal{P}_P(x, y, z) = (z^{-1}y)^{q^{\deg(P)}} \rho_P \left(\frac{x}{y} \right) - 1 = \mathcal{P}_P(z^{-1}x, z^{-1}y) - 1 \\ &= \mathcal{P}_P(x_1, y_1) - 1 = y_1^{q^{\deg(P)}} \rho_{P-1} \left(\frac{x_1}{y_1} \right) + x_1 y_1^{q^{\deg(P)}-1} - 1 \equiv x_1 - 1 \pmod{P}. \end{aligned}$$

So $x_1 = 1 + cP$, c is a unit in the local ring $A_{(P)}$. Taking $\mathcal{P}_P(x_1, y_1) = 0$, modulo P^2 gives,

$$\begin{aligned} 0 &= \mathcal{P}_P(x_1, y_1) - 1 = y_1^{q^{\deg(P)}} \rho_{P-1} \left(\frac{1 + cP}{y_1} \right) + (1 + cP) y_1^{q^{\deg(P)}-1} - 1 \\ &\equiv y_1^{q^{\deg(P)}} \rho_P \left(\frac{1}{y_1} \right) - 1 \pmod{P^2}. \end{aligned}$$

So we obtain $\rho_P(a) \equiv a^{q^{\deg(P)}} = a^{|P|} \pmod{P^2}$, where $a \equiv \frac{1}{y_1} \pmod{P^2}$. \square

Remark 4.3.8. *The proofs for the analogous classical result are much harder.*

Remark 4.3.9. *Setting $a = 1$, we obtain $\rho_{P-1}(1) \equiv 0 \pmod{P^2}$ which is in agreement with the definition for Carlitz Wieferich primes coined by D. Thakur in [28, page 6].*

Definition 4.3.10 (D. Thakur, ([28], 1994)). *Let $a \in A - \{0\}$, a Carlitz Wieferich prime to base a is a prime P satisfying the congruence $\rho_P(a) \equiv a^{|P|} \pmod{P^2}$. If $a \in A^*$, then we call such a prime a Carlitz Wieferich prime or c -Wieferich prime. A non c -Wieferich prime to the base a is any P that is not a c -Wieferich prime to base a . If $\rho_P(a) \equiv a^{|P|} \pmod{P^2}$ is replaced by the hypercongruence $\rho_P(a) \equiv a^{|P|} \pmod{P^s}$, $s \geq 3$, the associated primes are super c -Wieferich primes to base a .*

Unlike the classical situation, where the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ is elegant and easy to check, its analogue, the congruence $\rho_{P-1}(1) \equiv 0 \pmod{P^2}$ is simple but messy when unpacked. It is computationally expensive to check due to the large degrees that are involved. It is almost impossible to do any significant computations in $\mathbb{F}_q[T]$ with degrees and $q \geq 5$. It is for this reason that we first derive equivalent congruences that are easier to work with in order to study properties of c -Wieferich primes. Moreover, these congruences indicate that c -Wieferich primes are also c -Wieferich primes to base T in any ring $\mathbb{F}_q[T]$.

Recall the fundamental numbers used in the arithmetic of A ; $L_0 = 1 = D_0$ and for $i \in \mathbb{Z}_{\geq 1}$, $L_i = [i][i-1] \cdots [1]$ and $D_i = [i][i-1]^q \cdots [1]^{q^{i-1}}$, where $[i] = T^q - T$. For any $i \in \mathbb{Z}_{\geq 0}$, let

$$S_i := \frac{(-1)^i}{L_i} = \sum_{a \in A_{i+}} \frac{1}{a}, \quad (4.9)$$

where the sum runs over all monics of degree i , [29]. Let F_i be the numerator of $\sum_{j=0}^i S_j$ (without cancelling of the common factors of the numerator and denominator, if present). Using

Equation (4.9), it is clear that $F_0 = 1$ and $L_0 = 1$. For each $i \in \mathbb{Z}_{\geq 0}$, we have

$$\frac{F_{i+1}}{L_{i+1}} = \sum_{j=0}^{i+1} \frac{(-1)^j}{L_j} = \frac{(-1)^{i+1}}{L_{i+1}} + \sum_{j=0}^i \frac{(-1)^j}{L_j} = \frac{(-1)^{i+1}}{L_{i+1}} + \frac{F_i}{L_i}.$$

Multiplying both sides with L_{i+1} , yields $F_{i+1} = (-1)^{i+1} + [i+1]F_i$. Moreover, if $\deg(P) = n$, then $[n] = T^q - T \equiv 0 \pmod{P}$ and so $F_n = (-1)^n + [n]F_{n-1} \equiv (-1)^n \pmod{P}$. We now show that P is a c -Wieferich prime if and only if $F_{-1+\deg(P)} \equiv 0 \pmod{P}$. The advantage of this congruence is that it is easier to check than the definition of c -Wieferich primes, Definition 4.3.10. However, it gets computationally expensive quickly as the degree increases.

Proposition 4.3.11. *P is a c -Wieferich prime in $\mathbb{F}_q[T]$ if and only if $F_{-1+\deg(P)} \equiv 0 \pmod{P}$.*

Proof. Let $n = \deg(P)$. By Lemma 2.2.1, $\rho_P(1) = \sum_{i=0}^n a_{P,i}$, with $a_{P,0} = P$, $a_{P,n} = 1$, and $[i]a_{P,i} = a_{P,i-1}^q - a_{P,i-1} \equiv -a_{P,i-1} \pmod{P^2}$. So, $L_i a_{P,i} \equiv (-1)^i a_{P,0} \pmod{P^2}$, $0 \leq i < n$, and

$$\rho_{P-1}(1) = \left(-1 + \sum_{i=0}^n a_{P,i} \right) \equiv \left(\sum_{i=0}^{n-1} a_{P,i} \right) \equiv \left(a_{P,0} \sum_{i=0}^{n-1} \frac{(-1)^i}{L_i} \right) \equiv P \sum_{i=0}^{n-1} S_i \equiv P \frac{F_{n-1}}{L_{n-1}} \pmod{P^2}.$$

Since $L_{\deg(P)-1} \not\equiv 0 \pmod{P}$, the proposition is now clear. \square

Remark 4.3.12. Proposition 4.3.11 is analogous to the following statement attributed to J. Sylvester, "a prime p is a Wieferich prime if and only if it divides the numerator of $\frac{1}{2} \sum_{i=1}^{\frac{\phi(p)}{2}} \frac{1}{i}$ ", see [21].

Remark 4.3.13. Proposition 4.3.11 is a micro form of D. Thakur's criterion for a prime to be a c -Wieferich prime, (quite hard to check). This asserts that, a prime P is a c -Wieferich prime if and only if P divides $\zeta_P(1)$, the P -adic Goss zeta function for the ring A at 1, see ([30], Theorem 5).

Below is an immediate consequence of Proposition 4.3.11.

Corollary 4.3.14. *There are no c -Wieferich primes of degree 1.*

Proof. If $\deg(P) = 1$, then $S_0 = 1$ and so $\rho_{P-1}(1) \equiv PF_0 = P \not\equiv 0 \pmod{P^2}$. \square

Theorem 4.3.15. *Let P be a prime of degree > 1 . P is a c -Wieferich prime in $\mathbb{F}_q[T]$ if and only if*

$$\rho_{P-1}(T) \equiv 0 \pmod{P^2}.$$

To prove Theorem 4.3.15, we shall need the following result.

Lemma 4.3.16. *For any monic irreducible P of degree n , $P' \equiv (-1)^{n-1} L_{n-1} \pmod{P}$.*

Proof. To prove this congruence, we compute the derivative of D_n with respect to T , reduce it modulo P in two different ways, and relate the results. Upon reduction modulo P , no two distinct monic polynomials of degree n map to the same element modulo P (or residue

class in A/PA). Moreover, the prime P is mapped to 0 and the rest to the units in A/PA . So we get $P^{-1}D_n \equiv \prod_{a \in (A/PA)^*} a \equiv -1 \pmod{P}$, the last equivalence is by Wilson's Theorem, Corollary 1.1.10. So $D_n \equiv -P \pmod{P^2}$. Differentiating both sides of the congruence with respect to T yields $D'_n \equiv -P' \pmod{P}$. Also $D_n = [n][n-1]^q \cdots [1]^{q^{n-1}} = [n]D_{n-1}^q$ which upon differentiation with respect to T yields $D'_n = -D_{n-1}^q$. Reducing D'_n modulo P , yields

$$D'_n = -D_{n-1}^q = -[n-1]^q \cdots [1]^{q^{n-1}} = -([n] - [1]) \cdots ([n] - [n-1]) \equiv (-1)^n L_{n-1} \pmod{P}.$$

Combining the two congruences, we get $-P' \equiv (-1)^n L_{n-1} \pmod{P}$, and we are done. \square

Proof of Theorem 4.3.15. Let P be a prime of degree n , then $\rho_P(T) = \sum_{i=0}^n a_{P,i} T^i$, where $a_{P,0} = P$, $a_{P,n} = 1$ and $[i]a_{P,i} = a_{P,i-1}^q - a_{P,i-1}$. Differentiating $[i]a_{P,i} = a_{P,i-1}^q - a_{P,i-1}$, $1 \leq i \leq n$ with respect to T , followed by reduction modulo P yields $[i]a'_{P,i} \equiv -a'_{P,i-1} \pmod{P}$. This yields the following recursive relation $a'_{P,i} \equiv a'_{P,0} S_i \equiv P' S_i \pmod{P}$, $1 \leq i \leq n$. So,

$$\begin{aligned} (\rho_{P-1}(T))' &= \left(-T + \sum_{i=0}^n a_{P,i} T^i \right)' \\ &\equiv \left(-1 + \sum_{i=0}^{n-1} a'_{P,i} T^i \right) \\ &\equiv \left(-1 + P' \sum_{i=0}^{n-1} S_i T^i \right) \\ &\equiv \left(-1 + P'T + P' \left(\sum_{i=1}^{n-1} S_i (T + [i]) \right) \right) \\ &\equiv \left(-1 + P'T + P' \left(\sum_{i=1}^{n-1} TS_i + [i]S_i \right) \right) \\ &\equiv \left(-1 + P'T + P' \left(\sum_{i=1}^{n-1} TS_i - S_{i-1} \right) \right) \\ &\equiv \left(-1 + P' \left(TS_{n-1} + (T-1) \sum_{i=0}^{n-2} S_i \right) \right) \\ &\equiv \left(-1 + P' \left(S_{n-1} + (T-1) \sum_{i=0}^{n-1} S_i \right) \right) \\ &\stackrel{\text{Lemma 4.3.16}}{\equiv} (T-1)P' \sum_{i=0}^{n-1} S_i \\ &\equiv (T-1)P' \frac{F_{n-1}}{L_{n-1}} \equiv 0 \pmod{P}. \end{aligned}$$

by assumption, and so $\rho_{P-1}(T) \equiv 0 \pmod{P^2}$. If $\deg(P) > 1$, then $\rho_{P-1}(T) \equiv 0 \pmod{P^2}$ if and only if $F_{-1+n} \equiv 0 \pmod{P}$, the condition in Proposition 4.3.11. Lastly Corollary 4.3.14, tells us there are no degree 1 c -Wieferich primes so all these are c -Wieferich primes. \square

Remark 4.3.17. *If P is c - Wieferich prime then it is also a non c - Wieferich prime to the base T .*

Theorem 4.3.18. *There are infinitely many c - Wieferich primes in $\mathbb{F}_2[T]$.*

Proof. It is not hard to show by induction on n , that $[1]F_{-1+n} = [n]$ for $n \geq 1$. So

$$[1]F_n = [1](1 + [n]F_{n-1}) = [1] + [1][n]F_{-1+n} = [1] + [n]^2 = [1] + [n + 1] + [1] = [n + 1].$$

Since $[n]$ is the product of all primes in A of degree dividing n . We have $F_{-1+n} \equiv 0 \pmod{Q_n}$ and so all primes in $\mathbb{F}_2[T]$ are c - Wieferich primes, with exception of degree one primes. \square

The same result had been observed earlier on by D. Thakur, (*through private communications*).

Remark 4.3.19. *Theorem 4.3.18 is a simple consequence of $\rho_{P-1}(1) = 0$ for any prime P in $\mathbb{F}_2[T]$.*

Proposition 4.3.11 provides a schematic way of checking whether a prime P is c - Wieferich or not. Alternatively, it gives a schematic short-cut to computing c - Wieferich primes in A .

Algorithm 1 Computing Carlitz - Wieferich primes I.

Input: p - the characteristic of A , and n - the degree of a Wieferich prime.

Output: Product of c - Wieferich primes of degree dividing n

1. $F \leftarrow 1$

2. for $i = 1$ to $n - 1$

$$F \leftarrow (-1)^i + (T^{p^i} - T)F$$

3. $\mathcal{B} \leftarrow \text{GCD}(T^{p^n} - T, F)$

Return: \mathcal{B}

The disadvantage of this scheme is the exponential growth in the degrees involved in step 2.

Below is some experimental evidence for existence of c - Wieferich primes in $\mathbb{F}_p[T]$. We obtained it upon implementing Algorithm 1 in SAGE. Over $\mathbb{F}_3[T]$, we got the following sequence of primes $T^6 + T^4 + T^3 + T^2 + 2T + 2$, $T^9 + T^6 + T^4 + T^2 + 2T + 2$, $T^{12} + 2T^{10} + T^9 + 2T^4 + 2T^3 + T^2 + 1$ and $T^{15} + T^{13} + T^{12} + T^{11} + 2T^{10} + 2T^7 + 2T^5 + 2T^4 + T^3 + T^2 + T + 1$. The first three primes have appeared in the works of D. Thakur. There were no c - Wieferich primes of degrees 3, 18, 21, \dots , 48 in this sequence for $\mathbb{F}_3[T]$. It took 3 days using brute force on a *duo core 32-bit machine with intel microprocessor* to search the third term of the sequence, 5 minutes to check it using the definition of c - Wieferich primes and it took under a minute to compute it using the congruence in Proposition 4.3.11. It took 30 seconds to find the fourth term while using the same criterion, (*we were unable to compute this using brute force algorithm*,

even on an i5 machine, with intel microprocessor). Over $\mathbb{F}_5[T]$, we obtained $T^5 + 4T + 1$ and $T^{10} + 3T^6 + 4T^5 + T^2 + T + 1$, after which we ran out of computation memory. This gives an idea on how difficult it is to compute c -Wieferich primes in $\mathbb{F}_q[T]$, even for small q .

We now prove Theorem 4.3.21, the first step in our characterisation of c -Wieferich primes.

Proposition 4.3.20. *Let $\alpha \in \mathbb{F}_p^*$, then $f = T^p - T - \alpha$ is a prime in $\mathbb{F}_p[T]$ and for any $n \in \mathbb{Z}_+$*

$$[n] \equiv n\alpha \pmod{T^p - T - \alpha}.$$

Proof. f is an Artin Schreier polynomial for $\mathbb{F}_p[T]$, and these are irreducible over \mathbb{F}_p , so f is a prime. Lastly, $[n] = (T^p - T)^{p^{n-1}} + (T^p - T)^{p^{n-2}} + \dots + (T^p - T)^{p^0} \equiv n\alpha \pmod{f}$. \square

Let us denote the n th partial sum of the complex exponential function by $s_n(x) := \sum_{i=0}^n \frac{x^i}{i!}$.

Theorem 4.3.21 (Horizontal Existence Theorem). *If there exists an $\alpha \in \mathbb{F}_p^*$ such that p divides $s_{p-1}(-\alpha^{-1})$, then $T^p - T - \alpha$ is a c -Wieferich prime in $\mathbb{F}_p[T]$.*

Proof. Fix $\alpha \in \mathbb{F}_p^*$ and define u_n by, $u_0 = 1$, $u_n = (-1)^n + n\alpha u_{n-1} \in \mathbb{F}_p^*$ for $1 \leq n < p$. Then,

$$\frac{u_n}{n!\alpha^n} = \frac{(-1)^n}{n!\alpha^n} + \frac{u_{n-1}}{(n-1)!\alpha^{n-1}} = \frac{(-1)^n}{n!\alpha^n} + \frac{(-1)^{n-1}}{(n-1)!\alpha^{n-1}} + \frac{u_{n-2}}{(n-2)!\alpha^{n-2}} = \dots = \sum_{i=0}^n \frac{(-1)^i}{i!\alpha^i}.$$

Since $n < p$, this $s_n(-\alpha^{-1})$ makes sense in \mathbb{F}_p . So $u_{p-1} = -s_{p-1}(-\alpha^{-1})$. Now, $F_n = (-1)^n + [n]F_{-1+n} \equiv (-1)^n + n\alpha F_{-1+n} \pmod{T^p - T - \alpha}$ for any $n \geq 1$ and $F_0 = 1$. So $u_n \equiv F_n \pmod{T^p - T - \alpha}$. So if $s_{p-1}(-\alpha^{-1}) \equiv 0 \pmod{p}$, then we get

$$u_{-1+p} \equiv F_{p-1} \equiv 0 \pmod{T^p - T - \alpha},$$

where $T^p - T - \alpha$ is Artin Schreier in $\mathbb{F}_p[T]$. The result follows from Proposition 4.3.11. \square

Remark 4.3.22. *Theorem 4.3.21 is referred to as Horizontal Existence Theorem because we vary the prime p , (i.e., characteristic of $\mathbb{F}_q[T]$) and give a criterion for obtaining a c -Wieferich prime in $\mathbb{F}_p[T]$, as opposed to searching c -Wieferich primes of higher degrees in $\mathbb{F}_p[T]$ for a fixed p .*

If $s_{p-1}(x)$ is irreducible over \mathbb{F}_p as a polynomial in x , then no c -Wieferich primes of the form $T^p - T + x^{-1}$ exist in $\mathbb{F}_p[T]$. We apologise for the description below is purely experimental and no proofs are available at the moment. Almost two thirds of the primes less than 10^7 satisfy the congruence in Proposition 4.3.21, and c -Wieferich primes of degree p exist, e.g., 2, 5, 7, 11, 13, 19, 31, 37, 41, 43, 47, 53, 59, 67, 71, 73, 79, 83, 89, 97, (primes less than 100). The primes 3, 17, 23, 29, 61 are examples for which there are no c -Wieferich primes of degree p in the ring $\mathbb{F}_p[T]$. We pose two questions: are there infinitely many primes p_1 such that $s_{p_1-1}(\alpha) \equiv 0 \pmod{p_1}$ for some $\alpha \in \mathbb{F}_{p_1}^*$ and prime p_2 such that $s_{p_2-1}(\beta) \not\equiv 0 \pmod{p_2}$ for all $\beta \in \mathbb{F}_{p_2}^*$? At the end of 2013, D. Thakur pointed out to me that he had discovered the

same horizontal existence result at almost the same time as me [30]. D. Thakur and N. Elkies believe this horizontal distribution of the primes p may be close to being random, [30].

The examples of c - Wieferich primes obtained by the horizontal existence result above all have a property that they are invariant under the translation automorphisms of $\mathbb{F}_q[T]$. This turns out to be an important property exhibited by many c - Wieferich primes in $\mathbb{F}_q[T]$. It is this property that we explore next. Let $m \in \mathbb{F}_q[T]$, m is said to be a fixed polynomial if for any $i \in \mathbb{F}_q$, $m(T + i) = m(T)$. Let $m \in \mathbb{F}_q[T]$ be non fixed, then fixed polynomials can be obtained from m as follows. Firstly, by summing up all the translations for m , e.g., over $\mathbb{F}_3[T]$, $m = T^2 + T$ is not fixed, however $a = \sigma_0(m) + \sigma_1(m) + \sigma_2(m) = 2$ is fixed. Secondly, by taking the product of all the translations of m , e.g., $b = \sigma_0(m)\sigma_1(m)\sigma_2(m) = T^6 + T^4 + T^2$ is fixed. Lastly as a sum or product of fixed polynomials. In other words, fixed polynomials form a subring of $\mathbb{F}_q[T]$. When $q = p$, the situation is simple, however when q is a prime power, the notion of fixed is replaced by G fixed, where G is a non trivial subgroup of \mathbb{F}_q . In this setting, $m \in A$ is G - fixed if $m(T + j) = m(T)$ for all $j \in G$. With the exception of Theorem 4.3.24, all the statements that follow will be in respect to prime subfields.

Definition 4.3.23. Let P be a prime in $\mathbb{F}_q[T]$. P is a fixed c - Wieferich prime if it is both fixed and a c - Wieferich prime. A non fixed c - Wieferich prime is a c - Wieferich prime that is not fixed.

We shall need the following facts about fixed polynomials.

Theorem 4.3.24. Let $f \in \mathbb{F}_q[T]$. f is fixed if and only if $f = g([1])$ for some $g \in \mathbb{F}_q[T]$.

Proof. Let $f = \sum \alpha_i [1]^i \in \mathbb{F}_q[T]$. For any $j \in \mathbb{F}_q$, $f(T + j) = \sum \alpha_i ((T + j)^i - (T + j)^i) = f(T)$ hence f is fixed. Let $f \in \mathbb{F}_q[T]$ be fixed, (assume f is monic), then $g_1 = f - f(0)$ is also fixed. Since $g_1(0) = 0$, g_1 is divisible by T , and since g_1 is fixed, we have g_1 is divisible by all the translates $T + \alpha$, $\alpha \in \mathbb{F}_q$. Therefore, g_1 is divisible by $[1]$. Let $f_1 = [1]^{-s} g_1$, where s is the number of times T divides g_1 , then repeat the procedure. Since f is a polynomial in T (of degree n), this procedure eventually terminates (after at most n steps). Looking at the sequence of operations in reverse reveals that f is indeed a polynomial in $[1]$. \square

Our initial formulation of Theorem 4.3.24 was long, the statement above is due to A. Keet.

Corollary 4.3.25. If m is a fixed polynomial in $\mathbb{F}_p[T]$, then its degree is divisible by p .

Corollary 4.3.26. There are no fixed c - Wieferich primes in $\mathbb{F}_p[T]$ of degree less than p .

Proposition 4.3.27. There are infinitely many fixed prime polynomials in $\mathbb{F}_p[T]$.

Proof. Adapt the proof of Theorem 5.2.1. \square

Remark 4.3.28. If a prime f is fixed, then there exists another prime g such that $f = g([1])$. However, the converse is false, for example take $g = T$ is a prime while $f = g([1]) = [1]$ is not.

Proposition 4.3.29. *For each $n \in \mathbb{Z}_{\geq 0}$, F_n is a fixed polynomial in $\mathbb{F}_p[T]$.*

Proof. Proceed by induction on n . For $n = 0$, we have $F_0 = 1$ which is clearly a fixed polynomial. We are left to show that F_i is a fixed polynomial whenever F_{-1+i} is a fixed polynomial. Let $\sigma \in \text{Aut}(\mathbb{F}_p[T])$ be a non trivial translation, then

$$\sigma(F_i) = \sigma((-1)^i + [i]_{F_{-1+i}}) = (-1)^i + [i]\sigma(F_{-1+i}) = (-1)^i + [i]_{F_{-1+i}} = F_i.$$

□

Remark 4.3.30. *Not all of prime factors of F_n are fixed primes, e.g., F_3 in $\mathbb{F}_2[T]$ and $\mathbb{F}_3[T]$.*

The following lemma will be important in the proof of Theorem 4.3.32.

Lemma 4.3.31. *Every fixed prime in $\mathbb{F}_p[T]$ is a product of Artin Schreier primes in some $\mathbb{F}_{p^r}[T]$.*

Proof. Let $f \in \mathbb{F}_p[T]$ be a fixed prime of degree ps , $\alpha \in \mathbb{F}_{p^{ps}}$ be a root of f but not in any $\mathbb{F}_{p^{ps}}$ sub-extension. Since f is irreducible over \mathbb{F}_p , $\mathbb{F}_{p^{ps}} = \mathbb{F}_p(\alpha)$ is the splitting field of f over \mathbb{F}_p . Since f is fixed, for any chosen root $\alpha \in \mathbb{F}_{p^{ps}}$, of f , $\alpha + \mathbb{F}_p$ is a subset of roots of f . Consider

$$g = \prod_{j \in \{0, 1, \dots, p-1\}} (T - (\alpha + j)) = (T - \alpha)^p - (T - \alpha) = T^p - T - \alpha^p + \alpha.$$

$\alpha^p - \alpha \in \mathbb{F}_{p^{ps}}$ but is no longer primitive. To be precise, (take $\beta = \alpha$), then

$$\mathcal{N}_{\mathbb{F}_{p^{ps}}/\mathbb{F}_{p^s}}(\alpha) = (-1)^p \prod_{j=0}^{p-1} (\alpha + j) = -\alpha^p + \alpha \in \mathbb{F}_{p^s} \subset \mathbb{F}_{p^{ps}},$$

Since $s \geq 1$, and $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(\alpha^p - \alpha) \neq 0$, g is an Artin Schreier polynomial (prime in $\mathbb{F}_{p^s}[T]$) dividing f . All the other roots will yield the same conclusion, hence the required result. □

Let E, F be finite fields of the same characteristic such that E/F is a Galois extension. An $\alpha \in E/F$ is normal if $\{\sigma(\alpha) : \sigma \in \text{Gal}(E/F)\}$ is a basis of E as an F -vector space. The Galois group $\text{Gal}(E/F)$ is cyclic, with Frobenius ($x \mapsto x^{|F|}$) as its generator. Lemma 4.3.31 shows that fixed c -Wieferich primes factor into Artin Schreier primes in some $\mathbb{F}_{p^r}[T]$, $r > 0$.

Theorem 4.3.32 (Fixed c -Wieferich Prime Existence Theorem). *There exists a fixed c -Wieferich prime of degree ps in $\mathbb{F}_p[T]$ if and only if there exists $\alpha \in \mathbb{F}_{p^s}$, normal with $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(\alpha) \neq 0$ and*

$$F_{-1+ps} \equiv 0 \pmod{T^p - T - \alpha}.$$

Proof. (\Leftarrow) Given $F_{-1+ps} \equiv 0 \pmod{T^p - T - \alpha}$, we have $F_{-1+ps} = (T^p - T - \alpha)g$, for some non zero polynomial $g \in \mathbb{F}_{p^{ps}}[T]$. Since the absolute trace of α over \mathbb{F}_p is non zero, by [18, Corollary 3.79], $T^p - T - \alpha$ is irreducible over \mathbb{F}_p . For any $\sigma \in \text{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)$, $\sigma(\alpha)$ is a conjugate to α , (there are s distinct elements since α is normal in $\mathbb{F}_{p^s}/\mathbb{F}_p$), so

$$F_{-1+ps} = \sigma(F_{-1+ps}) = \sigma(T^p - T - \alpha)\sigma(g) = (T^p - T - \sigma(\alpha))\sigma(g) \equiv 0 \pmod{T^p - T - \sigma(\alpha)}.$$

Let $Q_{ps} = (T^p - T - \alpha_1) \cdots (T^p - T - \alpha_s)$, where α_i are α -conjugates. By Galois theory $Q_{ps} \in \mathbb{F}_p[T]$ and by the Chinese Remainder Theorem, we have $F_{-1+ps} \equiv 0 \pmod{Q_{ps}}$. Since the α_i 's are normal in $\mathbb{F}_{p^s}/\mathbb{F}_p$, Q_{ps} is irreducible over \mathbb{F}_p and has degree ps . By Proposition 4.3.11, Q_{ps} is a fixed c -Wieferich prime. (\Rightarrow) The converse follows from Lemma 4.3.31. \square

Remark 4.3.33. Every fixed c -Wieferich prime factors into Artin Schreier primes in some $\mathbb{F}_{p^r}[T]$.

The above results can be extended to \mathbb{F}_q , where q is a prime power. Preliminary results suggest that this comes at a cost, e.g., the notion of fixed is replaced by G -fixed. In addition, Theorem 4.3.32 gives a better algorithm compared to Algorithm 1.

Algorithm 2 Computing Carlitz - Wieferich primes II.

Input: p, s , and \mathcal{B} , the list of normal elements of $\mathbb{F}_{p^s}/\mathbb{F}_p$.

Output: \mathcal{B} , list of Wieferich primes of degree ps .

1. \mathcal{W} , // List of non conjugate normal elements of \mathbb{F}_{p^s} , (as an \mathbb{F}_p -vector space).
2. for $i = 1$ to size of \mathcal{W}
 - $W \leftarrow (T^p - T - \mathcal{W}_i)W$, // \mathcal{W}_i is the i th element in \mathcal{W} .
3. $\mathcal{B} \leftarrow$ Prime factors of W as an element in $\mathbb{F}_p[T]$.

Return: \mathcal{B}

Using Algorithm 2, we were able to extend the list of c -Wieferich primes in $\mathbb{F}_5[T]$ by $T^{20} + T^{16} + 4T^{15} + T^{12} + 3T^{11} + T^8 + 2T^7 + T^5 + T^4 + T^3 + 4T + 1$. For $\mathbb{F}_7[T]$, we found $T^7 + 6T + 3$, $T^{14} + 5T^8 + 5T^7 + T^2 + 2T + 3$. For $\mathbb{F}_{11}[T]$, we found $T^{11} + 10T + 4$, $T^{33} + 8T^{23} + 4T^{22} + 3T^{13} + 3T^{12} + 10T^{11} + 10T^3 + 4T^2 + T + 4$. For $\mathbb{F}_{13}[T]$, we found $T^{13} + 12T + 1$, $T^{13} + 12T + 8$. For $p = 13$, we found two Wieferich primes of degree 13, all of which are Artin Schreier primes. There are at most $p - 1$ Carlitz Wieferich primes of degree p in $\mathbb{F}_p[T]$, this depends on the solubility of the polynomial congruence $s_{p-1}(x) \equiv 0 \pmod{p}$. We also observed that higher degree c -Wieferich primes appear in degrees divisible by p . Apart from $p = 3$, another example worthy pointing out is the prime number $p = 29$. A hard computation revealed $T^{58} + 27T^{30} + 15T^{29} + T^2 + 14T + 3$ as a c -Wieferich prime in $\mathbb{F}_{29}[T]$. We failed to find any examples of c -Wieferich primes for $p = 17, 23$. For $p = 37$, we found $T^{37} + 36T + 1$, $T^{37} + 36T + 7$, $T^{37} + 36T + 15$, $T^{37} + 36T + 21$, $T^{74} + 35T^{38} + 12T^{37} + T^2 + 25T + 5$.

In Tables 4.1 and 4.2, we show the first few fixed c -Wieferich primes in $\mathbb{F}_3[T]$ and $\mathbb{F}_5[T]$ with their corresponding normal elements in subfields of $\overline{\mathbb{F}_p}$ used to compute them.

s	$f_{\min}^t(x)$	Normal elements $\alpha \in \mathbb{F}_3^s$	Wieferich primes P
1	-	-	-
2	$x^2 + 2x + 2$	$\{2t, t + 2\}$	$T^6 + T^4 + T^3 + T^2 + 2T + 2$
3	$x^3 + 2x + 1$	$\{t^2, t^2 + t + 1, t^2 + 2t + 1\}$	$T^9 + T^6 + T^4 + T^2 + 2T + 2$
4	$x^4 + 2x^3 + 2$	$\{t^3 + t^2 + t + 2, 2t^3 + 2t^2 + 2t + 2, t^3 + t^2 + 2, 2t^3 + 2t^2\}$	$T^{12} + 2T^{10} + T^9 + 2T^4 + 2T^3 + T^2 + 1$
5	$x^5 + 2x + 1$	$\{t^3 + 2t^2 + 2t + 1, 2t^4 + 2t^3 + 2t, 2t^4 + t^2, t^3 + t^2 + 1, 2t^4 + 2t^3 + 2t^2 + 2t\}$	$T^{15} + T^{13} + T^{12} + T^{11} + 2T^{10} + 2T^7 + 2T^5 + 2T^4 + T^3 + T^2 + T + 1$
6	-	-	-
7	-	-	-

Table 4.1. Normal elements in subfields of $\overline{\mathbb{F}}_3$ and the corresponding c - Wieferich primes.

s	$f_{\min}^t(x)$	Normal elements $\alpha \in \mathbb{F}_5^s$	Wieferich primes P
1	$x + 1$	$\{4\}$	$T^5 + 4T + 1$
2	$x^2 + 4x + 2$	$\{2t + 2, 3t + 4\}$	$T^{10} + 3T^6 + 4T^5 + T^2 + T + 1$
3	$x^3 + 3x + 3$	-	-
4	$x^4 + 4x^2 + 4x + 2$	$\{t^3 + t^2 + 4, 3t^3 + 3t^2 + t + 4, t + 4, t^3 + t^2 + 3t + 4\}$	$T^{20} + T^{16} + 4T^{15} + T^{12} + 3T^{11} + T^8 + 2T^7 + T^5 + T^4 + T^3 + 4T + 1$
5	-	-	-
6	-	-	-

Table 4.2. Normal elements in subfields of $\overline{\mathbb{F}}_5$ and the corresponding c - Wieferich primes.

Our computations together with the above results motivate the following questions.

Question 4.3.34. *Are there finitely or infinitely many fixed c - Wieferich primes in $\mathbb{F}_p[T]$, $p > 2$?*

Question 4.3.35. *Suppose $p \neq 2$, are there any examples of non fixed c - Wieferich primes in $\mathbb{F}_p[T]$?*

Or equivalently, if $p \neq 2$, does P being a c - Wieferich prime in $\mathbb{F}_p[T]$ imply P is fixed?

We do not know the complete answer to these problems, however, in the case where $p = 2$, Theorem 4.3.18 gives a complete answer. Below are a few arguments in this direction.

Let $a \in \mathbb{Z}_{\geq 2}$ be a primitive root modulo p , a is said to be a *bad primitive root* if it is not a primitive root modulo p^2 . In fact, if a is a bad primitive root modulo p , then p is a Wieferich prime to the base a . In addition, we define a prime p to be "generous" if the least positive primitive root modulo p is also primitive root modulo p^2 . We are interested in this class of primes because of their connection with Wieferich primes, (here is the link, if a prime p is non generous, then p is a Wieferich prime to the base a , where a is the least positive primitive root modulo p). Most primes are generous, the only known examples of non generous primes are 2, 40487, 6692367337, see SLOANE's **A055578** on OEIS. There are other Wieferich primes, e.g., 1093 and 3511 which do not arise from primitive roots. In the $\mathbb{F}_q[T]$ case, we have the following analogous results, but first we give the following definition.

Definition 4.3.36. .

1. Let P be a prime and $a \in \{f \in A : \deg(f) < \deg(P)\} - \{0\}$. a is a primitive root modulo P if there exists not proper monic divisor D of $P - 1$ such that $\rho_D(a) \equiv 0 \pmod{P}$.
2. Let $a \in A$ be a primitive root modulo P , a is a bad primitive root modulo P if it is not a primitive root modulo P^2 . In addition, we define a prime P to be "generous" if for any least (in degree) monic primitive root modulo P is also primitive root modulo P^2 .

Theorem 4.3.37. *Let $p \neq 2$. If 1 is a bad primitive root mod P , then P is a fixed c - Wieferich prime.*

Proof. For the prime P , 1 is a bad primitive root mod P means that there is no D of $P - 1$ different from $P - 1$ such that $\rho_D(1) \equiv 0 \pmod{P}$ and $\rho_{P-1}(1) \equiv 0 \pmod{P^2}$. This means that P is a c - Wieferich prime. Assume P is a non fixed in $\mathbb{F}_p[T]$. For any non trivial translation $\mathbb{F}_p[T]$ automorphism σ , we have $\sigma(\rho_{P-1}(1)) = \rho_{\sigma(P)-1}(1) \equiv 0 \pmod{\sigma(P)^2}$. Alternatively $F_{-1+\deg(P)} \equiv 0 \pmod{P, \sigma(P)}$ since F_i is a fixed polynomial. This implies that $\sigma(P)$ is also a non fixed c - Wieferich prime in $\mathbb{F}_p[T]$. So $F_{-1+\deg(P)} = g \prod_{\sigma \in \text{Aut}(\mathbb{F}_p[T])} \sigma(P)$ and

$$\begin{aligned} \rho_{\sigma(P)-1}(1) &= \sigma(\rho_{P-1}(1)) \equiv \sigma\left(\frac{PF_{-1+\deg(P)}}{L_{-1+\deg(P)}}\right) \\ &\equiv \sigma\left(\frac{g \prod_{\sigma'} \sigma'(P)}{L_{-1+\deg(P)}}\right) \equiv \frac{P\sigma(g)\sigma(\prod_{\sigma' \neq \sigma^{-1}} \sigma'(P))}{L_{-1+\deg(P)}} \pmod{P^2}. \end{aligned}$$

For any $\sigma \in \text{Aut}(\mathbb{F}_p[T])$, we have $\rho_{\sigma(P)-1}(1) \equiv 0 \pmod{P}$. Since $p \neq 2$, $\rho_{\sigma(P)-1}(1) \neq 0$, and in addition since 1 is a primitive root modulo P , we have two possible cases to consider.

1. Suppose that $P \equiv 1 \pmod{\sigma(P) - 1}$, by degree comparison and the fact that σ preserves monicity, we have $\sigma(P) = P$, and so P is a fixed prime, a contradiction.
2. Suppose $\sigma(P) - 1 \equiv 0 \pmod{P}$. Since σ preserves monicity, $\deg(P) = \deg(\sigma(P) - 1)$. So the supposition $\sigma(P) - 1 \equiv 0 \pmod{P}$ implies that $\sigma(P) = P + 1$. Without loss of generality, take $\sigma = \sigma^1$, then we have the recursive formula $\sigma^i(P) = \sigma^{i-1}(P) + 1 = \sigma^{i-j}(P) + j = P + i$ for $i = 0, 1, \dots, p - 1$. Since P is prime, $P(0) \neq 0$, as i runs through $0, 1, \dots, p - 1$, there is a $j \in \mathbb{F}_q$ such that $P(0) + j = 0$ in which case, we have $\sigma^j(P) = P + j = P - P(0) + P(0) + j$ which is no longer irreducible, a contradiction.

These contradictions show that P must be a fixed polynomial. □

Remark 4.3.38. Theorem 4.3.37 shows that in addition to the prime P being c -Wieferich, it is also fixed. However, we have no right analogue for the notion "fixed" in the case of integers.

Remark 4.3.39. In general, the converse of Theorem 4.3.37 is false. There are some fixed c -Wieferich primes which do not satisfy this criterion, e.g., $P = T^9 + T^6 + T^4 + T^2 + 2T + 2$ in $\mathbb{F}_3[T]$ and $T^{20} + T^{16} + 4T^{15} + T^{12} + 3T^{11} + T^8 + 2T^7 + T^5 + T^4 + T^3 + 4T + 1$ in $\mathbb{F}_5[T]$.

Remark 4.3.40. All primes for which $a = 1$ is a bad primitive root are necessarily generous.

Proposition 4.3.41. The number of fixed polynomials in $\mathbb{F}_p[T]$ of degree pi is p^i .

Proof. The fixed monics in $\mathbb{F}_p[T]$ of degree pi are in bijection with monics in $\mathbb{F}_p[T]$ of degree i . The result follows from the fact that there are p^i monics in $\mathbb{F}_p[T]$ of degree i . □

Remark 4.3.42. The ratio of number of fixed to non fixed polynomials of degree n tends to 0 as $n \rightarrow \infty$. In other words, fixed polynomials become more rare compared to non fixed ones as $n \rightarrow \infty$.

What follows is background material for our probabilistic heuristics on the number of c -Wieferich primes. The underlying heuristic is commonly used throughout (computational) number theory. We apologise for this part of the thesis, since this is, of course, an extremely vague and completely non-rigorous mathematics, requiring a subjective and ad hoc determination of what an "obvious reason" is. However, in practice it tends to give remarkably plausible predictions, some fraction of which can in fact be backed up by rigorous argument.

Heuristic 4.3.43 (Borel - Cantelli). Suppose E_1, E_2, \dots is a sequence of number-theoretic statements, which we heuristically interpret as probabilistic events with probabilities $\mathbf{P}(E_1), \mathbf{P}(E_2), \dots$. Suppose we know of no obvious reason for these events to have correlations with each other. Then:

1. If $\sum_{i=1}^{\infty} \mathbf{P}(E_i) < \infty$, we expect only finitely many of the statements E_n to be true. (And if $\sum_{i=1}^{\infty} \mathbf{P}(E_i)$ is much smaller than 1, we in fact expect none of the E_n to be true.)
2. If $\sum_{i=1}^{\infty} \mathbf{P}(E_i) = \infty$, we expect infinitely many of the statements E_n to be true.

This heuristic is motivated both by the Borel - Cantelli Lemma, and by the standard probabilistic computation that if one is given jointly independent, and genuinely probabilistic, events E_1, E_2, \dots with $\sum_{i=1}^{\infty} \mathbf{P}(E_i) = \infty$, then one almost surely has an infinite number of the E_i occurring. We imitate classical heuristics first, then suggest more realistic assumptions.

Classical heuristic. Consider $\mathbb{F}_p[T]$, $p \neq 2$. By Fermat's Little Theorem, $\rho_{P-1}(1) \equiv 0 \pmod{P}$ for any prime P . Assume $g_{1,P} = P^{-1}\rho_{P-1}(1)$ is a random polynomial modulo P , so that it is divisible by P with probability² $\frac{1}{|P|}$. This assumption and therefore the argument fails for $p = 2$, because $\rho_{P-1}(1) = 0$ for any prime P with $\deg(P) \geq 2$. We are led to suspect that the total number of primes P such that $|P| \leq x$ and $\rho_{P-1}(1) \equiv 0 \pmod{P^2}$ is asymptotically

$$\sum_{|P| \leq x} \frac{1}{|P|} = \sum_{i=1}^{\lfloor \log_p(x) \rfloor} \frac{\pi_{\mathbb{F}_p[T]}(i)}{p^i} = \sum_{i=1}^{\lfloor \log_p(x) \rfloor} \left(\frac{1}{i} + \mathcal{O}\left(\frac{1}{ip^{\frac{i}{2}}}\right) \right) \approx \log(\log_p(x)).$$

□

This is analogous to the classically conjectured asymptotic which asserts that, the number of Wieferich primes $p \leq x$ is $\sim \log(\log(x))$. However, the above heuristic is misleading, a more accurate heuristic is obtained by assuming $g_{1,P}$ is not entirely random modulo P . It has some exotic structure and conspiracies that are not quite obvious on surface value.

A new heuristic. Firstly, assume that if P is a fixed prime, then $g_{1,P}$ is random modulo P . Secondly, if P is not a fixed prime, the probability of P dividing $g_{1,P}$ is $\frac{1}{|P|^p}$. This is because every time a non fixed prime P divides $g_{1,P}$, p other primes of the same degree (from the orbit of P) must divide $g_{1,P}$, see proof of Theorem 4.3.37. Alternatively, think of this as the probability that a (prime) polynomial of degree $p \deg(P)$ divides $g_{1,P}$. This is equivalent to asking the probability that $F_{-1+\deg(P)} \equiv 0 \pmod{P}$ happens. Let $\pi_F(i)$ be the number of fixed primes of degree i and $\pi_N(i)$ be the number of non fixed primes of degree i . Let

$$\chi(P) := \begin{cases} \frac{1}{|P|}, & \text{if } P \text{ is fixed,} \\ \frac{1}{|P|^p}, & \text{if } P \text{ is not fixed,} \end{cases}$$

be a sieve. By Proposition 4.3.41, we have $\pi_F(pi) = \pi_{\mathbb{F}_p[T]}(i)$, (since all the fixed primes of degree pi arise from monic irreducibles of degree i) and in addition $\pi_N(i) \leq \pi_{\mathbb{F}_p[T]}(i)$, so

²The term probability here is fraught with some peril. It is better to say the natural density of the polynomials divisible by P is $\frac{1}{|P|}$. This captures what we would think of as probability, i.e., the limiting proportion.

$$\begin{aligned}
\sum_P \text{Prob}(g_{1,P} \equiv 0 \pmod{P}) &= \lim_{x \rightarrow \infty} \left(\sum_{|P| \leq x} \chi(P) \right) = \lim_{x \rightarrow \infty} \left(\sum_{i=1}^{\lfloor \log_p(x) \rfloor} \sum_{\deg(P)=i} \chi(P) \right) \\
&= \lim_{x \rightarrow \infty} \left(\sum_{i=1}^{\lfloor \frac{\log_p(x)}{p} \rfloor} \frac{\pi_F(pi)}{p^{pi}} + \sum_{i=1}^{\lfloor \log_p(x) \rfloor} \frac{\pi_N(i)}{p^{pi}} \right) \\
&\leq \lim_{x \rightarrow \infty} \left(\sum_{i=1}^{\lfloor \frac{\log_p(x)}{p} \rfloor} \frac{p^i}{p^{pi}} + \sum_{i=1}^{\lfloor \log_p(x) \rfloor} \frac{p^i}{p^{pi}} + \mathcal{O} \left(\sum_{i=1}^{\lfloor \log_p(x) \rfloor} \frac{p^{\frac{i}{2}}}{ip^{pi}} \right) \right) \\
&= \sum_{i=1}^{\infty} \frac{1}{p^{(p-1)i}} + \sum_{i=1}^{\infty} \frac{1}{ip^{(p-1)i}} + c_p < \infty,
\end{aligned}$$

all of which are convergent by the comparison test. So it is likely that the number of primes P in $\mathbb{F}_p[T]$ for which $\rho_{p-1}(1) \equiv 0 \pmod{P^2}$ tends to a finite limit as $|P| \rightarrow \infty$. \square

As a consequence, we have finitely many c -Wieferich primes in $\mathbb{F}_p[T]$.

In summary, we examined the Carlitzian analogue of $x^n - y^n$, its properties and Zsigmondy factors. We imitated D. Birkhoff and H. Vandiver's proof [7] to establish an analogue of the Bang - Zsigmondy Theorem [3]. We connected Carlitz polynomial theory to the study of geometric Fermat equations, then gave Carlitzian analogues of Fermat pseudoprimes and Wieferich primes. Lastly, we proved some new existence results about this class of primes.

Chapter 5

Carlitz Wieferich primes (Part II)

This chapter is a follow up of the material on c - Wieferich primes in the preceding chapter. We extend results about fixed c - Wieferich primes to $\mathbb{F}_q[T]$. In chapter 4, we saw that if F_i is the numerator of $\sum_{j=0}^i (-1)^j (L_j)^{-1}$, then F_i satisfies the following recurrence relation, $F_0 = 1$ and for each $i \in \mathbb{Z}_{\geq 0}$, $F_{i+1} = (-1)^{i+1} + [i+1]F_i$. In Proposition 4.3.11, we proved that a prime P is a c - Wieferich prime in $\mathbb{F}_q[T]$ if and only if $F_{-1+\deg(P)} \equiv 0 \pmod{P}$. This gives an algorithmic short-cut to computing c - Wieferich primes in $\mathbb{F}_q[T]$, see Algorithm 3 below. Its worst disadvantage is the exponential growth in the degrees involved in step 3.

Algorithm 3 Computing Carlitz - Wieferich primes III.

Input: q - size of the base field of A , and n degree of Carlitz Wieferich primes required.

Output: Product of Wieferich primes of degree less than or equal to n .

1. $F \leftarrow 1$

2. for $i = 1$ to $n - 1$ $F \leftarrow (-1)^i + (T^{q^i} - T)F$

3. $\mathcal{B} \leftarrow \text{GCD}(T^{q^n} - T, F)$

Return: \mathcal{B}

In all the examples that follow, we shall let t be a primitive element in \mathbb{F}_q , where q is a p power, i.e., a root of the irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ such that $\mathbb{F}_q \cong \mathbb{F}_p[x]/\langle f(x) \rangle$. Below is some experimental evidence for existence of c - Wieferich primes in $\mathbb{F}_q[T]$, obtained using Algorithm 3 in SAGE. In $\mathbb{F}_{2^2}[T]$, we found $T^2 + T + t$ and $T^2 + T + t + 1$, while over $\mathbb{F}_{2^3}[T]$, we found $T^2 + T + 1, T^2 + T + t + 1, T^2 + T + t^2 + 1, T^2 + T + t^2 + t + 1, T^4 + T + 1, T^4 + T + t + 1, T^4 + T + t^2 + 1, T^4 + T + t^2 + t + 1$. Over $\mathbb{F}_{3^2}[T]$, we found $T^3 + (t+1)T + 1, T^3 + (t+1)T + t, T^3 + (t+1)T + 2t + 2, T^3 + (2t+2)T + 1, T^3 + (2t+2)T + t + 1, T^3 + (2t+2)T + 2t + 1$. Over $\mathbb{F}_{3^3}[T]$, we found no c - Wieferich primes of degree less than 6. In

$\mathbb{F}_{5^2}[T]$, we had $T^5 + 4T + 3$, $T^5 + 4T + t$, $T^5 + 4T + 2t + 2$, $T^5 + 4T + 3t + 4$ and $T^5 + 4T + 4t + 1$, after which we ran out of memory. Over $\mathbb{F}_{7^2}[T]$, we obtained $T^{49} + 6T + 3$ as the product of c -Wieferich primes. Below is the preliminary theory behind our algorithms.

5.1 Some results from the theory of finite fields

Theorem 5.1.1 ([18], Theorem 3.46). *Let s be a positive integer, and f be a prime in $\mathbb{F}_q[T]$ of degree n . Then f factors into d primes in $\mathbb{F}_{q^s}[T]$ of the same degree $\frac{n}{d}$, where $d = \gcd(s, n)$.*

Corollary 5.1.2. *A prime $f \in \mathbb{F}_q[T]$ of degree n is a prime in $\mathbb{F}_{q^s}[T]$ if and only if $\gcd(s, n) = 1$.*

Theorem 5.1.3. *Let p be the characteristic of \mathbb{F}_q , $\beta \in \mathbb{F}_q^*$ and $\gamma \in \mathbb{F}_{q^r}^*$ for some $r \in \mathbb{Z}_+$. The trinomial $T^p - \beta T - \gamma$ is irreducible over \mathbb{F}_{q^r} if and only if it has no root in \mathbb{F}_{q^r} .*

Proof. (\Leftarrow) Suppose $T^p - \beta T - \gamma$ has no root in \mathbb{F}_q and \mathbb{F}_{q^t} is the splitting field for $T^p - \beta T - \gamma$. Let $W = \{\chi \in \mathbb{F}_{q^{p-1}} : \chi^p - \beta\chi = 0\}$. Since the derivative of $T^p - \beta T - \gamma$ is $-\beta \neq 0$, the trinomial $T^p - \beta T - \gamma$ is separable. For a fixed root $\zeta \in \mathbb{F}_{q^t}$, the set of roots of $T^p - \beta T - \gamma$ is $\zeta + W = \zeta + \chi\mathbb{F}_p$, where $\chi \in W - \{0\}$. To show that $T^p - \beta T - \gamma$ is irreducible over \mathbb{F}_{q^r} , we assume it is divisible by $g \in \mathbb{F}_{q^r}[T]$ of degree $n < p$ to derive a contradiction. Let

$$g = \prod_{i=1}^n (T - \zeta - \chi_i),$$

where $\chi_i \in W$ are distinct. The coefficient of T^{n-1} in g is $n\zeta + \sum_{i=1}^n \chi_i \in \mathbb{F}_{q^r}$. Since $1 \leq n < p$, n is invertible in \mathbb{F}_{q^r} , so $\zeta \in \mathbb{F}_{q^r}$ if and only if $\sum_{i=1}^n \chi_i \in \mathbb{F}_{q^r}$. Since each χ_i is of the form $\alpha\chi$ for some $\chi \in W - \{0\}$ and $\alpha \in \mathbb{F}_p$, we have $\sum_{i=1}^n \chi_i = \kappa\chi$ for some $\kappa \in \mathbb{F}_p$. If $\kappa = 0$, then $\zeta \in \mathbb{F}_{q^r}$, a contradiction since all the roots are in \mathbb{F}_{q^t} , a non-trivial \mathbb{F}_{q^r} extension. Assume $\kappa \neq 0$, in this case $n\zeta + \kappa\chi \in \mathbb{F}_{q^r}$. Moreover, $(n\zeta + \kappa\chi)^p - \beta(n\zeta + \kappa\chi) - \gamma = n(\zeta^p - \beta\zeta) - \gamma + \kappa(\chi^p - \beta\chi) = (n-1)\gamma = 0$ if and only if $n = 1$. So g is of degree 1 hence $\zeta + \kappa\chi \in \mathbb{F}_{q^r}$ and so are the other roots (i.e., $T^p - \beta T - \gamma$ splits), which is a contradiction. (\Rightarrow) Trivial. \square

Theorem 5.1.4. *Let $\alpha \in \mathbb{F}_{q^r}$ with $\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) \neq 0$. Then there exists a $\beta \in \mathbb{F}_q^*$ and $\gamma_1, \dots, \gamma_{\frac{q}{p}} \in \mathbb{F}_{q^r}$, (all distinct) such that the trinomial $T^q - T - \alpha$ factorises as follows,*

$$T^q - T - \alpha = \prod_{j=1}^{\frac{q}{p}} (T^p - \beta T - \gamma_j). \quad (5.1)$$

If $\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = 0$, then $T^q - T - \alpha$ splits completely in $\mathbb{F}_{q^r}[T]$.

We shall refer to primes of the form $T^p - \beta T - \gamma$ in $\mathbb{F}_{q^s}[T]$ as *almost Artin Schreier* primes.

Proof. Firstly, if $\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = 0$, and ζ is a root to $T^q - T - \alpha$ in some \mathbb{F}_{q^r} extension. Then

$$0 = \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \dots + \alpha^{q^{r-1}} = (\zeta^q - \zeta) + (\zeta^q - \zeta)^q + \dots + (\zeta^q - \zeta)^{q^{r-1}} = \zeta^{q^r} - \zeta,$$

which implies that $\zeta \in \mathbb{F}_{q^r}$. So if $\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = 0$, it follows that $T^q - T - \alpha$ splits over \mathbb{F}_{q^r} .

Given $T^q - T - \alpha$, where $\alpha \in \mathbb{F}_{q^r}$ but not in any of its subfields since $\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) \neq 0$. Since derivative of $T^q - T - \alpha$ is a unit in $\mathbb{F}_q[T]$, it follows that $T^q - T - \alpha$ is square free. The set of roots of $T^q - T - \alpha$ is $\zeta + \mathbb{F}_q$, where $\zeta \in \mathbb{F}_{q^{rs}}$, (where s is a positive integer) is a root to $T^q - T - \alpha$. It follows that the $\text{Tr}_{\mathbb{F}_{q^{rs}}/\mathbb{F}_{q^r}}(\zeta_i)$ is the same for any $\zeta_i \in \zeta + \mathbb{F}_q$. Since finite field extensions are normal, the smallest field in which ζ sits is also the splitting field $T^q - T - \alpha$ over \mathbb{F}_q . We show that $\mathbb{F}_{q^{pr}}$ is the splitting field of $T^q - T - \alpha$. The trinomial $T^q - T - \alpha \in \mathbb{F}_{q^{rs}}[T]$ splits in $\mathbb{F}_{q^{rs}}[T]$ if (and only if) $\text{Tr}_{\mathbb{F}_{q^{rs}}/\mathbb{F}_q}(\alpha) = 0$. Since $\zeta^q - \zeta - \alpha = 0$, we have

$$\text{Tr}_{\mathbb{F}_{q^{sr}}/\mathbb{F}_q}(\alpha) = \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\text{Tr}_{\mathbb{F}_{q^{sr}}/\mathbb{F}_{q^r}}(\zeta^q - \zeta)) = \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(s\alpha) = s \cdot \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha).$$

The least $s \geq 1$ such that $\text{Tr}_{\mathbb{F}_{q^{rs}}/\mathbb{F}_q}(\alpha) = 0$ is p and so $\mathbb{F}_{q^{pr}}$ is the splitting field of $T^q - T - \alpha$. Since $\text{Gal}(\mathbb{F}_{q^{pr}}/\mathbb{F}_{q^r})$ is cyclic of order p , the prime factors of $T^q - T - \alpha$ all have degree p .

We now show these polynomials are of the form $T^p - \beta T - \gamma_j$, where β, γ_j are to be determined. Set $\gamma_j = \text{Norm}_{\mathbb{F}_{q^{pr}}/\mathbb{F}_{q^r}}(\zeta_j)$, the norm of ζ_j in \mathbb{F}_{q^r} and $\beta = \zeta_j^{-1}(\zeta_j^p - \gamma_j)$, it is clear $\beta \neq 0$. The roots of $T^p - \beta T - \gamma_j$ are $\zeta_j + W \subseteq \zeta_j + \mathbb{F}_q$, where $W := \{\chi \in \mathbb{F}_q : \chi^p - \beta\chi = 0\}$. To see that all the roots give the same β , note that $\mathcal{N}_{\mathbb{F}_{q^{pr}}/\mathbb{F}_{q^r}}(\zeta_j + \nu) = \gamma_j$ for any $\nu \in W$. So

$$\beta' = \frac{(\zeta_j + \nu)^p - \gamma_j}{\zeta_j + \nu} = \frac{\zeta_j^p - \gamma_j + \nu^p}{\zeta_j + \nu} = \frac{\beta\zeta_j + \beta\nu}{\zeta_j + \nu} = \beta.$$

So,

$$\alpha = \zeta^q - \zeta = \prod_{i \in \mathbb{F}_q} (\zeta + i) = \prod_{i \in W} (\zeta_j + i) \prod_{i \in \mathbb{F}_q - W} (\zeta_j + i) = (\zeta_j^p - \beta\zeta_j) \prod_{i \in \mathbb{F}_q - W} (\zeta_j + i) = \gamma_j \gamma'.$$

By construction, $T^p - \beta T - \gamma_j$ has no roots in \mathbb{F}_{q^r} and so by Proposition 5.1.3, $T^p - \beta T - \gamma_j$ is the minimal polynomial of its roots ζ_j over \mathbb{F}_{q^r} . Since there are $p^{-1}q$ distinct γ_i 's, we have $p^{-1}q$ different irreducible polynomials over \mathbb{F}_{q^r} all of the form $T^p - \beta T - \gamma_i$, one for each distinct γ_i . Comparing leading terms in addition to the fact that both sides of Equation (5.1) have the same roots, we have equality. \square

The examples below demonstrate Theorem 5.1.4 for different finite extensions with p small.

Example 5.1.5. Consider $q = 3^4$, and \mathbb{F}_{3^4} be a finite field parametrised by t , with $f_{\min}^t(x) = x^4 + 2x^3 + 2$, where irreducibility here is over \mathbb{F}_3 . Clearly $\alpha = t$ is a primitive element in \mathbb{F}_{3^4} and $\text{Tr}_{\mathbb{F}_{3^2}/\mathbb{F}_9}(t) = t^9 + t = t^3 + t^2 \neq 0$. By Proposition 5.1.4, there exists a unique $\beta \in \mathbb{F}_9^*$ such that $T^9 - T - t$ factors in $\mathbb{F}_{3^4}[T]$ into almost Artin Schreier primes. It is no surprise that,

$$\begin{aligned} T^9 - T - t &= (T^3 + (2t^3 + 2t^2 + 2)T + 2t^2 + t)(T^3 + (2t^3 + 2t^2 + 2)T + t^3 + t) \\ &\quad (T^3 + (2t^3 + 2t^2 + 2)T + 2t^3 + t^2 + t). \end{aligned}$$

Observe that, $p = 3$, $\beta = t^3 + t^2 + 1$ and the set of the γ_i 's is $\{2t^2 + t, t^3 + t, 2t^3 + t^2 + t\}$.

Take $\alpha = t^3 + t + 1$ another primitive element in \mathbb{F}_{3^4} . We find that $\text{Tr}_{\mathbb{F}_{3^2}/\mathbb{F}_9}(t^3 + t + 1) = 0$. By

Proposition 5.1.4, $T^9 - T - (t^3 + t + 1)$ splits completely in $\mathbb{F}_{3^4}[T]$. It is not surprising that,

$$\begin{aligned} T^9 - T - (t^3 + t + 1) &= (T + t^2 + 2t)(T + t^2 + 2t + 1)(T + t^2 + 2t + 2) \\ &\quad (T + t^3 + 2t^2 + 2t)(T + t^3 + 2t^2 + 2t + 1)(T + t^3 + 2t^2 + 2t + 2) \\ &\quad (T + 2t^3 + 2t)(T + 2t^3 + 2t + 1)(T + 2t^3 + 2t + 2). \end{aligned}$$

Example 5.1.6. Consider $q = 5^6$, and \mathbb{F}_{5^6} be a finite field parametrised by t , with $f_{\min}^t(x) = x^6 + x^4 + 4x^3 + x^2 + 2$, where irreducibility of $f_{\min}^t(x)$ is over \mathbb{F}_5 . Clearly $\alpha = t$ is a primitive element in \mathbb{F}_{5^6} and $\text{Tr}_{\mathbb{F}_{5^6}/\mathbb{F}_{5^2}}(t) = 0$. By *Proposition 5.1.4*, $T^{25} - T - t$ splits over \mathbb{F}_{5^2} .

$$\begin{aligned} T^{25} - T - t &= (T + t^4 + t^3 + t^2 + t)(T + t^4 + t^3 + t^2 + t + 1)(T + t^4 + t^3 + t^2 + t + 2) \\ &\quad (T + t^4 + t^3 + t^2 + t + 3)(T + t^4 + t^3 + t^2 + t + 4)(T + t^5 + 4t^4 + t^3 + 2t^2) \\ &\quad (T + t^5 + 4t^4 + t^3 + 2t^2 + 1)(T + t^5 + 4t^4 + t^3 + 2t^2 + 2) \\ &\quad (T + t^5 + 4t^4 + t^3 + 2t^2 + 3)(T + t^5 + 4t^4 + t^3 + 2t^2 + 4) \\ &\quad (T + 2t^5 + 2t^4 + t^3 + 3t^2 + 4t)(T + 2t^5 + 2t^4 + t^3 + 3t^2 + 4t + 1) \\ &\quad (T + 2t^5 + 2t^4 + t^3 + 3t^2 + 4t + 2)(T + 2t^5 + 2t^4 + t^3 + 3t^2 + 4t + 3) \\ &\quad (T + 2t^5 + 2t^4 + t^3 + 3t^2 + 4t + 4)(T + 3t^5 + t^3 + 4t^2 + 3t) \\ &\quad (T + 3t^5 + t^3 + 4t^2 + 3t + 1)(T + 3t^5 + t^3 + 4t^2 + 3t + 2) \\ &\quad (T + 3t^5 + t^3 + 4t^2 + 3t + 3)(T + 3t^5 + t^3 + 4t^2 + 3t + 4) \\ &\quad (T + 4t^5 + 3t^4 + t^3 + 2t)(T + 4t^5 + 3t^4 + t^3 + 2t + 1) \\ &\quad (T + 4t^5 + 3t^4 + t^3 + 2t + 2)(T + 4t^5 + 3t^4 + t^3 + 2t + 3) \\ &\quad (T + 4t^5 + 3t^4 + t^3 + 2t + 4). \end{aligned}$$

Let $\alpha = t + 1$, a primitive element in \mathbb{F}_{5^6} and $\text{Tr}_{\mathbb{F}_{5^6}/\mathbb{F}_{5^2}}(t) = 3 \neq 0$. By *Proposition 5.1.4*, there is a unique $\beta \in \mathbb{F}_{5^2}^*$ such that $T^{25} - T - (t + 1)$ factors in $\mathbb{F}_{5^6}[T]$ into almost Artin Schreier primes.

$$\begin{aligned} T^{25} - T - (t + 1) &= (T^5 + 4T + 4t^4 + 3t^3 + 4t^2 + 4)(T^5 + 4T + t^5 + 2t^4 + 3t^3 + 4t + 2) \\ &\quad (T^5 + 4T + 2t^5 + 3t^3 + t^2 + 3t)(T^5 + 4T + 3t^5 + 3t^4 + 3t^3 + 2t^2 + 2t + 3) \\ &\quad (T^5 + 4T + 4t^5 + t^4 + 3t^3 + 3t^2 + t + 1). \end{aligned}$$

Example 5.1.7. Consider $q = 2^6$, and \mathbb{F}_{2^6} be a finite field parametrised by t , with $f_{\min}^t(x) = x^6 + x^4 + x^3 + x + 1$ irreducible over \mathbb{F}_2 . Clearly $\alpha = t$ is a primitive element in \mathbb{F}_{2^6} and $\text{Tr}_{\mathbb{F}_{2^6}/\mathbb{F}_{2^3}}(t) = t^5 + t^4 + t^2 + 1 \neq 0$. By *Proposition 5.1.4*, there exists a unique $\beta \in \mathbb{F}_8^*$ such that

$$\begin{aligned} T^8 - T - t &= (T^2 + (t^5 + t^4 + t^2 + 1)T + t)(T^2 + (t^5 + t^4 + t^2 + 1)T + t^4 + t^2) \\ &\quad (T^2 + (t^5 + t^4 + t^2 + 1)T + t^5)(T^2 + (t^5 + t^4 + t^2 + 1)T + t^5 + t^4 + t^2 + t). \end{aligned}$$

If $\alpha = t$, a primitive element in \mathbb{F}_{2^6} and $\text{Tr}_{\mathbb{F}_{2^6}/\mathbb{F}_{2^2}}(t) = 1 \neq 0$, then by *Proposition 5.1.4*, there exists

a unique $\beta \in \mathbb{F}_4^*$ such that $T^4 - T - t$ factors in $\mathbb{F}_{2^6}[T]$ into almost Artin Schreier primes.

$$T^4 - T - t = (T^2 + T + t^5 + t^3)(T^2 + T + t^5 + t^3 + 1).$$

Take $\alpha = t^5 + t^4 + t^2 + t$ another primitive element in \mathbb{F}_{2^6} , then $\text{Tr}_{\mathbb{F}_{2^6}/\mathbb{F}_{2^2}}(t^5 + t^4 + t^2 + t) = 0$. By Proposition 5.1.4, $T^4 - T - (t^5 + t^4 + t^2 + t)$ splits completely in $\mathbb{F}_{2^6}[T]$. So,

$$\begin{aligned} T^4 - T - (t^5 + t^4 + t^2 + t) &= (T + t^5 + t^4 + t)(T + t^5 + t^4 + t + 1) \\ &\quad (T + t^5 + t^4 + t^3 + t^2)(T + t^5 + t^4 + t^3 + t^2 + 1). \end{aligned}$$

5.2 Computing G -fixed Carlitz Wieferich primes in $\mathbb{F}_q[T]$

Let $m \in \mathbb{F}_q[T]$, we define m to be a fixed polynomial in $\mathbb{F}_q[T]$ if for any $i \in \mathbb{F}_q$, we have $m(T + i) = m$. All constants in $\mathbb{F}_q[T]$ are fixed, and all degree one polynomials are not fixed. The least degree non constant fixed polynomial is $T^q - T$. Let G be a subgroup of \mathbb{F}_q , we shall refer to $m \in \mathbb{F}_q[T]$ as a G -fixed polynomial if for any $i \in G$, $m(T + i) = m(T)$. Moreover, such a G is a p -group. The c -Wieferich primes in $\mathbb{F}_q[T]$ of this type are called G -fixed c -Wieferich primes. For example, we considered \mathbb{F}_{3^2} with a primitive element t such that $f_{\min}^t(x) = x^2 + 2x + 2$ is irreducible over \mathbb{F}_3 . Using SAGE, we found that $P_0 = T^3 + (t + 1)T + 1$ is one of the c -Wieferich primes in $\mathbb{F}_{3^2}[T]$. Let $G_1 = \{0, 1, 2\}$ and $G_2 = \{0, t + 2, 2t + 1\}$ both subgroups of \mathbb{F}_{3^2} . It is easy to check that P_0 is invariant under translation by elements of G_2 but not G_1 , so P_0 is a G_2 -fixed c -Wieferich prime. If $G = \mathbb{F}_q$, then a G -fixed polynomial is also a fixed polynomial in $\mathbb{F}_q[T]$, (in this case, the two notions coincide).

Proposition 5.2.1. *Let $q > 2$ and G be a subgroup of \mathbb{F}_q . There are infinitely many G -fixed primes.*

Proof. Let $m \in \mathbb{F}_q[T]$, G be a subgroup of \mathbb{F}_q , $\text{stab}(m) = \{i \in \mathbb{F}_q : m(T + i) = m(T)\}$ and $\text{orb}(m) = \{m(T + i) : i \in \mathbb{F}_q\}$. Next we consider the map $\mathbb{F}_q \times \mathbb{F}_q[T] \rightarrow \mathbb{F}_q[T]$, defined by $(i, m(T)) \mapsto m(T + i)$. This is induced by the automorphism σ_i and $|\text{orb}(m)| = \frac{|\mathbb{F}_q|}{|\text{stab}(m)|}$. It is clear that if $|\text{orb}(m)| = 1$, then m is fixed. Let $\pi_{\mathbb{F}_q[T]}(n)$ be the number of degree n primes in $\mathbb{F}_q[T]$. If $\pi_{\mathbb{F}_q[T]}(n) \not\equiv 0 \pmod{q}$, then there is a prime P such that $1 \leq |\text{orb}(P)| < q$. This guarantees existence of a G -fixed prime P of degree n in $\mathbb{F}_q[T]$ for some G .

Let $q^w \parallel n$, by Gauss' Formula (see Theorem 1.2.9), we obtain

$$\pi_{\mathbb{F}_q[T]}(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}} = \frac{q^w}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d} - w} \equiv \frac{q^w}{n} \left(\pm q^{q^w - w} \mp q^{q^{w-1} - w} \right) \not\equiv 0 \pmod{q},$$

if and only if $w = 1$. We obtain G -fixed primes if $q \parallel n$, where q is an odd prime power. \square

Theorem 5.2.2. *Let G be a subgroup of \mathbb{F}_q and $f \in \mathbb{F}_q[T]$ be a G -fixed prime. Then f factors into almost Artin Schreier primes in some $\mathbb{F}_{q^s}[T]$.*

Proof. This proof has two parts, first we show that, f is G -fixed implies and p divides its degree. Secondly, f decomposes into almost Artin Schreier primes in some \mathbb{F}_q extension.

1. Assume f is G -fixed and its degree is not divisible by p , there are two cases to consider. Firstly, suppose f is G -fixed with $1 \leq \deg(f) < p$, and then show that f must be a constant polynomial. Since f is G -fixed, this implies there exists a non trivial subgroup G of order less than p that fixes f . This is impossible because $G \subseteq \mathbb{F}_q$ is a p -group, so G has order at least p , (take $|G| = p$). Since f is G -fixed, so is $f_1 = f - f(0)$, moreover $T \mid f_1$. Let $g = \prod_{j \in G} (T - j)$, then $G = \chi \mathbb{F}_p$ for some $0 \neq \chi \in G$. So $g = T^p - \beta T$ for some $\beta \in \mathbb{F}_q^*$. Since T is not G -fixed and divides f_1 , we must have $g \mid f_1$, which implies that $f_1 = 0$, since $\deg(f) < p$ and so f is a constant, which contradicts $p \nmid \deg(f)$. Secondly, suppose $\deg(f) > p$ and is not divisible by p . In this case, by the Fundamental Theorem of Arithmetic for $\mathbb{F}_q[T]$, f decomposes into a product of prime powers. We can divide its factors into G -fixed primes and non G -fixed prime factors. If f has a non G -fixed (prime) factor, then the p distinct prime elements in its G orbit, for some non trivial G are also prime factors, and so the total degree of the non fixed factors is always a multiple of p . It remains to check that the degree of the G -fixed (prime) factors is divisible by p . Take f to be a G -fixed prime of degree greater and coprime to p . By the argument in the first part, $f_1 = f - f(0)$ is also G -fixed and in addition divisible by a power of T . Since T is not G -fixed, we must have a power of $T^p - \beta T$ divides f_1 for some $\beta \in \mathbb{F}_q^*$ and some other G -fixed and non G -fixed factors. Since f_1 is G -fixed, its non G -fixed factors contribute a total degree which is a multiple of p . Similarly, we again consider the lower degree G -fixed prime factors of f_1 . Every time we do this, we reduce the degree of f by a multiple of p . Since f has a finite degree this process will eventually stop with G -fixed prime factors of degree $< p$, contradicting the first case. So the degree of f is a multiple of p .
2. Let $f \in \mathbb{F}_q[T]$ be a G -fixed prime of degree $\#G$. Since f is irreducible over \mathbb{F}_q , with α as one of its roots, we have $\mathbb{F}_{q^{\#G}} = \mathbb{F}_q(\alpha)$, the splitting field of f over \mathbb{F}_q . Since f is G -fixed, for any root $\alpha \in \mathbb{F}_{q^{\#G}}$ of f , $\alpha + i$ is also a root of f for any $i \in G$. Now,

$$g = \prod_{i \in G} (T - (\alpha + i)) \quad \text{divides} \quad h = \prod_{i \in \mathbb{F}_q} (T - (\alpha + i)) = T^q - T - (\alpha^q - \alpha).$$

To show that f decomposes into almost Artin Schreier primes in some $\mathbb{F}_{q^s}[T]$, it suffices to show that h splits into almost Artin Schreier primes in some $\mathbb{F}_{q^s}[T]$. We now show that this is indeed the case, i.e., h splits into almost Artin Schreier primes. The element $\alpha^q - \alpha \in \mathbb{F}_{q^{sq}}$ but is no longer primitive since

$$\mathcal{N}_{\mathbb{F}_{q^{sq}}/\mathbb{F}_{q^s}}(\alpha) = (-1)^q \prod_{j \in \mathbb{F}_q} (\alpha + j) = -\alpha^q + \alpha \in \mathbb{F}_{q^s}.$$

Since $s \geq 1$, and $\alpha \notin \mathbb{F}_{q^s}$, we have $\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha^q - \alpha) = \alpha^{q^s} - \alpha \neq 0$. It is clear by construction, every root of g is also a root of f and so g divides f , moreover $\deg(g) \leq \deg(f)$. In other words f factors into polynomials of the form $T^q - T - \gamma$ over \mathbb{F}_{q^s} . Since $\mathbb{F}_{q^{sq}}/\mathbb{F}_q$ is normal and by assumption $\mathbb{F}_{q^{sq}}$ is the splitting field of f over \mathbb{F}_q . Since $\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha^q - \alpha) \neq 0$, invoking Theorem 5.1.4, each g factors into almost Artin Schreier polynomials in $\mathbb{F}_{q^s}[T]$ and so does f . Moreover f splits completely in $\mathbb{F}_{q^{sq}}[T]$.

□

Corollary 5.2.3. *Every G -fixed c - Wieferich prime is a product of almost Artin Schreier primes.*

Lemma 5.2.4. *Let $n, d \in \mathbb{Z}_{\geq 1}$, $s, l \in \mathbb{Z}_{\geq 0}$ such that $n = sd + l$, $Q_d \in \mathbb{F}_q[T]$ be a degree d prime and F_i be expression given recursively as, $F_0 = 1$ and $F_i = (-1)^i + [i]F_{i-1}$, $i \in \mathbb{Z}_+$. Then*

$$F_{-1+n} \equiv \begin{cases} (-1)^{sd} F_{-1+l} \pmod{Q_d}, & n \not\equiv 0 \pmod{d} \\ (-1)^{(s-1)d} F_{-1+d} \pmod{Q_d}, & n \equiv 0 \pmod{d}. \end{cases}$$

Proof. We have $F_{sd} = (-1)^{sd} + [sd]F_{-1+sd} \equiv (-1)^{sd} \pmod{Q_d}$ and if $n_0 \in \mathbb{Z}_+$ is such that $n_0 = jd + i$, then $[n_0] = [jd]^q + [i] \equiv [i] \pmod{Q_d}$. Suppose $l \neq 0$, and label $t = l - 1$, then

$$\begin{aligned} F_{sd+t} &= (-1)^{sd+t} + [sd+t]F_{-1+sd+t} \\ &\equiv (-1)^{sd+t} + [sd+t]((-1)^{-1+sd+t} + [-1+sd+t]F_{-2+sd+t}) \\ &\quad \vdots \\ &\equiv (-1)^{sd+t} + [t] \left((-1)^{-1+sd+t} + [-1+t] \left(\cdots + [2] \left((-1)^{1+sd} + [1](-1)^{sd} \right) \cdots \right) \right) \\ &\equiv (-1)^{sd} \left((-1)^t + [t] \left((-1)^{-1+t} + [-1+t] \left(\cdots + [2] \left((-1)^1 + [1] \cdot 1 \right) \cdots \right) \right) \right) \\ &\quad \vdots \\ &\equiv (-1)^{sd} F_t \pmod{Q_d}. \end{aligned}$$

If $l = 0$, we repeat the procedure above and expand F_{-1+sd} to the first $d - 1$ terms. Since $F_{(s-1)d} = (-1)^{(s-1)d} \pmod{Q_d}$, we get $F_{-1+sd} \equiv (-1)^{(s-1)d} F_{-1+d} \pmod{Q_d}$. □

Theorem 5.2.5 (c - Wieferich Prime Existence Criterion). *There exists a pseudo-fixed c - Wieferich prime in $\mathbb{F}_q[T]$ of degree ps if and only if there exists a normal element $\alpha \in \mathbb{F}_{q^s}$ such that*

$$F_{-1+qs} \equiv 0 \pmod{T^q - T - \alpha}.$$

Proof. Given $F_{-1+qs} \in \mathbb{F}_q[T]$ and $F_{-1+qs} = (T^q - T - \alpha)g$, $g \in \mathbb{F}_{q^s}[T]$. For any $\sigma \in \text{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$,

$$F_{-1+qs} = \sigma F_{-1+qs} = \sigma(T^q - T - \alpha)\sigma(g) = (T^q - T - \sigma(\alpha))\sigma(g) \equiv 0 \pmod{T^q - T - \sigma(\alpha)}.$$

By Galois theory, $Q_{qs} = (T^q - T - \alpha_1) \cdots (T^q - T - \alpha_s)$, (where α_i are Galois conjugates of α in $\mathbb{F}_{q^s}/\mathbb{F}_q$) belongs to $\mathbb{F}_q[T]$. Since each $(T^q - T - \alpha_i)$ is a product of almost Artin Schreier primes, for any choice α, β and γ such that $T^p - \beta T - \gamma$ divides $T^q - T - \alpha$, we have that $Q_{ps} = (T^p - \beta_1 T - \gamma_1) \cdots (T^p - \beta_s T - \gamma_s)$, where $\beta_i = \sigma_i(\beta), \alpha_i = \sigma_i(\alpha)$ is by construction a prime in $\mathbb{F}_q[T]$. Now $Q_{qs} \in \mathbb{F}_q[T]$ has $\frac{q}{p}$ distinct such prime factors each of degree ps . For each such a Q_{ps} , the Chinese Remainder Theorem implies that $F_{-1+qs} \equiv 0 \pmod{Q_{ps}}$. By Lemma 5.2.4, $F_{-1+ps} \equiv 0 \pmod{Q_{ps}}$, so each Q_{ps} is a c - Wieferich prime of degree ps . □

Below is an algorithm for computing pseudo-fixed c - Wieferich primes in $\mathbb{F}_q[T]$.

Algorithm 4 Computing Carlitz - Wieferich primes IV.

Input: p, s , and \mathcal{B} , the list of normal elements of $\mathbb{F}_{q^s}/\mathbb{F}_q$.

Output: \mathcal{B} , list of Wieferich primes of degree ps .

1. $\mathcal{W}, W \leftarrow 1 // \mathcal{W}$ is the list of non conjugate normal elements of \mathbb{F}_{q^s} .
2. for $i = 1$ to size of \mathcal{W}

$$W \leftarrow (T^q - T - \mathcal{W}_i)W$$
3. $\mathcal{B} \leftarrow$ Prime factors of W as an element in $\mathbb{F}_q[T]$.

Return: \mathcal{B}

The Tables 5.1 and 5.2 below show products of the first few fixed c - Wieferich primes in $\mathbb{F}_{32}[T]$ and $\mathbb{F}_{52}[T]$ with their corresponding normal elements (used to compute them).

s	Normal elements in \mathbb{F}_{9^s}	Product of Wieferich primes
1	$\{t, 2t + 1\}$	$T^{18} + T^{10} + 2T^9 + T^2 + T + 2$
2	$\{2t^3 + 2t^2 + 1, t^3 + t^2\}$	$T^{18} + T^{10} + 2T^9 + T^2 + T + 2$
3	$\{2t^5 + 2t^3 + t^2 + 2t + 2, t^5 + t^3 + 2t^2 + t + 2\}$	$T^{18} + T^{10} + 2T^9 + T^2 + T + 2$
4	$\{2t^7 + 2t^6 + 2t^5 + t + 2, t^7 + t^6 + t^5 + 2t + 2\}$	$T^{18} + T^{10} + 2T^9 + T^2 + T + 2$

Table 5.1. Normal elements in subfields of $\overline{\mathbb{F}}_{32}$ and the product of Wieferich primes.

s	Normal elements in subfields of \mathbb{F}_{25^s}	Product of Wieferich primes
1	$\{4\}$	$T^{25} + 4T + 1$
2	$\{4\}$	$T^{25} + 4T + 1$
3	$\{4\}$	$T^{25} + 4T + 1$
4	$\{4\}$	$T^{25} + 4T + 1$

Table 5.2. Normal elements in subfields of $\overline{\mathbb{F}}_{52}$ and the product of Wieferich primes.

Lastly, we comment on the characterisation of c - Wieferich primes mimicking J. Silverman's approach. Let $m \in \mathbb{F}_q[T]$ be a monic, $m = \prod P^i$, where the product is over distinct primes $P \mid m$, we define the *powerful part* of m to be the product of prime powers $P^i \parallel m$ and $i \geq 2$.

Proposition 5.2.6. *Let $m \in \mathbb{F}_q[T]$. Suppose $\rho_{m-1}(1)$ is factored into $C_m D_m$, where D_m is the powerful part of $\rho_{m-1}(1)$. If P divides C_m , then P is a non c - Wieferich prime.*

Proof. This proof follows J. Silverman's idea [24]. Suppose $P \mid C_m$, a moment's reflection shows that $P \nmid m - 1$, other wise, we would have $\rho_{m-1}(1) = \rho_a(\rho_P(1)) = \rho_a(1) \equiv 0 \pmod{P}$ and $\rho_{m-1}(1) = \rho_P(\rho_a(1)) \equiv 0 \pmod{P^2}$, contradicting the supposition $P \mid m - 1$. Let E be the Carlitz order of 1 modulo P . $E \mid P - 1$, and so $\rho_E(1) = PM$, for some $M \in \mathbb{F}_q[T]$. By

assumption $P \mid C_m$, so $\rho_{m-1}(1) \equiv 0 \pmod{P}$, and

$$\rho_{m-1}(1) = \rho_{\frac{m-1}{E}}(\rho_E(1)) = \rho_{\frac{m-1}{E}}(PM) \equiv \frac{m-1}{E} \cdot PM \pmod{P^2}.$$

In addition, since C_m is squarefree, then $P^2 \nmid \rho_{m-1}(1)$, hence $P \nmid M$. Similarly,

$$\rho_{P-1}(1) = \rho_{\frac{P-1}{E}}(\rho_E(1)) = \rho_{\frac{P-1}{E}}(PM) \equiv \frac{P-1}{E} \cdot PM \pmod{P^2}.$$

and $P \nmid M$, $P^2 \nmid \frac{P-1}{E} \cdot PM$ and so $\rho_{P-1}(1) \not\equiv 0 \pmod{P^2}$. \square

Remark 5.2.7. A prime P is c -Wieferich if whenever there is an $m \in \mathbb{F}_q[T]$ such that P divides $\rho_{m-1}(1)$, we have P is a prime factor of the powerful part of $\rho_{m-1}(1)$. By Theorem 4.3.18, it is clear that there are only two non c -Wieferich primes in $\mathbb{F}_2[T]$.

We now reveal the infinitude of non c -Wieferich primes in $\mathbb{F}_q[T]$.

Theorem 5.2.8. Let $q > 2$, there are infinitely many non c -Wieferich primes in $\mathbb{F}_q[T]$.

Proof. To show infinitude of non c -Wieferich primes in $\mathbb{F}_q[T]$, Proposition 4.3.11 suggests it is enough to show infinitude of $n \in \mathbb{Z}_+$ for which there exists a prime Q of degree n such that $F_{-1+n} \not\equiv 0 \pmod{Q}$. We do this by showing that the degree of the product of primes in $\mathbb{F}_q[T]$ each of degree n is greater than $\deg(F_{-1+n})$. This implies that there is at least one prime that does not divide F_{-1+n} . Let $n = q^s$, then $\deg(F_{-1+q^s}) = q^{q^s-1} + \dots + q^2 + q$ and

$$\begin{aligned} q^s \pi_{\mathbb{F}_q[T]}(q^s) - \deg(F_{-1+q^s}) &= \left(\sum_{d|q^s} \mu(d) q^{\frac{q^s}{d}} \right) - (q^{q^s-1} + \dots + q^2 + q) \\ &= q^{q^s} - q^{q^s-1} - q^{q^s-1} - \left(\frac{q^{q^s-1} - q}{q-1} \right) \\ &> (q-3)q^{q^s-1} \geq 0. \end{aligned}$$

\square

Remark 5.2.9. This is an analogue of J. Silverman's result on classical non Wieferich primes, see [24]. It asserts that the abc-Conjecture implies infinitely many classical non Wieferich primes.

In summary, we gave evidence that some c -Wieferich primes in $\mathbb{F}_q[T]$ are pseudo-fixed and revealed infinitude of non c -Wieferich primes in $\mathbb{F}_q[T]$. In addition, we described an algorithm used to compute pseudo-fixed c -Wieferich primes as well as giving examples.

Conclusion

In this thesis, we reviewed the most recent and current research findings on the arithmetic theory and computational aspects of Carlitz (cyclotomic) polynomials. In chapter 2, we used the Carlitz module action ρ to construct $\rho_m(x)$ and $\Phi_m(x)$ as well as prove its elementary properties. In chapter 3, we proved Theorem 3.2.4, an analogue of a classical result in [16] due to C. Ji, W. Li and P. Moree. As a corollary, we obtained Theorem 3.2.3, the Carlitzian analogue of Suzuki's Theorem. In chapter 4, Theorem 4.2.10, we imitated D. Birkhoff and H. Vandiver's proof in [7] and proved an $\mathbb{F}_q[T]$ analogue of the Bang - Zsigmondy Theorem. In Theorem 4.1.10, we gave an upper bound for the number of Zsigmondy primes for the pair $\langle f, N \rangle$. The existence of Carlitzian analogues of non Zsigmondy factors, Fermat pseudo-primes and Wieferich primes in $\mathbb{F}_q[T]$ was discussed. We gave a computable criterion for c - Wieferich primes and used it to prove Theorem 4.3.18, i.e., infinitude of c - Wieferich primes in $\mathbb{F}_2[T]$. We do not know the answer for q , but have a heuristic argument for finitude of c - Wieferich primes in $\mathbb{F}_q[T]$, $q \neq 2$. In Theorem 5.2.8, we proved infinitude of non c - Wieferich primes in $\mathbb{F}_q[T]$. Lastly, in Appendix A, we describe algorithms for computing $\Phi_m(x)$.

What next? To answer this question we suggest possible directions in which this research could be extended. Firstly, the distribution of the coefficients of $\Phi_m(x)$ is still mysterious. We do not even know whether these coefficients are of any arithmetic importance. The question of how $\Phi_m(x)$ factors in towers of Galois fields would make an interesting research topic, and perhaps may have applications in faster polynomial factorisation over finite fields. Generalisation of the results on c - Wieferich primes, e.g., Questions 4.3.34 and 4.3.35 are also possible directions to which this research can be steered. There is a beautiful connection between c - Wieferich primes and Carlitz Fermat quotients. Perhaps, studying the general theory of Carlitz Fermat quotients would give us more insights about the distribution of c - Wieferich primes to different bases. *This is one of our current projects.* Lastly, the algorithms described in Appendix A may not be the best, perhaps algorithms that exploit the power of parallel computing, Fast Fourier Transforms or quantum technology may be better.

"If I have seen further, it is by standing on the shoulders of giants",

- Sir Isaac Newton.

Appendix A

A.1 Algorithms for computing $\rho_m(x)$ and $\Phi_m(x)$

A naive algorithm is usually the most obvious solution when one is asked a problem. It may not be a smart algorithm but will probably get the job done (... eventually!). Normally, naive algorithms may not be very time/space efficient, and what one really considers 'naive' depends on the speaker, the context, and the weather of the next day. It is often used to distinguish a very sophisticated solution (*that uses some kind of trick*) from the obvious implementation. For example, Algorithm 5 and Algorithm 7 are naive in the sense that, they are implemented directly from properties of $\rho_m(x)$ and its factors. They involve no special tricks, no wonder they become slow quickly as the degree of the polynomial increases.

Algorithm 5 utilises Lemma 2.2.1 to compute $\rho_m(\tau)$ as a list of coefficients. This is an endomorphism in $k\{\tau\}$ associated to m through the Carlitz module $\rho : A \rightarrow k\{\tau\}$. It requires its input as a non zero polynomial m of degree \mathcal{N} , creates a zero list \mathcal{B} of size $\mathcal{N} + 1$, to be replaced by a list of coefficients of the same size after the computation. Its complexity can easily be realised as $\mathcal{O}(\mathcal{N})$, from the \mathcal{N} steps in the for loop at line 2.1.

Algorithm 5 Computing $\rho_m(\tau)$ using Lemma 2.2.1.

Input: m - monic polynomial in A of degree \mathcal{N} , $\mathcal{B} = [0, \dots, 0]$ -zero list of size $\mathcal{N} + 1$

Output: $\mathcal{B} = [a_{m,0}, \dots, a_{m,\mathcal{N}}]$,

1. $a_{m,0} \leftarrow m$

2. for $i = 1$ to \mathcal{N}

$$a_{m,i} \leftarrow \frac{a_{m,i-1}^q - a_{m,i-1}}{T^{q^i} - T}$$

Return: $\mathcal{B} = [a_{m,0}, \dots, a_{m,\mathcal{N}}]$

A variant of Algorithm 5 that computes $\rho_m(x)$ as a polynomial in x can be implemented. This algorithm utilises the relationship between $\rho_m(\tau)$ and $\rho_m(x)$ through the Frobenius au-

tomorphism τ , i.e., $\rho_m(\tau) = \sum_{i=0}^n a_{m,i} \tau^i$, then $\rho_m(x) = \sum_{i=0}^n a_{m,i} x^{qi}$. So to compute $\rho_m(x)$, it suffices to compute the coefficients of $\rho_m(\tau)$. Both are advantageous as follows, $\rho_m(x)$ is better for representation and further calculations where as $\rho_m(\tau)$ has an added computational advantage as it involves lower degrees hence less storage space, i.e., \mathcal{N} instead of $q^{\mathcal{N}}$.

We now discuss the algorithms for computing $\Phi_m(x)$. These depend largely on the prime factorisation of m . The first algorithm, Algorithm 6, uses Proposition 2.2.2, where

$$\Phi_m(x) = \prod_{D|m} \rho_m(x)^{\mu(\frac{m}{D})} = \prod_{D|m} \rho_{\frac{m}{D}}(x)^{\mu(D)}. \quad (\text{A.1})$$

Algorithm 6 Computing $\Phi_m(x)$ using Proposition 2.2.2.

Input: m - monic polynomial in A

Output: $\Phi_m(x)$

1. $\mathcal{D} \leftarrow$ list of all monic divisors of m , $f \leftarrow 1$

2. for D in \mathcal{D}

$$f \leftarrow \rho_D(x)^{\mu(\frac{m}{D})} \cdot f // \mu - \text{THE MÖBIUS FUNCTION}$$

3. $\Phi_m(x) \leftarrow f$

Return $\Phi_m(x)$

We have as input a monic polynomial m , in step 1 we compute the list of monic divisors of m (and order them using any monomial ordering, e.g., lexicographic ordering). In step 2, we do a for loop on them, for each D we compute the corresponding Carlitz polynomial $\rho_D(x)$ using Algorithm 5, (of course constructing the polynomial $\rho_D(x)$), then raise it to the power of $\mu(\frac{m}{D})$. The end result is $\Phi_m(x)$. During the implementation in SAGE, the second formula in Equation (A.1) does not work well, although it is algebraically correct. This is because of the way the code for $\rho_m(x)$ is implemented, it only accepts elements of A , so any kind of division changes their type to elements of k , and so the algorithm does not work.

Algorithm 7 computes $\Phi_m(x)$ in x - form by using Proposition 2.2.4 (or Corollary 2.2.5) recursively. It requires its input as a non zero polynomial m of degree \mathcal{N} , uses a variant of Algorithm 5 to compute $\Phi_m(x)$. Its computation complexity is $\mathcal{O}(\mathcal{N}^2)$.

Theorem 2.2.6 asserts that, given $\Phi_{m_0}(x)$, where m_0 is the square-free factor of m ¹, we can calculate $\Phi_m(x)$ using the relation $\Phi_m(x) = \Phi_{m_0}(\rho_{\frac{m}{m_0}}(x))$. This means we can get a variant of Algorithm 7 by combining it with a variant of Algorithm 5 to get Algorithm 8. This is done at step 3 of Algorithm 8. It is advantageous over Algorithm 7 in two ways. Firstly, it is

¹is easy and quick to compute compared to the full m (because it contains only single distinct prime factors)

Algorithm 7 Computing $\Phi_m(x)$ by repeated polynomial division I.

Input: $m = P_1^{e_1} \cdots P_t^{e_t}$, where $e_i > 0$ for all $1 \leq i \leq t$ **Output:** $\Phi_m(x)$ 1. $a \leftarrow 1, \Phi_a(x) \leftarrow x$ 2. for $i = 1$ to t

$$\Phi_{aP_i}(x) \leftarrow \frac{\Phi_a(\rho_{P_i}(x))}{\Phi_a(x)}, a \leftarrow aP_i,$$

for $j = 2$ to e_i

$$\Phi_{aP_i}(x) \leftarrow \Phi_a(\rho_{P_i}(x)), a \leftarrow aP_i,$$

3. $\Phi_m(x) \leftarrow \Phi_a(x)$ **Return** $\Phi_m(x)$

much faster than Algorithm 7 since it is easier to compute $\rho_{\frac{m}{m_0}}(x)$ and it does away with the extra for loops which may involve multivariate polynomial division. Secondly, substitution takes less computation time as compared to polynomial division. As such, unless otherwise specified, if one does not want to use Fourier transforms, then this is the algorithm to go for. One considers only $\Phi_m(x)$ corresponding to a square free m . In all the algorithms so far, the brunt of the work takes place in the polynomial divisions on line 2.1. So it is much slower to perform line 2.1 using the traditional polynomial division. One obvious way to perform this division step faster is by way of the Fast Fourier Transform (FFT). There are other ways of computing $\rho_m(x)$ characterised by action of the Carlitz module ρ on the generators of A as an \mathbb{F}_q -algebra. They are fast but they require a lot of memory for storage. In summary, we described algorithms for computing $\rho_m(x)$ and $\Phi_m(x)$, see Algorithms 5, 6, 7 and 8.

Algorithm 8 Computing $\Phi_m(x)$ by repeated polynomial division II.

Input: $m = P_1^{e_1} \cdots P_t^{e_t}$, where $e_i > 0$ for all $1 \leq i \leq t$ **Output:** $\Phi_m(x)$ 1. $a \leftarrow 1, \Phi_a(x) \leftarrow x$ 2. for $i = 1$ to t

$$\Phi_{aP_i}(x) \leftarrow \frac{\Phi_a(\rho_{P_i}(x))}{\Phi_a(x)}, a \leftarrow aP_i,$$

// a -THE SQUARE-FREE PART OF m 3. $s \leftarrow \frac{m}{a}, \Phi_m(x) \leftarrow \Phi_a(\rho_s(x))$ **Return** $\Phi_m(x)$

Bibliography

- [1] ALFORD W. AND GRANVILLE A. AND POMERANCE C., *There are infinitely many Carmichael numbers*, *Annals Math.*, 139 (1994), pp. 703–722.
- [2] APOSTOL T., *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.
- [3] BAE S., *The arithmetic of Carlitz polynomials*, *J. Korean Math. Soc.*, 35 (1998), pp. 341–360.
- [4] BAMUNOBA A., *Cyclotomic Polynomials*, Master’s thesis, Stellenbosch University, 2011.
- [5] ———, *A note on Carlitz Wieferich primes*, (Submitted), (2014), p. .
- [6] ———, *On some properties of Carlitz cyclotomic polynomials*, *J. Number Theory*, 143 (2014), pp. 102 – 108.
- [7] BIRKHOFF D. AND VANDIVER H., *On the integral divisors of $a^n - b^n$* , *Ann. of Math.*, (1904), pp. 173–180.
- [8] CARLITZ L., *A class of polynomials*, *Trans. Amer. Math. Soc.*, 43 (1938), pp. 167–182.
- [9] DENIS L., *Le théorème de Fermat-Goss*, *Trans. Amer. Math. soc.*, 343 (1994), pp. 713–726.
- [10] DRINFELD V., *Elliptic Modules*, *Mathematics of the USSR-Sbornik*, 23 (2007), p. 561.
- [11] EFFINGER G. AND HAYES D., *Additive Number Theory of Polynomials Over a Finite Field*, USA, 1991.
- [12] GOSS D., *Basic Structures of Function Field Arithmetic*, Springer, 1996.
- [13] GRZYCZUK A. AND TROPAK B., *A numerical method for the determination of the cyclotomic polynomial coefficients*, *Computational number theory (Debrecen, 1989)*, (1991), pp. 15–19.
- [14] HSU C., *On Carmichael polynomials*, *J. Number Theory*, 71 (1998), pp. 257–274.
- [15] IRELAND K. AND ROSEN M., *A Classical Introduction to Modern Number Theory*, vol. 84, Springer, 1990.
- [16] JI C. AND LI W. AND MOREE P., *Values of coefficients of cyclotomic polynomials II*, *Discrete Math.*, 309 (2009), pp. 1720–1723.
- [17] LEHMER D., *Some properties of the cyclotomic polynomial*, *J. Math. Anal. Appl.*, 15 (1966), pp. 105–117.
- [18] LIDL R. AND NIEDERREITER H., *Introduction to Finite Fields and their Applications*, Cambridge University Press, Cambridge, 1986.
- [19] NATHANSON M., *Additive Number Theory, The Classical Bases*, Springer (1 Edition), 1996.
- [20] PRASOLOV V., *Polynomials*, Springer-Verlag Berlin Heidelberg, 2004.
- [21] RIBENBOIM P., *My numbers, my friends: Popular Lectures on Number Theory*, Springer, 2000.
- [22] ROSEN M., *Number Theory in Function Fields*, Springer-Verlag, Berlin, New York, 2002.
- [23] SALVADOR G., *Topics in the Theory of Algebraic Function Fields*, Birkhäuser, 2006.
- [24] SILVERMAN J., *Wieferich’s criterion and the abc - Conjecture*, *J. Number Theory*, 30 (1988), pp. 226–237.
- [25] STEIN W. ET AL., *SAGE Mathematical Software Version 5.3*. <http://www.sagemath.org>, 2012.
- [26] SUZUKI J., *On coefficients of cyclotomic polynomials*, *Proc. Jpn Acad., Ser. A, Math. Sci.*, 63 (1987), pp. 279–280.
- [27] ———, *On the generalized Wieferich criteria*, *Proc. Japan Acad., Ser. A*, 70 (1994), pp. 230–234.
- [28] THAKUR D., *Iwasawa Theory and Cyclotomic Function Fields*, in *Arithmetic Geometry (Tempe, AZ 1993)*, vol. 174 of *Contemp. Math.*, American Mathematical Soc., 1994, pp. 157–165.
- [29] ———, *Function Field Arithmetic*, World Scientific Publishing Co, Inc., 2004.
- [30] ———, *Fermat - Wilson congruences and zeta values*, Preprint in *J. of Number Theory*, (2013).
- [31] WADE L., *Certain Quantities Transcendental over $GF(p^n, x)$* , *Duke Math. J.*, 8 (1941), pp. 701–720.
- [32] WIEFERICH A., *Zum letzten Fermat’schen Theorem*, *J. Reine Angew. Math.*, 136 (1909), pp. 293–302.