SOME CRITERIA FOR PRIMITIVE POLYNOMIALS AND k-NORMAL POLYNOMIALS OVER FINITE FIELDS

THANED ONNOM

A Thesis Submitted to the Graduate School of Naresuan University
in Partial Fulfillment of the Requirements
for the Master of Science Degree in Mathematics
19 December 2017

Thesis entitled "Some criteria for primitive polynomials and k-normal polynomials over finite fields"

by Mr. Thaned Onnom

has been approved by the Graduate School as partial fulfillment of the requirements for the Master of Science Degree in Mathematics of Naresuan University.

Oral Defense Committee

Pattira Ruengsinsub ..... Chair

(Assistant Professor Pattira Ruengsinsub, Ph.D.)

Umarin Pintoptang ..... Advisor

(Assistant Professor Umarin Pintoptang, Ph.D.)

Manoj Siripitukdet ..... Internal Examiner

(Associate Professor Manoj Siripitukdet, Ph.D.)

Approved

.....

(Associate Professor Paisarn Muneesawang, Ph.D.)

Dean of the Graduate School

1 DEC 2017

ACKNOWLEDGEMENT

Firstly, I would like to express my sincerest gratitude to Assistant Professor Dr. Umarin Pintoptang, my thesis advisor, for her kind support and inspiration throughout the period of this thesis. Her guidance helped me in all the time of research including writing of this thesis. Moreover I would like to thank for her teaching and advice, not only the research but also the way of life. I wish to acknowledge Assistant Professor Dr. Pattira Ruengsinsub and Associate Professor Dr. Manoj Siripitukdet for their valuable suggestion, commentary and correction for this thesis.

Special thanks to all my teachers who taught me to come to this stage of learning.

Finally, I would like to thank my family for their support of studying in a master's degree and the last gratefully special thanks to my friends for their help and encouragement.

Thaned Onnom

Title	SOME CRITERIA FOR PRIMITIVE POLYNOMIALS AND k -NORMAL POLYNOMIALS OVER FINITE FIELDS
Author	Thaned Onnom
Advisor	Assistant Professor Umarin Pintoptang, Ph.D.
Academic Paper	Thesis M.S. in Mathematics, Naresuan University, 2017
Keywords	Finite field, Primitive polynomial , Normal polynomial, Primitive normal polynomial, q-Cycle mod n, k-Normal element, Trace function

ABSTRACT

For a finite field $\mathbb{F}_{q^n}$, it is well-known that $\mathbb{F}_{q^n}^*$ is a cyclic group. A monic irreducible $f(x) \in \mathbb{F}_q[x]$ of degree n is said to be a primitive polynomial if all its roots are primitive elements of $\mathbb{F}_{q^n}$. On the other hand, $\mathbb{F}_{q^n}$ can be viewed as a vector space over $\mathbb{F}_q$ of dimension n. A monic irreducible $f(x) \in \mathbb{F}_q[x]$ of degree n is a normal polynomial if all its roots form a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. There are many researchers investigate on these polynomials over $\mathbb{F}_q$. One aspect of research on these polynomials is to find criteria for such polynomials. In this thesis, we give some criteria for primitive polynomials and normal polynomials over finite fields by using q-cycles mod n and trace functions.

LIST OF CONTENTS

CHAPTER I

INTRODUCTION

In this chapter, we will give a brief overview on this thesis. In addition, we will explain why we are interested in primitive polynomials, normal polynomials and primitive normal polynomials over finite fields.

Let $\mathbb{F}_{q^n}$ be a finite field with $q = p^k$ elements where p is a prime number and k a positive integer. We know that $\mathbb{F}_{q^n}^* = \mathbb{F}_{q^n} \backslash \{0\}$ is a multiplicative cyclic group and a generator of this cyclic group is called a primitive element of $\mathbb{F}_{q^n}$. Let $f(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree n. $f(x)$ is said to be a primitive polynomial if it is the minimal polynomial of a primitive element. It is well-known that for any positive integer n there always exist primitive polynomials of degree n over $\mathbb{F}_q$ and all n roots of a primitive polynomial are primitive elements of $\mathbb{F}_{q^n}$. Hence a primitive polynomial of degree n over $\mathbb{F}_q$ is another way of finding primitive elements of $\mathbb{F}_{q^n}$. Primitive elements and primitive polynomials over finite fields have been studied for many years by many researchers [3], [4], [5], [6], [7], [8], [14], [16], [18], [22], and are widely used in cryptography system, coding theory and design theory. One aspect of primitive polynomial research is finding criteria for primitive polynomials over finite fields, see e.g. [17], [9] and [15]. Lidl and Niederreiter [17] gave a criterion based on the order of polynomial $f(x)$. It states that an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is primitive if and only if $f(x)$ is monic, $f(0) \neq 0$ and $ord(f) = q^n - 1$ where $ord(f)$ is the order of polynomial $f(x)$. Fitzgerald [9] gave a criterion depending on the number of nonzero terms of polynomial $g(x)$, which states that for irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n, $f(x)$ is primitive if and only if $g(x) = (x^{q^n-1} - 1)/(x-1)f(x)$ has exactly $(q-1)q^{n-1} - 1$ nonzero terms. In this thesis, we give a new criterion for primitive polynomials which are monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$. This criterion is based on concept of q-cycles mod n.

For a finite field $\mathbb{F}_{q^n}$, we can view $\mathbb{F}_{q^n}$ as a vector space over field $\mathbb{F}_q$ with dimension n. Let $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a basis of vector space $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then any $\beta \in \mathbb{F}_{q^n}$ can be represented uniquely as a linear combination

$$\beta = c_0\alpha_0 + c_1\alpha_1 + \cdots + c_{n-1}\alpha_{n-1},$$

where $c_i \in \mathbb{F}_q$, $0 \leqslant i \leqslant n-1$. Then the number of elements in $\mathbb{F}_{q^n}$ is $|\mathbb{F}_{q^n}| = q^n$. There are many types of bases for vector space $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such as polynomial basis, self-dual basis, normal basis, optimal normal basis. Now, we focus on normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ because normal bases are widely used in applications of finite fields, in areas such as coding theory, cryptography, signal processing, etc. A normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ where $\alpha \in \mathbb{F}_{q^n}$. We say α is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. It is well-known that for every prime power q and every integer n, the normal bases exist in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. A monic irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ is called a normal polynomial (or N-polynomial) if its root α is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. For an irreducible $f(x) \in \mathbb{F}_q[x]$ of degree n, all distinct roots of $f(x)$ are $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$. If $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are linearly independent, then $f(x)$ is a normal polynomial and $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Hence a normal polynomial of degree n over $\mathbb{F}_q$ is another way of describing a normal basis: for a given positive integer n and the ground field $\mathbb{F}_q$, construction of a normal polynomial in $\mathbb{F}_q[x]$ of degree n is equivalent to construction of a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. There are many researchers investigate on normal polynomials over $\mathbb{F}_q$. The work of Blake, I.F. et.al., [1] collects some of results about normal polynomials over finite fields. One aspect of research of normal polynomials (elements) is to find a criterion for normal polynomials (elements) over finite fields, see e.g. [1] and [12]. For finite field $\mathbb{F}_q$ where $q = p^k$ is a prime power, Blake, I.F. et.al., [1] gave a criterion depending on the coefficients of polynomial $f(x)$. Any irreducible polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$ of degree n where n is a power of p or n is a prime such that q is primitive modulo n, is normal polynomial over $\mathbb{F}_q$ if and only if the coefficient of x^{n-1} in $f(x)$ is

nonzero, that is, $a_{n-1} \neq 0$. In 1888, Hensel, K. [12] gave a criterion based on the greatest common divisor of the polynomial $x^n - 1$ and $\alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}$ in $\mathbb{F}_{q^n}[x]$. It states that $\alpha \in \mathbb{F}_{q^n}$ is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $gcd(x^n - 1, \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}) = 1$, which is the motivation for the definition of k-normal elements over $\mathbb{F}_q$. In 2013, k-normal elements over finite fields is defined and characterized by Huczynska, S. et.al., [13]. An element $\alpha \in \mathbb{F}_{q^n}$ is k-normal over $\mathbb{F}_q$ if the greatest common divisor of the polynomials $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ and $x^n - 1$ in $\mathbb{F}_{q^n}[x]$ has degree k. Thus an element α which is normal in the usual sense is 0-normal and Huczynska, S. et.al., gave a characterization of k-normal elements in terms of the rank of a Sylvester matrix. We call $f(x) \in \mathbb{F}_q[x]$ a monic irreducible polynomial of degree n is a k-normal polynomial if it is the minimal polynomial of a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this thesis, we show some properties and some criteria for k-normal elements (especially, $0, 1$-normal elements), which based on trace functions from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, and then we apply these criteria for k-normal polynomials over $\mathbb{F}_q$. In similarly way, $\alpha \in \mathbb{F}_{q^n}$ is called a primitive normal element if it is both primitive and normal. If α is a primitive normal element, then $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is called a primitive normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $f(x)$ be a monic irreducible polynomial of degree n over $\mathbb{F}_q$. $f(x)$ is called a primitive normal polynomial if its root α is a primitive normal elememt of $\mathbb{F}_{q^n}$.

This thesis is organized into five chapters. In Chapter I, we show the literature review of this research and how important of our research including the objectives of this thesis. Chapter II collects all of the preliminaries dealing with structure of finite fields, polynomial over fields and its roots, trace functions, primitive polynomials, normal polynomials, k-normal elements and q-cycles mod n. In Chapter III - IV, the main results about criteria for primitive polynomials and normal polynomials over finite fields are investigated, respectively. In Chapter V, we sumarize all of finding results.

CHAPTER II

PRELIMINARIES

In this chapter, we present definitions, notations, and some useful results that will be used through this thesis.

2.1 Structure of finite fields

This first section contains fundamental properties of finite fields.

Definition 2.1.1. ([20]) A *group* is a nonempty set G equipped with an operation $*$ that satisfies the following properties:

(1) $a * b \in G$ for all $a, b \in G$.

(2) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

(3) There is an element $e \in G$ (called the identity element) such that $a * e = a = e * a$ for every $a \in G$.

(4) For each $a \in G$, there is an element $d \in G$ (called the inverse of a) such that $a * d = e$ and $d * a = e$.

Definition 2.1.2. ([20]) A group G is said to be *abelian* if it satisfies

$$a * b = b * a \text{ for all } a, b \in G.$$

Definition 2.1.3. ([21]) A group G is said to be *finite* (or of finite order) if it has a finite number of elements. In this case, the number of elements in G is called the *order* of G and is denoted $|G|$. A group with infinitely many elements is said to have *infinite order*.

Definition 2.1.4. ([17]) A group G is said to be *cyclic* if there is an element $a \in G$ such that for any $b \in G$ there is some integer j with $b = a^j$. Such an element a is called a *generator* of the cyclic group, and we write $G = \langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.

Theorem 2.1.5. ([20]) Every subgroup of a cyclic group is itself cyclic.

Theorem 2.1.6. ([21]) Let $G = \langle a \rangle$ be a cyclic group of order n. For any integer k, a^k is a generator of G if and only if $gcd(k, n) = 1$.

Definition 2.1.7. ([20]) A *ring* is a nonempty set R equipped with two operations (usually written as addition and multiplication) that satisfy the following properties:

(1) $\langle R, + \rangle$ is an abelian group.

(2) $a \cdot b \in R$ for all $a, b \in R$.

(3) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$.

(4) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.

Definition 2.1.8. ([20]) Let R and S be rings. A function $f : R \longrightarrow S$ is said to be a *homomorphism* if

(1) $f(a + b) = f(a) + f(b)$ for all $a, b \in R$.

(2) $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in R$.

Definition 2.1.9. ([20]) A ring R is *isomorphic* to a ring S (in symbol, $R \cong S$) if there is a function $f : R \longrightarrow S$ such that

(1) f is injective.

(2) f is surjective.

(3) f is a homomorphism.

Definition 2.1.10. ([21]) Let $\mathbb{F}$ be a nonempty set with two binary operations, one is called the addition and denoted by $+$, and the other is called the multiplication and denoted by $\cdot$. $\mathbb{F}$ is called a *field* with respect to the addition and multiplication, if the following manipulation rules are fulfilled:

(1) $\langle \mathbb{F}, + \rangle$ is an abelian group.

(2) $\langle \mathbb{F}^*, \cdot \rangle$ is an abelian group, where $\mathbb{F}^* = \mathbb{F} \backslash \{0\}$ and 0 is the identity element of the group $\langle \mathbb{F}, + \rangle$.

(3) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbb{F}$.

From above definition, we say that $\langle \mathbb{F}, +, \cdot \rangle$ is a field. $\langle \mathbb{F}, + \rangle$ is called the additive group of $\mathbb{F}$ and $\langle \mathbb{F}^*, \cdot \rangle$ is called the multiplicative group of $\mathbb{F}$.

Definition 2.1.11. ([21]) Let $\mathbb{F}$ be any field. For any $a, b \in \mathbb{F}$, $a + b$ is called the *sum* of a and b, and $a \cdot b$ the *product* of a and b. For convenience, $a \cdot b$ is denoted by ab. The identity element of the group $\langle \mathbb{F}, + \rangle$ is denoted by 0 and is called the *zero* of the field $\mathbb{F}$. For any $a \in \mathbb{F}$, the inverse of a in the group $\langle \mathbb{F}, + \rangle$ is denoted by $-a$ and is called the *negative* of a in the field $\mathbb{F}$. The identity of $\langle \mathbb{F}^*, \cdot \rangle$ is denoted by e or $1_{\mathbb{F}}$ and is called the *identity* of $\mathbb{F}$. For any $a \in \mathbb{F}^*$, the inverse of a in the group $\langle \mathbb{F}^*, \cdot \rangle$ is denoted by a^{-1} and is called the *inverse* of a.

Definition 2.1.12. ([21]) Let $\mathbb{F}$ be any field. If the number of elements in $\mathbb{F}$ is infinite, $\mathbb{F}$ is called an *infinite field*. If the number of elements in $\mathbb{F}$ is finite, $\mathbb{F}$ is called a *finite field* or *Galois field*.

Definition 2.1.13. ([17]) Let $\mathbb{F}$ be a field. A subset K of $\mathbb{F}$ that is itself a field under the operations of $\mathbb{F}$ will be called a *subfield* of $\mathbb{F}$.

Definition 2.1.14. ([21]) Let $\mathbb{F}$ be a field and e be its identity. If there exists a positive integer m such that $me = 0$, then the smallest positive integer p satisfying $pe = 0$ is called the *characteristic* of $\mathbb{F}$ and $\mathbb{F}$ is called a *field of characteristic* p. If

there is no such positive integer m, then we say the characteristic of $\mathbb{F}$ is 0 or $\mathbb{F}$ is a *field of characteristic* 0.

Theorem 2.1.15. ([21]) Let $\mathbb{F}$ be any field. Then the characteristic of $\mathbb{F}$ is either 0 or a prime p.

Corollary 2.1.16. ([21]) If $\mathbb{F}$ is a finite field, then the characteristic of $\mathbb{F}$ is a prime p.

Theorem 2.1.17. ([21]) Let $\mathbb{F}$ be a field of characteristic p, and let a, b be any two elements of $\mathbb{F}$, and n be any nonnegative integer. Then

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}.$$

Theorem 2.1.18. ([21]) Let $\mathbb{F}$ be a finite field of characteristic p. Then the number of elements of $\mathbb{F}$ is a power of p.

For finite field with q elements, we shall denote this field by $\mathbb{F}_q$. By Theorem 2.1.18, we have $q = p^k$ where p is the prime characteristic of $\mathbb{F}_q$ and k is a positive integer.

Theorem 2.1.19. ([21]) Let $\mathbb{F}$ be a finite field which contains a subfield $\mathbb{F}_q$. Then the number of elements of $\mathbb{F}$ is a power of q.

Theorem 2.1.20. ([21]) Let $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$ be finite fields of q^m and q^n elements, respectively, where m and n are positive integers. $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n}$ if and only if m is a divisor of n.

Theorem 2.1.21. ([21]) Let $\mathbb{F}_q$ be a finite field. Then $\alpha^{q-1} = 1$ for all $a \in \mathbb{F}_q^*$.

Corollary 2.1.22. ([21]) Let $\mathbb{F}_q$ be a finite field and E be a field which contains $\mathbb{F}_q$ as a subfield. Then $\alpha^q = \alpha$ for all $\alpha \in \mathbb{F}_q$ and, moreover, for any $\alpha \in E$, $\alpha^q = \alpha$ implies $\alpha \in \mathbb{F}_q$.

Theorem 2.1.23. ([17]) For every finite field $\mathbb{F}_q$ the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic.

Definition 2.1.24. ([20]) Let $\mathbb{F}$ be a field. A *vector space* over $\mathbb{F}$ is an additive abelian group V equipped with a scalar multiplication such that for all $a, a_1, a_2 \in \mathbb{F}$ and $v, v_1, v_2 \in V$:

(1) $av \in V$.

(2) $a(v_1 + v_2) = av_1 + av_2$.

(3) $(a_1 + a_2)v = a_1v + a_2v$.

(4) $a_1(a_2v) = (a_1a_2)v$.

(5) $1_{\mathbb{F}}v = v$ where $1_{\mathbb{F}}$ is the identity of $\mathbb{F}$.

Definition 2.1.25. ([20]) If $\mathbb{F}$ and E are fields with $\mathbb{F} \subseteq E$, we say that E is an *extension field* of $\mathbb{F}$.

Remark 2.1.26. If E is an extension field of $\mathbb{F}$, then E is a vector space over $\mathbb{F}$, with addition of vectors being ordinary addition in E and scalar multiplication being ordinary multiplication in E.

Theorem 2.1.27. ([21]) Finite field $\mathbb{F}_{q^n}$ is a vector space over $\mathbb{F}_q$ and $dim_{\mathbb{F}_q}\mathbb{F}_{q^n} = n$.

2.2 Polynomials over fields and its roots

Definition 2.2.1. ([20]) Let $\mathbb{F}$ be any field. A *polynomial* with cofficients in $\mathbb{F}$ is an expression of the form

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

where integer $n \geqslant 0$, $a_i \in \mathbb{F}$ for all $i \in \{0, 1, \ldots, n\}$. The $a_i's$ are called the *coefficients* of the polynomial, and x is called an *indeterminate*.

Let

$$f(x) = \sum_{i=0}^{n} a_ix^i \text{ and } g(x) = \sum_{i=0}^{n} b_ix^i$$

be two polynomials of degree n. Then the *sum* of $f(x)$ and $g(x)$ is defined by

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)x^i.$$

Similarly, let

$$f(x) = \sum_{i=0}^{n} a_i x^i \text{ and } g(x) = \sum_{j=0}^{m} b_j x^j$$

be two polynomials of degree n and m, respectively. Then the *product* of $f(x)$ and $g(x)$ is defined by

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, c_k = \sum_{i+j=k} a_i b_j,$$

where $0 \leqslant i \leqslant n$ and $0 \leqslant j \leqslant m$.

It is well-known that the set of all polynomials in x over $\mathbb{F}$ denote by $\mathbb{F}[x]$ is a ring with respect to the above-defined addition and multiplication in $\mathbb{F}[x]$. $\mathbb{F}[x]$ is called the *polynomial ring over* $\mathbb{F}$. The zero of $\mathbb{F}$ is the zero of $\mathbb{F}[x]$ and the identity $1_{\mathbb{F}}$ of $\mathbb{F}$ is the identity of $\mathbb{F}[x]$.

Definition 2.2.2. ([20]) Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial in $\mathbb{F}[x]$ with $a_n \neq 0$. Then a_n is called the *leading coefficient* of $f(x)$. If $a_n = 1$, Then we say $f(x)$ is *monic*. The *degree* of $f(x)$ is the integer n. For convenience, we denote polynomial $f(x)$ by f and denote the degree of $f(x)$ by $deg(f)$.

Example 2.2.3. For a polynomial $f(x) = 2x^4 + 3x^2 + 5x + 1 \in \mathbb{R}[x]$, we have $2, 3, 5$ and 1 as cofficients of $f(x)$, the leading coefficient is 2 and degree of $f(x)$ is 4. For $g(x) = x^5 + 3x^4 + 1x^2 + 2x + 1 \in \mathbb{R}[x]$, we have $1, 3, 1, 2$ and 1 as cofficients of $g(x)$, the leading coefficient is 1, so $g(x)$ is monic and $deg(g)$ is 5. .

Theorem 2.2.4. ([17]) Let $f(x), g(x) \in \mathbb{F}[x]$. Then

$$deg(f + g) \leqslant max\{deg(f), deg(g)\},$$

$$deg(fg) = deg(f) + deg(g).$$

Theorem 2.2.5. ([21]) Let $\mathbb{F}$ be a field and x an indeterminate. Then $\mathbb{F}[x]$ is an integral domain.

Theorem 2.2.6. ([20])(Division Algorithm) Let $\mathbb{F}$ be a field and $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Then there exists unique pair of polynomials $q(x)$ and $r(x)$ such that

$$f(x) = g(x)q(x) + r(x)$$

and either $r(x) = 0$ or $deg\ (r) < deg\ (g)$.

Definition 2.2.7. ([20]) Let $\mathbb{F}$ be a field and $f(x), g(x) \in \mathbb{F}[x]$ with $f(x)$ is nonzero. We say that $f(x)$ *divides* $g(x)$ [or $f(x)$ is a *factor* of $g(x)$], and write $f(x)|g(x)$, if $g(x) = f(x)h(x)$ for some $h(x) \in \mathbb{F}[x]$.

Definition 2.2.8. ([20]) Let $\mathbb{F}$ be a field and $f(x), g(x) \in \mathbb{F}[x]$, not both zero. A monic polynomial $d(x) \in \mathbb{F}[x]$ is the *greatest common divisor* of $f(x)$ and $g(x)$ if and only if $d(x)$ satisfies these conditions:

(1) $d(x)|f(x)$ and $d(x)|g(x)$,

(2) for $c(x) \in \mathbb{F}[x]$, if $c(x)|f(x)$ and $c(x)|g(x)$, then $c(x)|d(x)$.

Definition 2.2.9. ([20]) Let $f(x), g(x) \in \mathbb{F}[x]$. Then the polynomials $f(x)$ and $g(x)$ are said to be *relatively prime* if the greatest common divisor is $1_{\mathbb{F}}$.

Theorem 2.2.10. ([20]) Let $f(x), g(x), h(x) \in \mathbb{F}[x]$. If $f(x)|g(x)h(x)$ and $f(x)$ and $g(x)$ are relatively prime, then $f(x)|h(x)$.

Definition 2.2.11. ([20]) A polynomial $p(x) \in \mathbb{F}[x]$ of positive degree is said to be *irreducible* over $\mathbb{F}$ (or irreducible in $\mathbb{F}[x]$, or prime in $\mathbb{F}[x]$) if $p(x) = b(x)c(x)$ with $b(x), c(x) \in \mathbb{F}[x]$ implies that either $b(x)$ or $c(x)$ is a constant polynomial. A polynomial in $\mathbb{F}[x]$ of positive degree that is not irreducible over $\mathbb{F}$ is called *reducible* over $\mathbb{F}$.

Theorem 2.2.12. [17] For every finite field $\mathbb{F}_q$ and every positive integer n there exists an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n.

Lemma 2.2.13. [17] If an irreducible polynomial $f(x)$ in $\mathbb{F}[x]$ divides a product

$$f_1(x) \cdot f_2(x) \cdots f_m(x)$$

of polynomials in $\mathbb{F}[x]$, then at least one of the factors $f_i(x)$ is divisible by $f(x)$.

Theorem 2.2.14. ([17]) (Unique Factorization) Any polynomial $f(x) \in \mathbb{F}[x]$ of positive degree can be written in the form

$$f(x) = a p_1^{e_1}(x) p_2^{e_2}(x) \cdots p_k^{e_k}(x),$$

where $a \in \mathbb{F}$ and $p_1(x), p_2(x), \ldots, p_k(x)$ are distinct monic irreducible polynomials in $\mathbb{F}[x]$, and $e_1, e_2, \ldots, e_k$ are positive integers. Moreover, this factorization is unique apart from the order in which the factor occur.

Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ be a polynomial of degree $n > 0$. Then

$$\mathbb{F}[x]/(f(x)) = \{\ \overline{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}\ \}.$$

Definition 2.2.15. ([20]) Let $\mathbb{F}$ be a field and $f(x)$ a nonconstant polynomial in $\mathbb{F}[x]$. Addition and multiplication in $\mathbb{F}[x]/(f(x))$ are defined by

$$\overline{g(x) + h(x)} = \overline{g(x)} + \overline{h(x)},$$

$$\overline{g(x)h(x)} = \overline{g(x)}\ \overline{h(x)}.$$

Theorem 2.2.16. ([20]) Let $f(x) \in \mathbb{F}[x]$ be a polynomial with degree $n > 0$. Then the set $\mathbb{F}[x]/(f(x))$ of congruence classes modulo $f(x)$ is a commutative ring with identity.

Definition 2.2.17. ([21]) Let $f(x)$ be a polynomial in $\mathbb{F}[x]$ with degree $n > 0$. Then the ring $\mathbb{F}[x]/(f(x))$ is called the *residue class ring* of the polynomial ring $\mathbb{F}[x]$ modulo the polynomial $f(x)$.

Theorem 2.2.18. ([17]) For $f(x) \in \mathbb{F}[x]$ with degree $n > 0$, the residue class ring $\mathbb{F}[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible over $\mathbb{F}$.

Remark 2.2.19.

(1) If $f(x)$ is an irreducible polynomial over $\mathbb{F}$, the field $\mathbb{F}[x]/(f(x))$ is called the *residue class field* of the polynomial ring $\mathbb{F}[x]$ modulo the irreducible polynomial $f(x)$.

(2) If $f(x) \in \mathbb{F}_q[x]$ is irreducible with degree $n > 0$, then the residue class field $\mathbb{F}_q[x]/(f(x))$ contains q^n elements.

Example 2.2.20. ([17]) Let $f(x) = x^2+x+1 \in \mathbb{Z}_2[x]$ be irreducible over $\mathbb{Z}_2$ where $\mathbb{Z}_2$ is the field of residue classes of integers modulo 2. Then $\mathbb{Z}_2[x]/(f(x))$ has the $p^n = 2^2$ elements $\overline{0}, \overline{1}, \overline{x}, \overline{x+1}$. The operation tables for this residue class ring are obtained by performing table for this operations with the polynomials determining the residue classes and by carrying out reduction mod $f(x)$ if necessary:

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$[x+1]$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

By inspecting these tables, or from the irreducibility of $f(x)$ over $\mathbb{F}_2$ and Theorem 2.2.18, it follows that $\mathbb{Z}_2[x]/(x^2+x+1)$ is a field.

Definition 2.2.21. ([17]) Let $f(x) \in K[x]$ be of positive degree n and $\mathbb{F}$ an extension field of subfield K. Then $f(x)$ is said to *split* in $\mathbb{F}$ if $f(x)$ can be written as a product of linear factors in $\mathbb{F}[x]$, that is, if there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$ such that

$$a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where a is the leading coefficient of $f(x)$. The field $\mathbb{F}$ is a *splitting field* of $f(x)$ over K if $f(x)$ splits in $\mathbb{F}$, $\mathbb{F} = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, where $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is smallest subfield of $\mathbb{F}$ containing both K and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

Lemma 2.2.22. ([17]) If $\mathbb{F}$ is a finite field with q elements and K is a subfield of $\mathbb{F}$, then the polynomial $x^q - x$ in $K[x]$ factors in $\mathbb{F}[x]$ as

$$x^q - x = \prod_{a \in \mathbb{F}} (x - a)$$

and $\mathbb{F}$ is a splitting field of $x^q - x$ over K.

Theorem 2.2.23. ([17]) For every prime p and every positive integer n there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.

Remark 2.2.24. From above Theorem, we get any two finite fields of the same order are isomorphic.

Theorem 2.2.18 and Theorem 2.2.23 play an important role in finding examples to support our main results that we would investigate in the next chapter. So we will remark the following fact.

(1) By Theorem 2.2.18, for an irreducible polynomial $f(x)$ in $\mathbb{F}_q[x]$ of degree n, we have $\mathbb{F}_q[x]/(f(x))$ is a residue class field of order q^n.

(2) By Theorem 2.2.23, a finite field $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(f(x))$ where $f(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_q$.

(3) For finite field with $q = p$ elements and by Throrem 2.2.23, $\mathbb{F}_p \cong \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the field of residue classes of integers modulo p. Computing with elements of $\mathbb{F}_p$ therefore means ordinary arithmetic of integers with reduction modulo p.

Definition 2.2.25. ([17]) An element $\alpha \in \mathbb{F}$ is a *root* (or a *zero*) of the polynomial $f(x) \in \mathbb{F}[x]$ if $f(\alpha) = 0$.

Definition 2.2.26. ([17]) Let $\alpha \in \mathbb{F}$ be a root of the polynomial $f(x) \in \mathbb{F}[x]$. If k is a positive integer such that $f(x)$ is divisible by $(x-\alpha)^k$, but not by $(x-\alpha)^{k+1}$, then k is called the *multiplicity* of α. If $k = 1$, then α is called a *simple root* (or a *simple zero*) of $f(x)$, and if $k \geqslant 2$, then α is called a *multiple root* (or a *multiple zero*) of $f(x)$.

Theorem 2.2.27. ([17]) The polynomial $f(x) \in \mathbb{F}[x]$ of degree 2 or 3 is irreducible in $\mathbb{F}[x]$ if and only if $f(x)$ has no root in $\mathbb{F}$.

Theorem 2.2.28. ([20]) Let $f(x) \in \mathbb{F}[x]$ and $\alpha \in \mathbb{F}$. Then remainder when $f(x)$ is divided by the polynomial $x - \alpha$ is $f(\alpha)$.

Theorem 2.2.29. ([20]) Let $f(x) \in \mathbb{F}[x]$ and $\alpha \in \mathbb{F}$. Then α is a root of the polynomial $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$ in $\mathbb{F}[x]$.

Theorem 2.2.30. ([20]) Let $\mathbb{F}$ be a field and $f(x)$ a nonzero polynomial of degree n in $\mathbb{F}[x]$. Then $f(x)$ has at most n roots in $\mathbb{F}$.

Theorem 2.2.31. ([17]) If $f(x)$ is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n, then $f(x)$ has a root α in $\mathbb{F}_{q^n}$. Furthermore all the roots of $f(x)$ are simple and are given by the n distinct elements $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ of $\mathbb{F}_{q^n}$.

Example 2.2.32. Let $f(x) = x^4 + x + 1$ be an irreducible polynomial over $\mathbb{F}_2$. We consider $\mathbb{F}_{2^4} \cong \mathbb{F}_2[x]/(x^4 + x + 1)$ the residue class field constructed by $x^4 + x + 1$. Let $\alpha = \overline{x}$ be the residue class of x modulo $x^4 + x + 1$. Note that $\alpha = \overline{x} \in \mathbb{F}_{2^4}$ is a root of $x^4 + x + 1$. By Theorem 2.2.31, we get that

$$\alpha, \alpha^2, \alpha^{2^2} = \alpha^4 = \alpha + 1, \alpha^{2^3} = \alpha^8 = \alpha^2 + 1$$

are all distinct roots in $\mathbb{F}_{2^4}$ of $x^4 + x + 1$.

Definition 2.2.33. ([21]) Let $\alpha \in \mathbb{F}_{q^n}$ and $f(x) = (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{n-1}})$. Then $f(x)$ is called the *characteristic polynomial* of $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The monic polynomial of least degree over $\mathbb{F}_q$ having α as a root is called the *minimal polynomial* of $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Theorem 2.2.34. ([21]) Let $\alpha \in \mathbb{F}_{q^n}$. Then

(1) The minimal polynomial of α over $\mathbb{F}_q$ exists and unique. Moreover, it is irreducible over $\mathbb{F}_q$.

(2) Let $m(x)$ be the minimal polynomial of α over $\mathbb{F}_q$. If $f(x) \in \mathbb{F}_q[x]$ and $f(\alpha) = 0$, then $m(x)|f(x)$.

(3) Let d be the least positive integer such that $\alpha^{q^d} = \alpha$. Then $d|n$, $d = deg(m(x))$, and $m(x) = (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{d-1}})$.

Definition 2.2.35. ([17]) Let n be a positive integer. The splitting field of $x^n - 1$ over a field K is called the nth *cyclotomic field* over K and denoted by $K^{(n)}$. The roots of $x^n - 1$ in $K^{(n)}$ are called the nth *roots of unity* over K and the set of all these roots is denoted by $E^{(n)}$.

Theorem 2.2.36. ([17]) Let n be a positive integer and K a field of characteristic p. If p does not divide n, then $E^{(n)}$ is a cyclic group of order n with respect to multiplication in $K^{(n)}$.

Definition 2.2.37. ([17]) Let K be a field of characteristic p and n a positive integer not divisible by p. Then a generator of the cyclic group $E^{(n)}$ is called a *primitive* nth *root of unity* over K.

Example 2.2.38. Let $x^2 + x + 1$ be an irreducible polynomial over $\mathbb{F}_2$. Then $\mathbb{F}_2[x]/(x^2 + x + 1)$ is a finite field constructed by $x^2 + x + 1$. Let $\alpha = \overline{x}$ be the

residue class of x modulo x^2+x+1. Consider $x^3-1=(x-1)(x^2+x+1)$ over a field $K=\mathbb{F}_2$. Since $1,\alpha,\alpha+1\in\mathbb{F}_{2^2}\cong\mathbb{F}_2[x]/(x^2+x+1)$ are all roots of x^3-1. By Definition 2.2.21 and 2.2.35, we see that

$$K^{(3)}=\mathbb{F}_2^{(3)}=\mathbb{F}_2(1,\alpha,\alpha+1)=\mathbb{F}_2(\alpha,\alpha+1)$$

is the splitting field of x^3-1 over field $K=\mathbb{F}_2$. Since $1,\alpha,\alpha+1\in\mathbb{F}_{2^2}\cong\mathbb{F}_2[x]/(x^2+x+1)$ are all roots of x^3-1 in $K^{(3)}$, we have

$$E^{(3)}=\{1,\alpha,\alpha+1\}\subseteq K^{(3)}.$$

Since $K=\mathbb{F}_2$ is a field of characteristic $p=2$ and $n=3$ a positive integer not divisible by $p=2$, we have $E^{(3)}$ is cyclic with $\alpha=\overline{x}$ is a generator of this cyclic group. Therefore $\alpha=\overline{x}$ is a primitive 3th root of unity over $\mathbb{F}_2$.

2.3 Trace functions

Definition 2.3.1. ([17]) Let $\alpha\in\mathbb{F}_{q^n}$ be a finite field with q^n elements. Then $\alpha,\alpha^q,\ldots,\alpha^{q^{n-1}}$ are the *conjugates* of α over $\mathbb{F}_q$.

Definition 2.3.2. ([17]) Let $K=\mathbb{F}_q$ and $F=\mathbb{F}_{q^n}$. For $\alpha\in F$, we define the *trace* of α over K as $Tr_{F/K}(\alpha)=\alpha+\alpha^q+\cdots+\alpha^{q^{n-1}}$.

That is, $Tr_{F/K}(\alpha)$ is the sum of the conjugates of α.

Example 2.3.3. Let $K=\mathbb{F}_2$ and $F=\mathbb{F}_{2^3}$. We consider $\mathbb{F}_{2^3}$ as the finite field $\mathbb{F}_2[x]/(x^3+x^2+1)$ constructed by an irreducible polynomial x^3+x^2+1 over $\mathbb{F}_2$ and let $\alpha=\overline{x}$ be the residue class of x modulo x^3+x^2+1. Then

$$\begin{aligned}
Tr_{F/K}(1)&=1+1^2+1^{2^2}=1+1+1=1.\\
Tr_{F/K}(\alpha)&=\alpha+\alpha^2+\alpha^{2^2}=\alpha+\alpha^2+\alpha^2+\alpha=0.\\
Tr_{F/K}(\alpha^2)&=\alpha^2+(\alpha^2)^2+(\alpha^2)^{2^2}=\alpha^2+\alpha^4+\alpha\\
&=\alpha^2+\alpha^2+\alpha+\alpha=0.
\end{aligned}$$

Theorem 2.3.4. ([17]) Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^n}$. The trace function satisfies the following properties.

(1) $Tr_{F/K}(\alpha) \in K$ for all $\alpha \in F$.

(2) $Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$ for all $\alpha, \beta \in F$.

(3) $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$ for all $\alpha \in F, c \in K$.

(4) $Tr_{F/K}(c) = nc$ for all $c \in K$.

(5) $Tr_{F/K}(\alpha^q) = \alpha$ for all $\alpha \in F$.

2.4 Primitive polynomials

In [17], Lidl and Niederreiter concluded the definitions and properties of primitive polynomials over finite fields. Recall that for every finite field $\mathbb{F}_q$ the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic.

Definition 2.4.1. ([17]) A generator of the cyclic group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

Definition 2.4.2. ([17]) A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $n \geqslant 1$ is called a *primitive polynomial* over $\mathbb{F}_q$ if it is the minimal polynomial over $\mathbb{F}_q$ of a primitive element of $\mathbb{F}_{q^n}$.

A primitive polynomial over $\mathbb{F}_q$ of degree n may be described as a monic irreducible polynomial over $\mathbb{F}_q$ and has a root $\alpha \in \mathbb{F}_{q^n}$ that generates the multiplicative group of $\mathbb{F}_{q^n}$.

Example 2.4.3. We view $\mathbb{F}_{3^3} \cong \mathbb{F}_3[x]/(x^3 + 2x + 1)$ the finite field constructed by an irreducible polynomial $x^3 + 2x + 1$ over $\mathbb{F}_3$. Let $\alpha = \overline{x}$ be the residue class of x modulo $x^3 + 2x + 1$. Then α is a root of $f(x) = x^3 + 2x + 1$. By Theorem 2.2.31,

$\alpha, \alpha^3 = \alpha + 2, \alpha^{3^2} = \alpha^2 + 1$ are all distinct roots in $\mathbb{F}_{3^3}$ of $f(x)$. We can show that α is a primitive element of cyclic group $\mathbb{F}_{3^3}^*$. Thus $f(x) = x^3 + 2x + 1$ is a primitive polynomial over $\mathbb{F}_3$.

Next we give the definition of the order of a polynomial $f(x)$, which will be used to characterize primitive polynomials over finite fields.

Definition 2.4.4. ([17]) Let $f(x) \in \mathbb{F}_q[x]$ be a nonzero polynomial. If $f(0) \neq 0$, then the least positive integer e for which $f(x)$ divides $x^e - 1$ is called the *order of* $f(x)$ and denoted by $ord(f) := ord(f(x))$. If $f(0) = 0$, then $f(x) = x^h g(x)$, where $h \in \mathbb{N}$ and $g(x) \in \mathbb{F}_q[x]$ with $g(0) \neq 0$ are uniquely determined; $ord(f)$ is then defined to be $ord(g)$.

Theorem 2.4.5. ([17]) If $f(x) \in \mathbb{F}_q[x]$ is an irreducible polynomial over $\mathbb{F}_q$ of degree n, then $ord(f)$ divides $q^n - 1$.

Theorem 2.4.6. ([17]) Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n. Then $ord(f)$ is equal to the order of any root of $f(x)$ in the multiplicative group $\mathbb{F}_{q^n}^*$.

The order of an irreducible polynomial $f(x)$ can be used to characterize primitive polynomials as follows.

Theorem 2.4.7. ([17]) A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is a primitive polynomial over $\mathbb{F}_q$ if and only if $f(x)$ is monic, $f(0) \neq 0$, and $ord(f) = q^n - 1$.

Theorem 2.4.8. ([21]) For any positive integer n, there exist primitive polynomials of degree n over $\mathbb{F}_q$. Moreover, all n roots of a primitive polynomial of degree n over $\mathbb{F}_q$ are primitive elements of $\mathbb{F}_{q^n}$.

Theorem 2.4.9. ([21]) Let $2^n - 1$ be a prime and $f(x)$ an irreducible polynomial of degree n over $\mathbb{F}_2$. Then $f(x)$ is a primitive polynomial of degree n over $\mathbb{F}_2$.

2.5 Normal polynomials

As we known that $\mathbb{F}_{q^n}$ is a vector space over finite field $\mathbb{F}_q$ with dimension n. Now we summarize results of normal polynomials over finite fields.

Definition 2.5.1. ([21]) A *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ where $\alpha \in \mathbb{F}_{q^n}$. We say that α is a *normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, or α *generates* the normal basis $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$.

Example 2.5.2. Consider $\mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x^2 + 1)$ the finite field arise from an irreducible polynomial $x^3 + x^2 + 1$ over $\mathbb{F}_2$. Note that $\mathbb{F}_{2^3}$ is a vector space over $\mathbb{F}_2$ with dimension 3. Let $\alpha = \overline{x}$ be the residue class of x modulo $x^3 + x^2 + 1$. Then $\alpha, \alpha^2, \alpha^3 = \alpha^2 + 1, \alpha^4 = \alpha^2 + \alpha + 1, \alpha^5 = \alpha + 1, \alpha^6 = \alpha^2 + \alpha, \alpha^7 = 1$. Next we show that $\{\alpha, \alpha^2, \alpha^{2^2} = \alpha^4 = \alpha^2 + \alpha + 1\}$ is linearly independent over $\mathbb{F}_2$. Let $a, b, c \in \mathbb{F}_2$ be such that

$$
\begin{aligned}
&a\alpha + b\alpha^2 + c(\alpha^4) = 0,\\
&a\alpha + b\alpha^2 + c(\alpha^2 + \alpha + 1) = 0,\\
&a\alpha + b\alpha^2 + c\alpha^2 + c\alpha + c = 0,\\
&(b + c)\alpha^2 + (a + c)\alpha + c = 0,\\
&a = b = c = 0.
\end{aligned}
$$

We have that $\{\alpha, \alpha^2, \alpha^{2^2} = \alpha^4 = \alpha^2 + \alpha + 1\}$ is a normal basis of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$ and α is a normal element of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$.

The result in [21] guarantees that for a prime power $q = p^k$ and a positive integer n, there exists a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The following results are useful criteria for normal elements of $\mathbb{F}_{q^n}$.

Theorem 2.5.3. ([12]) Let $\alpha \in \mathbb{F}_{q^n}$. Then $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if the polynomials $x^n - 1$ and $\alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ in $\mathbb{F}_{q^n}[x]$ are relatively prime.

Theorem 2.5.4. ([21]) Let α be an element of $\mathbb{F}_{q^n}$ and assume that $n = p^e$ is a power of the characteristic p of $\mathbb{F}_{q^n}$. Then $\alpha \in \mathbb{F}_{q^n}$ is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$.

Theorem 2.5.5. ([21]) Let q be a power of a prime p, n be a prime different from p, α be an element of $\mathbb{F}_{q^n}$ not belonging to $\mathbb{F}_q$. Suppose q is a primitive element modulo n. Then α is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$.

Definition 2.5.6. ([1]) A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $n \geqslant 1$ is called a *normal polynomial* over $\mathbb{F}_q$ if it is the minimal polynomial over $\mathbb{F}_q$ of a normal element of $\mathbb{F}_{q^n}$.

A normal polynomial over $\mathbb{F}_q$ of degree n may be described as a monic irreducible polynomial over $\mathbb{F}_q$ and has a root $\alpha \in \mathbb{F}_{q^n}$ that generates the normal basis of $\mathbb{F}_{q^n}$.

Example 2.5.7. Let $f(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$ be irreducible over $\mathbb{F}_2$. Consider $\alpha = \overline{x} \in \mathbb{F}_{2^4} \cong \mathbb{F}_2[x]/(x^4 + x^3 + 1)$ the finite field arise from $x^4 + x^3 + 1$. Recall that $\mathbb{F}_{2^4}$ is a vector space over $\mathbb{F}_2$ with dimension 4. We see that α is a root of $f(x)$. By Theorem 2.2.31, $\alpha, \alpha^2, \alpha^{2^2} = \alpha^3 + 1, \alpha^{2^3} = \alpha^3 + \alpha^2 + \alpha$ are all distinct roots in $\mathbb{F}_{2^4}$ of $f(x)$. Next we show that $\{\alpha, \alpha^2, \alpha^{2^2} = \alpha^3 + 1, \alpha^{2^3} = \alpha^3 + \alpha^2 + \alpha\}$ is linearly independent over $\mathbb{F}_2$. Let $a, b, c, d \in \mathbb{F}_2$ be such that

$$a\alpha + b\alpha^2 + c(\alpha^3 + 1) + d(\alpha^3 + \alpha^2 + \alpha) = 0,$$

$$a\alpha + b\alpha^2 + c\alpha^3 + c + d\alpha^3 + d\alpha^2 + d\alpha = 0,$$

$$(c + d)\alpha^3 + (b + d)\alpha^2 + (a + d)\alpha + c = 0,$$

$$a = b = c = d = 0.$$

Thus $\{\alpha, \alpha^2, \alpha^{2^2} = \alpha^3 + 1, \alpha^{2^3} = \alpha^3 + \alpha^2 + \alpha\}$ is linearly independent over $\mathbb{F}_2$. We see that α generates this normal basis and α is a root of $f(x)$. Therefore $f(x) = x^4 + x^3 + 1$ is a normal polynomial over $\mathbb{F}_2$.

For some special n and polynomial $f(x)$, the coefficient a_1 of $f(x)$ can be used to determine when $f(x)$ is normal.

Theorem 2.5.8. ([1]) Let q be a power of a prime p and $n = p^e$. Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ be an irreducible polynomial over $\mathbb{F}_q$. Then $f(x)$ is a normal polynomial if and only if $a_1 \neq 0$.

Theorem 2.5.9. ([1]) Let $f(x) = x^2 + a_1x + a_2$ be an irreducible quadratic polynomial over $\mathbb{F}_q$. Then $f(x)$ is a normal polynomial if and only if $a_1 \neq 0$.

Theorem 2.5.10. ([1]) Let q be a power of a prime p and r be a prime different from p. Suppose that q is a primitive element modulo r. Then an irreducible polynomial $f(x) = x^r + a_1x^{r-1} + \cdots + a_r$ is a normal polynomial over $\mathbb{F}_q$ if and only if $a_1 \neq 0$.

Next we will give definition of primitive normal polynomials over finite fields.

Definition 2.5.11. ([2]) An element $\alpha \in \mathbb{F}_{q^n}$ is called a *primitive normal element* if it is both primitive and normal. In this case, $\{\alpha_0, \alpha_1, \ldots, \alpha_n\}$ where $\alpha_i = \alpha^{q^i}$, $0 \leqslant i \leqslant n-1$ is called a *primitive normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Definition 2.5.12. ([2]) A monic polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *primitive normal polynomial* if it is the minimal polynomial of a primitive normal element.

A primitive normal polynomial over $\mathbb{F}_q$ of degree n may be described as a monic irreducible polynomial over $\mathbb{F}_q$ and has a root $\alpha \in \mathbb{F}_{q^n}$ that α is a primitive normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Theorem 2.5.13. ([2]) For a prime power $q = p^k$ and a positive integer n, there exists a primitive normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

2.6 k-Normal elements

Following [12], for $\alpha \in \mathbb{F}_{q^n}$ is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $x^n - 1$ and $\alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ in $\mathbb{F}_{q^n}[x]$ are relatively prime, that is, the degree of their greatest common divisor is 0. In 2013, Huczynska S. et.al., defined and characterized k-normal elements over finite fields.

Definition 2.6.1. ([13]) Let q be a prime power and n a positive integer. $\alpha \in \mathbb{F}_{q^n}$ is a *k-normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if the greatest common divisor of $x^n - 1$ and $g_\alpha(x) := \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ over $\mathbb{F}_{q^n}$ has degree k. In case $k = 0$, a 0-normal element is a normal element in usual sense.

Remark 2.6.2. For $\alpha \in \mathbb{F}_{q^n}$, $g_\alpha(x)$ has degree $n-1$. Then $gcd(x^n - 1, g_\alpha(x))$ has degree less than n and so α can be only one of k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for some $k \in \{0, 1, \ldots, n-1\}$.

Definition 2.6.3. ([13]) A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $n \geqslant 1$ is called a *k-normal polynomial* over $\mathbb{F}_q$ if it is the minimal polynomial over $\mathbb{F}_q$ of a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

A k-normal polynomial over $\mathbb{F}_q$ of degree n may be described as a monic irreducible polynomial over $\mathbb{F}_q$ and has a root $\alpha \in \mathbb{F}_{q^n}$ which is a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Theorem 2.6.4. ([13]) Let $\alpha \in \mathbb{F}_{q^n}$. If α is a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then any conjugate of α is a k-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, that is, $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are also k-normal of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Example 2.6.5. We consider $\mathbb{F}_2[x]/(x^3 + x + 1)$ the finite field constructed by an irreducible polynomial $x^3 + x + 1$ over $\mathbb{F}_2$. Let $\alpha = \overline{x} \in \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1)$ be the residue class of x modulo $x^3 + x + 1$.

By the division algorithm, we see that

$$\begin{aligned} x^3 - 1 &= (\alpha^6 x + 1)(\alpha x^2 + \alpha^2 x + \alpha^4) + (\alpha^5 + \alpha^5 x) \\ \alpha x^2 + \alpha^2 x + \alpha^4 &= (\alpha^3 x + \alpha^6)(\alpha^5 + \alpha^5 x) + 0. \end{aligned}$$

Thus

$$gcd(x^3 - 1, \alpha x^2 + \alpha^2 x + \alpha^4) = \alpha^5 + \alpha^5 x,$$

and so

$$deg[gcd(x^3 - 1, \alpha x^2 + \alpha^2 x + \alpha^4)] = 1.$$

From the definition of k-normal element, we have α is a 1-normal element of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$. Moreover, $\alpha, \alpha^2, \alpha^{2^2}$ are also 1-normal elements of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$.
Similarly, we consider $\alpha^3 = \alpha + 1 \in \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1)$ where $\alpha = \overline{x}$ is the residue class of x modulo $x^3 + x + 1$. By the division algorithm, we have that

$$\begin{aligned} &x^3 - 1 = ((\alpha+1)^6 x + 1)((\alpha+1)x^2 + (\alpha+1)^2 x + (\alpha+1)^4) + (x + (\alpha+1)^6), \\ &(\alpha+1)x^2 + (\alpha+1)^2 x + (\alpha+1)^4 = ((\alpha+1)x + (\alpha+1)^3)(x + (\alpha+1)^6) + (\alpha+1)^5, \\ &x + (\alpha+1)^6 = ((\alpha+1)^2 + (\alpha+1))(\alpha+1)^5 + 0. \end{aligned}$$

Thus

$$gcd(x^3 - 1, (\alpha+1)x^2 + (\alpha+1)^2 x + (\alpha+1)^4) = (\alpha+1)^5 = \alpha,$$

and so

$$deg[gcd(x^3 - 1, (\alpha+1)x^2 + (\alpha+1)^2 x + (\alpha+1)^4)] = 0.$$

From the definition of k-normal element, we get that α is a 0-normal element of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$. Moreover, $\alpha+1, (\alpha+1)^2 = \alpha^2+1, (\alpha+1)^{2^2} = \alpha^2+\alpha+1$ are 0-normal elements of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$.

Example 2.6.6. Consider $\mathbb{F}_{2^2} \cong \mathbb{F}_2[x]/(x^2 + x + 1)$ the finite field arise from an irreducible polynomial $x^2 + x + 1$ over $\mathbb{F}_2$. Let $\alpha = \overline{x}$ be the residue class of x modulo $x^2 + x + 1$.

By the division algorithm, we get that

$$\begin{aligned} x^2-1 &= (\alpha^2 x+1)(\alpha x+\alpha^2)+(\alpha^2+1), \\ \alpha x+\alpha^2 &= (x+\alpha)(\alpha^2+1)+0. \end{aligned}$$

Thus $gcd(x^2-1, \alpha x+\alpha^2) = \alpha^2+1$, so $deg[gcd(x^2-1, \alpha x+\alpha^2)] = 0$. We have α is a 0-normal element of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$. Moreover, $\alpha, \alpha^2 = \alpha+1$ are 0-normal elements of $\mathbb{F}_{2^2}$ over $\mathbb{F}_2$. More precisely, α is a normal element of $\mathbb{F}_{2^2}$ over $\mathbb{F}_2$ and we see that α generates the normal basis $\{\alpha, \alpha^2 = \alpha+1\}$ of $\mathbb{F}_{2^2}$ over $\mathbb{F}_2$.

Remark 2.6.7. From Exmaple 2.6.6, we see that any nonzero element in $\mathbb{F}_{2^2}$ is 0-normal element of $\mathbb{F}_{2^2}$ over $\mathbb{F}_2$.

2.7 q-Cycles mod n

Now we will recall definitions and important results of q-cycles mod n.

Definition 2.7.1. ([21]) Let $\mathbb{F}_q$ denote a finite field of q elements and let $n \in \mathbb{N}$ be such that $gcd(q, n) = 1$. Suppose that $a_0, a_1, a_2, \ldots, a_{l-1}$ are l distinct numbers chosen from $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$. If

$$\begin{aligned} a_i q &\equiv a_{i+1} \pmod{n},\ i = 0, 1, 2, \ldots, l-2, \text{ and} \\ a_0 q^l &\equiv a_{l-1} q \equiv a_0 \pmod{n}, \end{aligned}$$

then we say $(a_0, a_1, a_2, ..., a_{l-1})$ forms a *q-cycle mod n* with leading element a_0, denoted by $q(a_0)$-cycle mod n, and call l the *length* of the q-cycle mod n.

The notion of q-cycles mod n was introduced by Wan in his book [21]. From above definition, we start with element $a_0 \in \mathbb{Z}_n$ and elements $a_1, a_2, \ldots, a_{l-1} \in \mathbb{Z}_n$ can get by $a_0 q \equiv a_1, a_0 q^2 \equiv a_2, \ldots, a_0 q^{l-1} \equiv a_{l-1}, a_0 q^l \equiv a_0$ and so $(a_0, a_1, a_2, ..., a_{l-1})$ is a q-cycle mod n of length l. Remark that $(a_0, a_1, a_2, ..., a_{l-1})$, $(a_1, a_2, a_3, ..., a_{l-1}, a_0)$, $\ldots, (a_{l-1}, a_0, a_1, ..., a_{l-2})$ are the same q-cycles mod n.

Theorem 2.7.2. ([21]) Let $\mathbb{F}_q$ be a finite field with q elements and n be a positive integer with $gcd(q,n) = 1$. Assume that α is a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exists a primitive nth root of unity in $\mathbb{F}_{q^m}$). If $(a_0, a_1, a_2, \ldots, a_{l-1})$ is a q-cycle mod n, then

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a monic irreducible factor of $x^n - 1$ in $\mathbb{F}_q[x]$. Conversely, if $f(x)$ is a monic irreducible factor of $x^n - 1$ in $\mathbb{F}_q[x]$, then all roots of $f(x)$ are power of α whose exponents form a q-cycle mod n.

Corollary 2.7.3. ([21]) The number of distinct monic irreducible factors of $x^n - 1$ in $\mathbb{F}_q[x]$ is equal to the number of q-cycles mod n formed by n numbers $0, 1, \ldots, n-1$.

Remark 2.7.4. If $(a_0, a_1, a_2, \ldots, a_{l-1})$ is a q-cycle mod n of length l, then the correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

has degree l.

Proposition 2.7.5. ([19]) Let $(a_0, a_1, a_2, \ldots, a_{l-1})$ be a q-cycle mod n of length l, and $g(x) = x^{a_0} + x^{a_1} + \cdots + x^{a_{l-1}}$. If the number of q-cycles mod n is equal to q, and if $gcd(x^n - 1, g(x) - c) \neq 1$ for all $c \in \mathbb{F}_q$, then each polynomial $gcd(x^n - 1, g(x) - c)$ is irreducible over $\mathbb{F}_q$.

Example 2.7.6. ([21]) For $q = 2, n = 15$ and $gcd(q,n) = 1$, factorize the polynomial

$$x^{15} - 1$$

over $\mathbb{F}_2$ into a product of irreducible polynomials. First, partition the 15 numbers $0, 1, 2, \ldots, 14$ into 2-cycles mod 15.

Assume that they have the properties:

$$\begin{aligned} a_i q &\equiv a_{i+1} \pmod{n},\ i = 0, 1, 2, \ldots, l-2, \text{ and} \\ a_0 q^l &\equiv a_{l-1} q \equiv a_0 \pmod{n}. \end{aligned}$$

Then we say that they form a 2-cycles mod 15 denoted by

$$(0), (1, 2, 4, 8), (3, 6, 12, 9), (5, 10), (7, 14, 13, 11).$$

So the length of the 2-cycles mod 15 constitute $1, 4, 4, 2, 4$, respectively. Corresponding to each of these 2-cycles, there is a monic irreducible factor of $x^{15} - 1$ over $\mathbb{F}_2$. The order of 2 in $\mathbb{Z}_{15}^*$ is $m = 4$. Then $15|(2^4 - 1)$. We can choose an irreducible polynomial $f(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$ with degree $4 = m$ to construct the finite field $\mathbb{F}_{16} = \mathbb{F}_{2^4} \cong \mathbb{F}_2[x]/(x^4 + x^3 + 1)$. Let $\alpha = \overline{x} \in \mathbb{F}_{2^4}$ be a root of $x^4 + x^3 + 1$. Then $\alpha^4 + \alpha^3 + 1 = 0$ and $\mathbb{F}_{2^4} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha + 1, \alpha^2 + 1, \alpha^3 + 1, \alpha^2 + \alpha, \alpha^3 + \alpha, \alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$. Moreover, α is a primitive 15th root of unity over $\mathbb{F}_2$. Hence $\mathbb{F}_{2^4} = \{0, \alpha, \alpha^2, \ldots, \alpha^{14}, \alpha^{15} = 1\}$. Then, the monic irreducible factors of $x^{15} - 1$ over $\mathbb{F}_2$ are

$$\begin{aligned} f_0(x) &= (x - \alpha^0) \\ f_1(x) &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) \\ f_2(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) \\ f_3(x) &= (x - \alpha^5)(x - \alpha^{10}) \\ f_4(x) &= (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{11})(x - \alpha^{13}). \end{aligned}$$

For each q-cycle mod n, its length and the degree of its correspondence polynomial are equal. Now we have the complete factorization of $x^{15} - 1$ over $\mathbb{F}_2$,

$$x^{15} - 1 = f_0(x) f_1(x) f_2(x) f_3(x) f_4(x).$$

To express $f_0(x), f_1(x), f_2(x), f_3(x), f_4(x)$ as polynomial with coefficient in $\mathbb{F}_2$,

we get

$$\begin{aligned} f_0(x) &= x+1 \\ f_1(x) &= x^4+x^3+1 \\ f_2(x) &= x^4+x^3+x^2+x+1 \\ f_3(x) &= x^2+x+1 \\ f_4(x) &= x^4+x+1. \end{aligned}$$

Therefore

$$x^{15}-1=(x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x+1).$$

This is the complete factorization of $x^{15}-1$ into a product of monic irreducible polynomials over $\mathbb{F}_2$. Moreover, the number of distinct monic irreducible factors in $\mathbb{F}_2[x]$ of $x^{15}-1$ is 5 and is equal to the number of 2-cycles mod 15.

Theorem 2.7.7. ([19]) Let $n \in \mathbb{N}$ be such that $gcd(q,n)=1$. Let $a,b \in \mathbb{Z}_n$ and $(a, aq, \ldots, aq^{l-1})$ be a q-cycle mod n. Then

(1) The element $b \in (a, aq, \ldots, aq^{l-1})$ if and only if $b \equiv aq^k \bmod n$ for some $k \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

(2) The length of each q-cycle mod n divides $O_n(q)$ where $O_n(q)$ is the order of q in $\mathbb{Z}_n^* := \mathbb{Z}_n \backslash \{0\}$.

CHAPTER III

PRIMITIVE POLYNOMIALS

In this chapter, we give some criteria for primitive polynomials over finite fields.

3.1 q-Cycle criteria for primitive polynomials

In this section, we focus on monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ where $gcd(q, n) = 1$. We give a new criterion for primitive polynomials which are monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$. This criterion is based on concept of q-cycles mod n. q-cycles mod n are not hard to construct, and hence the concept of q-cycles mod n is a good optional to check primitive polynomials over finite fields.

For any positive integer n, let $\mathbb{F}_{q^n}$ be a finite extension field of a finite field $\mathbb{F}_q$ with q^n and q elements, respectively, where q is a prime power. Let $n \in \mathbb{N}$ be such that $gcd(q, n) = 1$. Suppose that $a_0, a_1, a_2, \ldots, a_{l-1}$ are l distinct numbers chosen from $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. We now recall that if

$$\begin{aligned} a_i q &\equiv a_{i+1} \pmod{n},\ i = 0, 1, 2, \ldots, l-2, \text{ and} \\ a_0 q^l &\equiv a_{l-1} q \equiv a_0 \pmod{n}, \end{aligned}$$

then we say that $(a_0, a_1, a_2, ..., a_{l-1})$ is a q-cycle mod n and its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

has degree l and is a monic irreducible factor of $x^n - 1$. If $a_0 = 0$, then its correspondence polynomial $f_0(x) = (x - \alpha^0) = (x - 1)$ is not a primitive polynomial over $\mathbb{F}_q$. In this chapter, we will investigate the correspondence polynomial $f(x)$ of q-cycle $(a_0, a_1, a_2, ..., a_{l-1})$ where the starter element $a_0 \neq 0$. Our main theorem reads:

Theorem 3.1.1. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exists a primitive nth root of unity in $\mathbb{F}_{q^m}$). Suppose that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length l and $ord(\alpha) = q^l - 1$. Then its correspondence polynomial $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$ is a primitive polynomial over $\mathbb{F}_q$ if and only if $gcd(a_0, q^l - 1) = 1$.

Proof. Let $(a_0, a_1, \ldots, a_{l-1})$ be a q-cycle mod n of length l and let $ord(\alpha) = q^l - 1$. By Theorem 2.7.2, we have the correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}}) \in \mathbb{F}_q[x]$$

is a monic irreducible factor of $x^n - 1$ with degree l. Since l is the length of $(a_0, a_1, \ldots, a_{l-1})$, by Theorem 2.7.7, we have $l|m$. Since $l|m$ and by Theorem 2.1.20, $\mathbb{F}_{q^l}$ is a subfield of $\mathbb{F}_{q^m}$, so $\mathbb{F}_{q^l}^*$ is a cyclic group of order $q^l - 1$. Since $ord(\alpha) = q^l - 1$, we get α is a primitive element of $\mathbb{F}_{q^l}$, that is, $\mathbb{F}_{q^l}^* = \langle \alpha \rangle$.

We start by suppose $gcd(a_0, q^l - 1) = 1$. Since $gcd(q, q^l - 1) = 1$, we have $gcd(a_0 q, q^l - 1) = 1$. Proceeding in the same manner, $gcd(a_0 q^i, q^l - 1) = 1$ for all $i = 0, 1, \ldots, l - 1$. By constructing of q-cycles mod n, we have $a_0 q \equiv a_1, a_0 q^2 \equiv a_2, \ldots, a_0 q^{l-1} \equiv a_{l-1}, a_0 q^l \equiv a_0 \in \mathbb{Z}_n$. By Theorem 2.1.6, $\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}}$ are primitive elements of $\mathbb{F}_{q^l}$. Then $ord(\alpha^{a_i}) = q^l - 1$ and note that α^{a_i} are all roots of $f(x)$ for all $i = 0, 1, \ldots, l - 1$. By Theorem 2.4.6, $ord(f) = ord(\alpha^{a_i}) = q^l - 1$. Since $f(x)$ is monic irreducible degree l and by Theorem 2.4.7, $f(x)$ is a primitive polynomial over $\mathbb{F}_q$.

Now, assume that $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$ is a primitive polynomial over $\mathbb{F}_q$. We remark that $f(x)$ is monic irreducible of degree l. Thus all l roots of $f(x)$, $\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}} \in \mathbb{F}_{q^l}$ are primitive elements. Since α is a primitive element of $\mathbb{F}_{q^l}$ and by Theorem 2.1.6, $gcd(a_0, q^l - 1) = 1$. □

The next example support the result in Theorem 3.1.1.

Example 3.1.2. For $q = 2$ and $n = 9$, we consider the polynomial $x^9 - 1$ over $\mathbb{F}_2$.

Start with partition the 9 numbers $0, 1, 2, \ldots, 8$ into 2-cycles mod 9:

$$(0), (1, 2, 4, 8, 7, 5), (3, 6).$$

We see that $(0), (1, 2, 4, 8, 7, 5), (3, 6)$ are all 2-cycles mod 9 of length $1, 6$ and 2, respectively. The correspondence of each 2-cycle mod 9 is an irreducible factor of $x^9 - 1$ over $\mathbb{F}_2$. The order of 2 in $\mathbb{Z}_9^*$ is $m = 6$. We can choose $x^6 + x^3 + 1 \in \mathbb{F}_2[x]$ an irreducible polynomial to construct the finite field $\mathbb{F}_{2^6} \cong \mathbb{F}_2[x]/(x^6 + x^3 + 1)$. Let $\alpha = \bar{x} \in \mathbb{F}_{2^6}$ be a root of $x^6 + x^3 + 1$. Then α is a primitive 9th root of unity over $\mathbb{F}_2$. By Theorem 2.7.2, we can get all irreducible factors of $x^9 - 1$ over $\mathbb{F}_2$ as follow:

$$\begin{aligned} f_0(x) &= (x - \alpha^0) \\ f_1(x) &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^7)(x - \alpha^5) \\ f_2(x) &= (x - \alpha^3)(x - \alpha^6). \end{aligned}$$

Then the complete factorization of $x^9 - 1$ over $\mathbb{F}_2$ is $x^9 - 1 = f_0(x)f_1(x)f_2(x)$. By considering $\alpha = \bar{x} \in \mathbb{F}_{2^6} \cong \mathbb{F}_2[x]/(x^6 + x^3 + 1)$, we get the explicit terms of $f_0(x), f_1(x), f_2(x)$ as polynomials with coefficients in $\mathbb{F}_2$,

$$\begin{aligned} f_0(x) &= x + 1 \\ f_1(x) &= x^6 + x^3 + 1 \\ f_2(x) &= x^2 + x + 1. \end{aligned}$$

We first consider $(1, 2, 4, 8, 7, 5)$, 2-cycle mod 9 of length $l = 6$ and $ord(\alpha) = 63 = 2^6 - 1 = q^l - 1$. Thus we can apply Theorem 3.1.1 to this q-cycle $(1, 2, 4, 8, 7, 5)$ where $a_0 = 1$. Since $gcd(a_0, q^l - 1) = gcd(1, 63) = 1$ and by Theorem 3.1.1, its correspondence polynomial

$$f_1(x) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^7)(x - \alpha^5) = x^6 + x^3 + 1 \in \mathbb{F}_2[x]$$

is a primitive polynomial.

Next we consider $(3,6)$, 2-cycle mod 9 with length $l=2$ and $ord(\alpha)=63\neq 2^2-1=q^l-1$. Thus we can not apply Theorem 3.1.1 to this case. This 2-cycle has $a_0=3$ and $gcd(a_0,q^l-1)=gcd(3,2^2-1)=gcd(3,3)\neq 1$ but its correspondence polynomial $f_2(x)=(x-\alpha^3)(x-\alpha^6)=x^2+x+1$ is primitive over $\mathbb{F}_2$. In this case, we see that the assumption $ord(\alpha)=q^l-1$ is crucial for result in Theorem 3.1.1.

For $n\in\mathbb{N}$ with $gcd(q,n)=1$, if q-cycles mod n are only (0) and $(a_0,a_1,\ldots,a_{n-2})$ with length 1 and $n-1$, respectively, then we have $a_0=1$ and $gcd(a_0,q^{n-1}-1)=1$. By Theorem 3.1.1, its correspondence polynomial

$$f(x)=(x-\alpha^{a_0})(x-\alpha^{a_1})\cdots(x-\alpha^{a_{n-2}})$$

is primitive over $\mathbb{F}_q$. More precisely, we can state with the following remark.

Remark 3.1.3. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exists a primitive nth root of unity in $\mathbb{F}_{q^m}$). Suppose that $(a_0,a_1,\ldots,a_{l-1})$ is a q-cycle mod n of length l and $ord(\alpha)=q^l-1$. Then we have if length $l=n-1$, then its correspondence polynomial

$$f(x)=(x-\alpha^{a_0})(x-\alpha^{a_1})\cdots(x-\alpha^{a_{l-1}})$$

is primitive over $\mathbb{F}_q$.

Primitive polynomial in the next example arise from Remark 3.1.3.

Example 3.1.4. For $q=2$ and $n=5$, we consider the polynomial x^5-1 over $\mathbb{F}_2$. Start with partition the 5 numbers $0,1,2,3,4$ into 2-cycles mod 5:

$$(0),(1,2,3,4).$$

Then $(0),(1,2,4,3)$ are all 2-cycles mod 5 of length 1 and 4, respectively. The correspondence of each 2-cycle mod 5 is an irreducible factor of x^5-1 over $\mathbb{F}_2$. The order of 2 in $\mathbb{Z}_5^*$ is $m=4$. We can choose $x^4+x^3+1\in\mathbb{F}_2[x]$ an irreducible

polynomial to construct the finite field $\mathbb{F}_{2^4} \cong \mathbb{F}_2[x]/(x^4+x^3+1)$. Let $\alpha = \bar{x} \in \mathbb{F}_{2^4}$ be a root of x^4+x^3+1. Then α is a primitive 5th root of unity over $\mathbb{F}_2$. By Theorem 2.7.2, we can get all irreducible factors of x^5-1 over $\mathbb{F}_2$ as follows:

$$\begin{aligned} f_0(x) &= (x-\alpha^0) \\ f_1(x) &= (x-\alpha^1)(x-\alpha^2)(x-\alpha^4)(x-\alpha^3). \end{aligned}$$

Then the complete factorization of x^5-1 over $\mathbb{F}_2$ is $x^5-1 = f_0(x)f_1(x)$.
By considering $\alpha = \bar{x} \in \mathbb{F}_{2^4} \cong \mathbb{F}_2[x]/(x^4+x^3+1)$, we can express $f_0(x), f_1(x)$ as polynomials with coefficients in $\mathbb{F}_2$,

$$\begin{aligned} f_0(x) &= x+1 \\ f_1(x) &= x^4+x^3+x^2+x+1. \end{aligned}$$

Note that $(1,2,4,3)$ is the 2-cycle mod 5 of length $l = 4 = n-1$ and $ord(\alpha) = 15 = 2^4-1 = q^l-1$. Since $(1,2,4,3)$ is 2-cycle mod 5 with length $l = n-1$ and by Remark 3.1.3, its correspondence polynomial

$$f_1(x) = (x-\alpha^1)(x-\alpha^2)(x-\alpha^4)(x-\alpha^3) = x^4+x^3+x^2+x+1 \in \mathbb{F}_2[x]$$

is a primitive polynomial.

For p^l-1 where p is a prime number, if p is odd, then p^l-1 is not prime. Thus p^l-1 can be prime if $p=2$. Special case when $q^l-1 = 2^l-1$ is prime will be investigated in the next corollary.

Corollary 3.1.5. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exists a primitive nth root of unity in $\mathbb{F}_{q^m}$). Suppose that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length l and $ord(\alpha) = q^l-1$. Then we have if q^l-1 is a prime number where $q=2$, then its correspondence polynomial $f(x) = (x-\alpha^{a_0})(x-\alpha^{a_1})\cdots(x-\alpha^{a_{l-1}})$ is primitive over $\mathbb{F}_2$.

Proof. Since $a_0 \in \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and $n = q^l - 1$ is prime, we have

$$gcd(a_0, q^l - 1) = 1.$$

By Theorem 3.1.1,

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a primitive polynomial over $\mathbb{F}_2$. □

Example 3.1.6. For $q = 2$ and $n = 7$, we consider the polynomial $x^7 - 1$ over $\mathbb{F}_2$. Then $(0), (1, 2, 4), (3, 6, 5)$ are all 2-cycles mod 7 of length $1, 3$ and 3, respectively. The correspondence of each 2-cycle mod 7 is an irreducible factor of $x^7 - 1$ over $\mathbb{F}_2$. The order of 2 in $\mathbb{Z}_7^*$ is $m = 3$. We can choose $x^3 + x + 1 \in \mathbb{F}_2[x]$ an irreducible polynomial to construct the finite field $\mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1)$. Let $\alpha = \bar{x} \in \mathbb{F}_{2^3}$ be a root of $x^3 + x + 1$. Then α is a primitive 7th root of unity over $\mathbb{F}_2$. By Theorem 2.7.2, we can get all irreducible factors of $x^7 - 1$ over $\mathbb{F}_2$ as follows:

$$\begin{aligned} f_0(x) &= (x - \alpha^0) \\ f_1(x) &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4) \\ f_2(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^5). \end{aligned}$$

Then the complete factorization of $x^7 - 1$ over $\mathbb{F}_2$ is $x^7 - 1 = f_0(x) f_1(x) f_2(x)$. For $\alpha = \bar{x} \in \mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1)$, we can get $f_0(x), f_1(x), f_2(x)$ as polynomials with coefficients in $\mathbb{F}_2$,

$$\begin{aligned} f_0(x) &= x + 1 \\ f_1(x) &= x^3 + x + 1 \\ f_2(x) &= x^3 + x^2 + 1. \end{aligned}$$

We see that $(1, 2, 4)$ is 2-cycle mod 7 of length $l = 3$, $ord(\alpha) = 7 = 2^3 - 1 = q^l - 1$ and $a_0 = 1$. Since $q^l - 1 = 2^3 - 1 = 7$ is prime, $gcd(a_0, q^l - 1) = gcd(1, 7) = 1$.

By Corollary 3.1.5, its correspondence polynomial

$$f_1(x) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1 \in \mathbb{F}_2[x]$$

is primitive.

Similarly, $(3, 6, 5)$ is the 2-cycle mod 7 of length $l = 3$, $ord(\alpha) = 7 = 2^3 - 1 = q^l - 1$ and $a_0 = 3$. Since $q^l - 1 = 2^3 - 1 = 7$ is prime, $gcd(a_0, q^l - 1) = gcd(3, 7) = 1$. By Corollary 3.1.5, its correspondence polynomial

$$f_2(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$$

is primitive.

CHAPTER IV

k-NORMAL POLYNOMIALS

In this chapter, we focus to give some criteria for k-normal elements and k-normal polynomials (especially $k = 0, 1$) over finite fields by using trace functions.

4.1 Trace function criteria for k-normal polynomials

In this section, we show some properties and some criteria for k-normal elements, which based on trace functions from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. Then we use these criteria for normal polynomials over finite fields. We now recall, for $\alpha \in \mathbb{F}_{q^n}$, the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, is given by $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$, and for each $0 \leqslant k \leqslant n-1$, the element $\alpha \in \mathbb{F}_{q^n}$ is called a k-normal element if and only if $deg(gcd(x^n - 1, g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}})) = k$. In this section, we devote to the cases $n = 2$ and $n = q^m - 1$ where q is a prime power and m is a positive integer.

The first part of this section we will investigate $0, 1$-normal elements of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. When $n = 2$ and $\alpha \in \mathbb{F}_{q^2}$, we consider

$$gcd(x^2 - 1, g_\alpha(x) = \alpha x + \alpha^q).$$

If α is an element in the ground field $\mathbb{F}_q$, we have $\alpha^q = \alpha$ and then

$$gcd(x^2 - 1 = (x-1)(x+1), \alpha x + \alpha = \alpha(x+1)) = x + 1.$$

So implies α is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

Proposition 4.1.1. Let $\alpha \in \mathbb{F}_{q^2}^*$. If 1 is the unique root in $\mathbb{F}_{q^2}$ of $g_\alpha(x)$, then α is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

Proof. In this proposition, $n = 2$ and for $\alpha \in \mathbb{F}_{q^2}$, $g_\alpha(x) = \alpha x + \alpha^q$ has degree 1. Assume that 1 is the unique root of $g_\alpha(x)$. Then $g_\alpha(1) = 0$ and so $(x-1)|g_\alpha(x)$. Since $(x-1)|(x^2-1)$ and by definition of the greatest common divisor, we get that

$$gcd(x^2 - 1, g_\alpha(x)) = x - 1.$$

Thus $deg(gcd(x^2 - 1, g_\alpha(x))) = 1$. Therefore α is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. □

Example 4.1.2. We consider $\mathbb{F}_{3^2} \cong \mathbb{F}_3[x]/(x^2+2x+2) = \{\alpha, \alpha+1, 2\alpha+1, 2, 2\alpha, 2\alpha+2, \alpha+2, 1, 0\}$ the field constructed by irreducible polynomial $x^2 + 2x + 2 \in \mathbb{F}_3[x]$. Denote the residue class of x mod $x^2 + 2x + 2$ by α. Then

$$\mathbb{F}_{3^2} = \{0, 1, \alpha, 2\alpha, 2\alpha + 1, \alpha + 1, \alpha + 2, 2\alpha + 1, 2\alpha + 2\}$$

and

$$g_{2\alpha+2}(x) = (2\alpha + 2)(x) + (2\alpha + 2)^3.$$

We see that

$$g_{2\alpha+2}(0) = (2\alpha + 2)(0) + (2\alpha + 2)^3 = \alpha + 1,$$
$$g_{2\alpha+2}(1) = (2\alpha + 2)(1) + (2\alpha + 2)^3 = 0,$$
$$g_{2\alpha+2}(2) = (2\alpha + 2)(2) + (2\alpha + 2)^3 = 2\alpha + 2,$$
$$g_{2\alpha+2}(\alpha) = (2\alpha + 2)(\alpha) + (2\alpha + 2)^3 = 2\alpha,$$
$$g_{2\alpha+2}(2\alpha) = (2\alpha + 2)(2\alpha) + (2\alpha + 2)^3 = 2,$$
$$g_{2\alpha+2}(\alpha + 1) = (2\alpha + 2)(\alpha + 1) + (2\alpha + 2)^3 = \alpha + 2,$$
$$g_{2\alpha+2}(\alpha + 2) = (2\alpha + 2)(\alpha + 2) + (2\alpha + 2)^3 = 1,$$
$$g_{2\alpha+2}(2\alpha + 1) = (2\alpha + 2)(2\alpha + 1) + (2\alpha + 2)^3 = 2\alpha + 1,$$
$$g_{2\alpha+2}(2\alpha + 2) = (2\alpha + 2)(2\alpha + 2) + (2\alpha + 2)^3 = \alpha.$$

So 1 is the unique root in $\mathbb{F}_{3^2}$ of $g_{2\alpha+2}(x) = (2\alpha+2)(x)+(2\alpha+2)^3$. By Proposition 4.1.1, we obtain $2\alpha + 2$ is a 1-normal element of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$.

Next result is the main tool for studying 0-normal and 1-normal elements of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

Theorem 4.1.3. Let $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Then $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = 0$ if and only if α is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

Proof. For $n = 2$ and $\alpha \in \mathbb{F}_{q^2}^*$, $g_\alpha(x) = \alpha x + \alpha^q$. Since $g_\alpha(1) = \alpha(1) + \alpha^q = \alpha + \alpha^q = Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = 0$, we have $(x-1)|g_\alpha(x)$. Since $(x-1)|(x^2-1)$ and by definition of the greatest common divisor, we get that

$$gcd(x^2 - 1, g_\alpha(x)) = x - 1.$$

Thus $deg(gcd(x^2 - 1, g_\alpha(x))) = 1$. Therefore α is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Conversely, let α be a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Note that $x^2 - 1 = (x-1)(x+1)$. If $gcd(x^2 - 1, \alpha x + \alpha^q) = x + 1$, then $(x+1)|(\alpha x + \alpha^q)$ and -1 is a root of $\alpha x + \alpha^q$ and hence $\alpha = \alpha^q$ contradicts with $\alpha \notin \mathbb{F}_q$. Thus

$$gcd(x^2 - 1, \alpha x + \alpha^q) = x - 1,$$

and $(x-1)|(\alpha x + \alpha^q) = g_\alpha(x)$. Therefore $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q = \alpha(1) + \alpha^q = g_\alpha(1) = 0$. □

Remark 4.1.4. By the negation of Theorem 4.1.3, $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) \neq 0$ if and only if α is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, that is, $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) \neq 0$ if and only if $f(x) = (x - \alpha)(x - \alpha^q)$ is a normal polynomial over $\mathbb{F}_q$.

Example 4.1.5. Consider $\mathbb{F}_{3^2} \cong \mathbb{F}_3[x]/(x^2 + x + 2)$ the field constructed by irreducible polynomial $x^2 + x + 2 \in \mathbb{F}_3[x]$. Denote the residue class of x mod $x^2 + x + 2$ by α. Then

$$\mathbb{F}_{3^2} = \{0, 1, \alpha, 2\alpha, 2\alpha + 1, \alpha + 1, \alpha + 2, 2\alpha + 1, 2\alpha + 2\}$$

and we see that

$$Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha) = Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(2\alpha + 2) = Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(2\alpha) = Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha + 1) \neq 0,$$

but $Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(2\alpha+1) = Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha+2) = 0$, by Theorem 4.1.3, we obtain $2\alpha+1, \alpha+2$ are 1-normal elements of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$. Moreover, $\alpha, 2\alpha+2, 2\alpha, \alpha+1$ are 0-normal elements of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$ and for $\beta \in \{\alpha, 2\alpha+2, 2\alpha, \alpha+1\}$,

$$f(x) = (x-\beta)(x-\beta^q)$$

is a normal polynomial over $\mathbb{F}_3$.

For $\alpha, \beta \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$, we will apply the result of Theorem 4.1.3 to consider the sum of α amd β, and the inverse of α.

Corollary 4.1.6. Let $\alpha, \beta \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$. If α and β are 1-normal elements of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ with $\alpha+\beta \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$, then $\alpha+\beta$ is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

Proof. Let $\alpha, \beta \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$ be such that α and β are 1-normal elements of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ and $\alpha+\beta \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$. By Theorem 4.1.3, we get that $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = 0$ and $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta) = 0$. Thus

$$Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha+\beta) = Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta) = 0+0 = 0.$$

Therefore $\alpha+\beta$ is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. □

Example 4.1.7. This example constructs a 1-normal element of $\mathbb{F}_{3^2}$. Let

$$\mathbb{F}_{3^2} \cong \mathbb{F}_3[x]/(x^2+2x+2) = \{\alpha, \alpha+1, 2\alpha+1, 2, 2\alpha, 2\alpha+2, \alpha+2, 1, 0\}$$

be a field constructed by irreducible polynomial x^2+2x+2 in $\mathbb{F}_3[x]$ and denote the residue class of x mod x^2+2x+2 by α. From Example 4.1.2, we known that $2\alpha+2$ is a 1-normal element of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$. Since

$$(2\alpha+2)+(2\alpha+2) = \alpha+1 \in \mathbb{F}_{3^2}\backslash\mathbb{F}_3,$$

and

$$Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha+1) = (\alpha+1)+(\alpha+1)^3 = \alpha+1+2\alpha+2 = 0,$$

we have $\alpha+1$ is a 1-normal element of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$.

Corollary 4.1.8. Let $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. If α is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, then α^{-1} is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

Proof. Let α be a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Then $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = 0$.
Since $\alpha \notin \mathbb{F}_q, \alpha^{-1} \notin \mathbb{F}_q$. Note that $\alpha^{q^2-1} = \alpha\alpha^{q^2-2} = 1$, so $\alpha^{-1} = \alpha^{q^2-2}$ and $\alpha^q\alpha^{q^2-q-1} = 1$, so $(\alpha^q)^{-1} = \alpha^{q^2-q-1}$. Consider

$$\begin{aligned}
Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha^{-1}) &= \alpha^{-1} + (\alpha^{-1})^q \\
&= \alpha^{-1} + (\alpha^q)^{-1} \\
&= \alpha^{q^2-2} + \alpha^{q^2-q-1} \\
&= \frac{\alpha^{q^2}}{\alpha^2} + \frac{\alpha^{q^2}}{\alpha^{q+1}} \\
&= \frac{\alpha^{q^2}\alpha^{q+1} + \alpha^{q^2}\alpha^2}{\alpha^2\alpha^{q+1}} \\
&= \frac{\alpha^2(\alpha^q + \alpha)}{\alpha^2(\alpha^{q+1})} \\
&= \frac{\alpha^q + \alpha}{\alpha^{q+1}} \\
&= \frac{Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha)}{\alpha^{q+1}} \\
&= 0.
\end{aligned}$$

Therefore α^{-1} is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. □

Example 4.1.9. Let $\mathbb{F}_{3^2} \cong \mathbb{F}_3[x]/(x^2 + 2x + 2)$ be the field arised from irreducible polynomial $x^2 + 2x + 2 \in \mathbb{F}_3[x]$ and denote the residue class of x mod $x^2 + 2x + 2$ by α. By Example 4.1.7, we get that $\alpha + 1$ is a 1-normal element of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$. Since $(\alpha + 1)(2\alpha + 2) = 1$, we have $(\alpha + 1)^{-1} = 2\alpha + 2$. Note that

$$Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(2\alpha + 2) = (2\alpha + 2) + (2\alpha + 2)^3 = 0,$$

so $(\alpha + 1)^{-1} = 2\alpha + 2$ is a 1-normal element of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$.

For 1-normal elements $\alpha, \beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, we can conclude that $\alpha + \beta$ and α^{-1} are 1-normal elements in $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Before we investigate $\alpha + \beta$ and α^{-1} when α and β are 0-normal elements in $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, we will note the following example.

Example 4.1.10. We view $\mathbb{F}_{2^2} \cong \mathbb{F}_2[x]/(x^2+x+1)$ the field arised from irreducible polynomial x^2+x+1 over $\mathbb{F}_2$ and denote the residue class of x mod x^2+x+1 by α. Then $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha+1\}$, and we compute

$$Tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\alpha) = \alpha + \alpha^2 = \alpha + (\alpha+1) = 1,$$

and

$$Tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\alpha+1) = (\alpha+1) + (\alpha+1)^2 = (\alpha+1) + (\alpha) = 1.$$

Thus α and $\alpha+1$ are 0-normal elements of $\mathbb{F}_{2^2}$ over $\mathbb{F}_2$ by Theorem 4.1.3. Since $Tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(\alpha + (\alpha+1)) = Tr_{\mathbb{F}_{2^2}/\mathbb{F}_2}(1) = 1 + 1^2 = 0$, we have that $\alpha + (\alpha+1)$ is a 1-normal element of $\mathbb{F}_{2^2}$ over $\mathbb{F}_2$.

For $\alpha, \beta \in \mathbb{F}_{q^2}$, we obtain counterexample that α and β are 0-normal elements of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, but $\alpha+\beta$ is not 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. In the next result, we will find a sufficient condition for $\alpha+\beta$ is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

Proposition 4.1.11. Let $\alpha, \beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. If α and β are 0-normal elements of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ with $\alpha+\beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ and $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta) \neq 0$ in $\mathbb{F}_q$, then $\alpha+\beta$ is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

Proof. Let α and β be 0-normal elements of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ with $\alpha+\beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Then by Theorem 4.1.3, $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) \neq 0$ in $\mathbb{F}_q$ and $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta) \neq 0$ in $\mathbb{F}_q$. By assumption, we get that

$$Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha+\beta) = Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta) \neq 0 \text{ in } \mathbb{F}_q.$$

Therefore $\alpha+\beta$ is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. □

Example 4.1.12. We give $\mathbb{F}_{3^2} \cong \mathbb{F}_3[x]/(x^2+2x+2)$ the field constructed by irreducible polynomial $x^2+2x+2 \in \mathbb{F}_3[x]$ and let α be the residue class of x mod x^2+2x+2. Then

$$Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha) = \alpha + \alpha^3 = \alpha + (2\alpha+1) = 1$$

and

$$Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha^3) = \alpha^3 + (\alpha^3)^3 = \alpha^3 + \alpha^9 = \alpha^3 + \alpha = 1.$$

Thus by Theorem 4.1.3, α and α^3 are 0-normal elements of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$. Moreover,

$$Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha) + Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha^3) = 2 \text{ in } \mathbb{F}_3.$$

By Proposition 4.1.11, $\alpha + \alpha^3$ must be 0-normal element of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$ and

$$f(x) = (x - (\alpha + \alpha^3))(x - (\alpha + \alpha^3)^3)$$

is a normal polynomial over $\mathbb{F}_3$.

Proposition 4.1.13. Let $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. If α is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, then α^{-1} is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

Proof. Assume that α is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Then $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) \neq 0$. Since $\alpha \notin \mathbb{F}_q$, we have $\alpha^{-1} \notin \mathbb{F}_q$. Note that for $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, we get that $(\alpha^{q+1})^q = (\alpha^q \alpha)^q = \alpha^{q^2}\alpha^q = \alpha\alpha^q = \alpha^{q+1}$ and so $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q^*$ by Corollary 2.1.22. Since

$$Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha^{-1}) = \frac{Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha)}{\alpha^{q+1}},$$

we have $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha^{-1}) \neq 0$. Therefore α^{-1} is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. □

Example 4.1.14. We may regard $\mathbb{F}_{3^2} \cong \mathbb{F}_3[x]/(x^2 + x + 2)$ where $x^2 + x + 2$ is irreducible over $\mathbb{F}_3$. Let α be the residue class of x mod $x^2 + x + 2$. Note that

$$Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha) = \alpha + \alpha^3 = \alpha + (2\alpha + 2) = 2.$$

By Theorem 4.1.3, we get that α is a 0-normal element of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$. Since $(\alpha)(\alpha + 1) = 1$, we have $\alpha^{-1} = \alpha + 1$. Therefore $\alpha + 1$ is a 0-normal element of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$ by Proposition 4.1.13 and so

$$f(x) = (x - (\alpha + 1))(x - (\alpha + 1)^3)$$

is a normal polynomial over $\mathbb{F}_3$.

Next part of this section, we are interested in the case $n = q^m - 1$ where q is a prime power and m is a positive integer. For $\alpha \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q$, we can show that there is only two types of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, that is, 0-normal element and 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

For $n = q^m - 1$ and $\alpha \in \mathbb{F}_{q^n}$, If α is element in the ground field $\mathbb{F}_q$, then we have $\alpha^q = \alpha$ and

$$\begin{aligned} gcd(x^n - 1, g_\alpha(x)) &= gcd(x^n - 1, \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}) \\ &= gcd(x^n - 1, \alpha(x^{n-1} + x^{n-2} + \cdots + 1)) \\ &= x^{n-1} + x^{n-2} + \cdots + 1, \end{aligned}$$

hence we have α is a $(n-1)$-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. From now on we investigate only $\alpha \notin \mathbb{F}_q$.

It is well-known that if $gcd(q, n) = 1$, then the polynomial $x^n - 1$ has no multiple factors in $\mathbb{F}_q[x]$. In the next result, $n = q^m - 1$ and $gcd(q, q^m - 1) = 1$. We consequently get that $x^{q^m-1} - 1$ has no multiple factors in $\mathbb{F}_{q^{q^m-1}}[x]$.

Theorem 4.1.15. Let $n = q^m - 1$ where m is a positive integer and $\alpha \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q$. Then

(1) α is a 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$.

(2) α is a 0-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$.

Proof. Assume that $\alpha \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q = \mathbb{F}_{q^{q^m-1}} \backslash \mathbb{F}_q$. First we will show that

$$(x^{q^m-2} + x^{q^m-3} + \cdots + 1) \not| (\alpha x^{q^m-2} + \alpha^q x^{q^m-3} + \cdots + \alpha^{q^{q^m-2}}) = g_\alpha(x).$$

Suppose that

$$(x^{q^m-2} + x^{q^m-3} + \cdots + 1) | (\alpha x^{q^m-2} + \alpha^q x^{q^m-3} + \cdots + \alpha^{q^{q^m-2}}).$$

There exists $\beta \in \mathbb{F}_{q^{q^m-1}}[x]$ such that

$$(\alpha x^{q^m-2} + \alpha^q x^{q^m-3} + \cdots + \alpha^{q^{q^m-2}}) = \beta(x^{q^m-2} + x^{q^m-3} + \cdots + 1)$$

$$= \beta x^{q^m-2} + \beta x^{q^m-3} + \cdots + \beta.$$

This implies that $\alpha = \alpha^q = \cdots = \alpha^{q^{q^m-2}} = \beta$. Since $\alpha = \alpha^q$ and by Corollary 2.1.22, we have $\alpha \in \mathbb{F}_q$. It contradicts $\alpha \notin \mathbb{F}_q$. Thus

$$(x^{q^m-2} + x^{q^m-3} + \cdots + 1) \not| (\alpha x^{q^m-2} + \alpha^q x^{q^m-3} + \cdots + \alpha^{q^{q^m-2}}) = g_\alpha(x).$$

So $\alpha x^{q^m-2} + \alpha^q x^{q^m-3} + \cdots + \alpha^{q^{q^m-2}} \neq \gamma(x^{q^m-2} + x^{q^m-3} + \cdots + 1)$ for all $\gamma \in \mathbb{F}_{q^{q^m-1}}[x]$. Note that

$$\begin{aligned} x^{q^m} - x &= x(x^{q^m-1} - 1) \\ &= x(x-1)g(x) \text{ where } g(x) \in \mathbb{F}_{q^{q^m-1}}[x] \text{ with degree } q^m - 2 \\ &= x(x-1)(x^{q^m-2} + x^{q^m-3} + \cdots + x + 1) \\ &= x(x-1)g_1(x)g_2(x)\cdots g_r(x) \end{aligned}$$

by the unique factorization for polynomials and $x^{q^m-1} - 1$ has no multiple factors where $g_1(x)g_2(x)\cdots g_r(x) \in \mathbb{F}_{q^{q^m-1}}[x]$ are distinct irreducible polynomials.

Next we consider

$$\begin{aligned} \alpha x^{q^m-2} + \alpha^q x^{q^m-3} + \cdots + \alpha^{q^{q^m-2}} &\neq \gamma(x^{q^m-2} + x^{q^m-3} + \cdots + 1) \\ &= \gamma[g_1(x)g_2(x)g_3(x)\cdots g_r(x)] \\ &= \gamma g_1(x)[g_2(x)g_3(x)g_4(x)\cdots g_r(x)] \\ &= g_1(x)[\gamma g_2(x)g_3(x)g_4(x)\cdots g_r(x)]], \end{aligned}$$

for all $\gamma \in \mathbb{F}_{q^{q^m-1}}[x]$. Consequently, $g_1(x) \not| (\alpha x^{q^m-2} + \alpha^q x^{q^m-3} + \cdots + \alpha^{q^{q^m-2}})$. Similarly, $g_i(x) \not| (\alpha x^{q^m-2} + \alpha^q x^{q^m-3} + \cdots + \alpha^{q^{q^m-2}}) = g_\alpha(x)$, for all $1 \leqslant i \leqslant r$.

(1) If $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$, then

$$g_\alpha(1) = \alpha(1)^{q^m-2} + \alpha^q(1)^{q^m-3} + \cdots + \alpha^{q^{q^m-2}} = \alpha + \alpha^q + \cdots + \alpha^{q^{q^m-2}} = 0,$$

and so $(x-1)|(\alpha x^{q^m-2} + \alpha^q x^{q^m-3} + \cdots + \alpha^{q^{q^m-2}}) = g_\alpha(x)$. Since

$$(x^{q^m-1} - 1) = (x-1)(x^{q^m-2} + x^{q^m-3} + \cdots + 1) = (x-1)g_1(x)g_2(x)\cdots g_r(x)$$

and

$$(x-1)|g_\alpha(x) \text{ and } g_i(x) \not| g_\alpha(x) \text{ for all } 1 \leqslant i \leqslant r,$$

we have $x-1$ is only a common divisor of $x^{q^m-1}-1$ and $g_\alpha(x)$. Hence α is a 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Now, we assume that α is a 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then $deg(gcd(x^n-1, g_\alpha(x))) = 1$. Consider

$$\begin{aligned}
&gcd(x^n-1, g_\alpha(x)) \\
&= gcd((x-1)(x^{n-1}+x^{n-2}+\cdots+1), \alpha x^{n-1}+\alpha^q x^{n-2}+\cdots+\alpha^{q^{n-1}}) \\
&\text{since } n = q^m-1 \text{ and } (x^{q^m-2}+x^{q^m-3}+\cdots+1) \not| (\alpha x^{q^m-2}+\alpha^q x^{q^m-3}+\cdots \\
&+\alpha^{q^{q^m-2}}).
\end{aligned}$$

Now we get $gcd(x^n-1, g_\alpha(x)) = x-1$. Thus $(x-1)|(\alpha x^{n-1}+\alpha^q x^{n-2}+\cdots+\alpha^{q^{n-1}})$. Therefore $\alpha+\alpha^q+\cdots+\alpha^{q^{n-1}} = 0$. Hence $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$.

(2) If $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$, then $(x-1) \not| (\alpha x^{n-1}+\alpha^q x^{n-2}+\cdots+\alpha^{q^{n-1}})$ and so $x^{q^m-1}-1$ and $g_\alpha(x)$ has no a common divisor. Thus α is a 0-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Now, let α be a 0-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then $deg(gcd(x^n-1, g_\alpha(x))) = 0$. So $gcd(x^n-1, g_\alpha(x)) = 1$ and $(x-1) \not| g_\alpha(x)$. Therefore $0 \neq g_\alpha(1) = \alpha+\alpha^q+\cdots+\alpha^{q^{n-1}} = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$. Hence $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$. □

Remark 4.1.16. For $n = q^m-1$ and $\alpha \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q$ and by Theorem 4.1.15.(2), we obtain the followings.

(1) $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$ if and only if $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, that is, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$ if and only if $f(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$ is a normal polynomial over $\mathbb{F}_q$.

(2) If $q = 2$ and $q^n-1 = 2^n-1$ is a prime, then by Theorem 2.4.9, we have $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$ if and only if $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a primitive normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, that is, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$ if and only if $f(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$ is a primitive normal polynomial over $\mathbb{F}_q$.

Corollary 4.1.17. Let $n = q^m - 1$ where m is a positive integer and $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ be an irreducible polynomial over $\mathbb{F}_q$. Then $f(x)$ is a 1-normal polynomial over $\mathbb{F}_q$ if and only if $a_1 = 0$.

Proof. Assume that $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ is an irreducible polynomial over $\mathbb{F}_q$. Then there exists $\alpha \in \mathbb{F}_{q^n}$ such that α is a root of $f(x)$ and we have that $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are all distinct roots of $f(x)$ by Theorem 2.2.31. So we can write

$$f(x) = (x - \alpha)(x - \alpha^q)\cdots(x - \alpha^{q^{n-1}}).$$

Since $f(x)$ is a 1-normal polynomial over $\mathbb{F}_q$, we have α is a 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Thus $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are also 1-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ by Theorem 2.6.4. Hence $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$ by Theorem 4.1.15. From symmetric relation, we obtain that $a_1 = \alpha+\alpha^q+\cdots+\alpha^{q^{n-1}} = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$. Now, we assume that $a_1 = 0$. Note that $f(x) = x^n+a_1x^{n-1}+\cdots+a_n$ is an irreducible polynomial over $\mathbb{F}_q$. Then there is $\alpha \in \mathbb{F}_{q^n}$ such that α is a root of $f(x)$ and $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are all distinct roots of $f(x)$ by Theorem 2.2.31. Moreover, $f(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$. By symmetric relation, we see that $a_1 = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$, so $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$. By Theorem 4.1.15, α is a 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and we get that $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are also 1-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ by Theorem 2.6.4. Hence $f(x)$ is a 1-normal polynomial over $\mathbb{F}_q$. □

Corollary 4.1.18. Let $n = q^m - 1$ where m is a positive integer and $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ be an irreducible polynomial over $\mathbb{F}_q$. Then $f(x)$ is a 0-normal polynomial over $\mathbb{F}_q$ if and only if $a_1 \neq 0$.

Proof. Similarly, the proof of Corollary 4.1.17. □

Remark 4.1.19. Let $q = 2$ and $q^n - 1 = 2^n - 1$ is a prime. Then by Theorem 2.4.9, we have

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n$$

is a primitive normal polynomial over $\mathbb{F}_2$ if and only if $a_1 \neq 0$.

Example 4.1.20. Let $\mathbb{F}_{2^7} \cong \mathbb{F}_2[x]/(x^7+x+1)$ be the field constructed by irreducible polynomial x^7+x+1 in $\mathbb{F}_2[x]$ and let $\alpha = \overline{x}$ be a root of $f(x) = x^7+x+1$. For $\alpha \in \mathbb{F}_{2^7}$, we compute

$$\begin{aligned} Tr_{\mathbb{F}_{2^7}/\mathbb{F}_2}(\alpha) &= \alpha + \alpha^2 + \alpha^{2^2} + \alpha^{2^3} + \alpha^{2^4} + \alpha^{2^5} + \alpha^{2^6} \\ &= \alpha + \alpha^2 + \alpha^4 + (\alpha^2+\alpha) + (\alpha^4+\alpha^2) + (\alpha^4+\alpha^2+\alpha) + (\alpha^4+\alpha) \\ &= 0. \end{aligned}$$

By Theorem 4.1.15.(1), we get that α is a 1-normal element of $\mathbb{F}_{2^7}$ over $\mathbb{F}_2$. Similary, we consider $\alpha+1 \in \mathbb{F}_{2^7}$ and

$$\begin{aligned} Tr_{\mathbb{F}_{2^7}|\mathbb{F}_2}(\alpha+1) &= (\alpha+1) + (\alpha+1)^2 + (\alpha+1)^{2^2} + (\alpha+1)^{2^3} + (\alpha+1)^{2^4} + (\alpha+1)^{2^5} \\ &+ (\alpha+1)^{2^6} \\ &= (\alpha+1) + (\alpha^2+1) + (\alpha^4+1) + (\alpha^2+\alpha+1) + (\alpha^4+\alpha^2+1) \\ &+ (\alpha^4+\alpha^2+\alpha+1) + (\alpha^4+\alpha+1) \\ &= 1. \end{aligned}$$

By Theorem 4.1.15.(2), we obtain that is a 0-normal element of $\mathbb{F}_{2^7}$ over $\mathbb{F}_2$.

From the definition of k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, we have to consider

$$gcd(x^n-1, g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}).$$

The irreducibility of x^n-1 and $g_\alpha(x)$ is effect to k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. For $\alpha \in \mathbb{F}_q$ the ground field, α is a $(n-1)$-normal element. We next consider $\alpha \notin \mathbb{F}_q$. If $g_\alpha(x)$ is irreducible, then α is 0-normal over $\mathbb{F}_q$. If $g_\alpha(x)$ is reducible, then we will consider to factor x^n-1 for finding $gcd(x^n-1, g_\alpha(x))$. We note that

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

In next result, we use the irreducibility of polynomial $x^{n-1} + x^{n-2} + \cdots + x + 1$ as a condition for 1-normal elements.

Proposition 4.1.21. Let $\alpha \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q$. If $x^{n-1} + x^{n-2} + \cdots + x + 1$ is irreducible over $\mathbb{F}_q$ and $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$, then α is a 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Proof. Assume that $x^{n-1}+x^{n-2}+\cdots+x+1$ is irreducible over $\mathbb{F}_q$ and $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$. Note that $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}$. Since $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$, we have

$$g_\alpha(1) = \alpha(1)^{n-1} + \alpha^q(1)^{n-2} + \cdots + \alpha^{q^{n-1}} = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} = 0.$$

It follows that $(x-1) | g_\alpha(x)$. Since

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

and $x^{n-1} + x^{n-2} + \cdots + x + 1$ is irreducible over $\mathbb{F}_q$, we have

$$gcd(x^n - 1, \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}}) = x - 1.$$

Therefore $deg(gcd(x^n - 1, \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}})) = 1$. Hence $\alpha \in \mathbb{F}_q$ is a 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. □

Example 4.1.22. Let $\mathbb{F}_{3^5} \cong \mathbb{F}_3[x]/(x^5 + 2x + 2)$ be the field arised from irreducible polynomial $x^5 + 2x + 2$ over $\mathbb{F}_3$. Denote the residue class of x mod $x^5 + 2x + 2$ by α. We see that

$$\begin{aligned} Tr_{\mathbb{F}_{3^5}/\mathbb{F}_3}(\alpha) &= \alpha + \alpha^3 + \alpha^{3^3} + \alpha^{3^4} \\ &= (\alpha) + (\alpha^3) + (\alpha^4 + \alpha + 1) + (\alpha^4 + \alpha^2 + 1) + (\alpha^4 + 2\alpha^3 + 2\alpha^2 \\ &\quad + \alpha + 1) \\ &= 0 \end{aligned}$$

and the polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducile over $\mathbb{F}_3$. By Proposition 4.1.21, we obtain that α is a 1-normal element of $\mathbb{F}_{3^5}$ over $\mathbb{F}_3$.

4.2 Trace function criteria for k-normal polynomials constructed by q-cycles mod n

Let $\mathbb{F}_q$ be a finite field with q elements and n be a positive integer with q and n are relatively prime. Let $a_0, a_1, a_2, \ldots, a_{l-1}$ be l distinct numbers chosen from $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$. If

$$\begin{aligned} a_i q &\equiv a_{i+1} \pmod{n},\ i = 0, 1, 2, \ldots, l-2, \text{ and} \\ a_{l-1} q &\equiv a_0 \pmod{n}, \end{aligned}$$

then $(a_0, a_1, a_2, ..., a_{l-1})$ is called a q-cycle mod n of length l and its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a monic irreducible factor of $x^n - 1$ in $\mathbb{F}_q[x]$. Conversely, if $f(x)$ is a monic irreducible factor of $x^n - 1$ in $\mathbb{F}_q[x]$, then all roots of $f(x)$ are power of α whose exponents form a q-cycle mod n.

A monic irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is called a k-normal polynomial over $\mathbb{F}_q$ if its roots are the k-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

In this section, we give trace function criteria for k-normal polynomials (especially, 0, 1-normal polynomials), which are monic irreducible factors of $x^n - 1$ constructed by q-cycles mod n.

Proposition 4.2.1. Let $e \in \mathbb{N}$ and $n = 2^e + 1$. If the number of 2-cycles mod n is equal to 2, then $f(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$ is a 0-normal polynomial over $\mathbb{F}_2$.

Proof. Suppose that $(0), (1, 2, \ldots, n-1)$ are only 2-cycles mod n. Since $(1, 2, \ldots, n-1)$ is a 2-cycle mod n of length $n - 1 = 2^e$, which $n - 1$ is even, we have $1^{n-1} + 1^{n-2} + \cdots + 1^1 = 0$ in $\mathbb{F}_2$, so $(x - 1)|(x^{n-1} + x^{n-2} + \cdots + x^1)$. Thus

$$gcd(x^n - 1, x^{n-1} + x^{n-2} + \cdots + x) \neq 1.$$

Similarly, we known that $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$. Therefore

$$gcd(x^n - 1, x^{n-1} + x^{n-2} + \cdots + x + 1) \neq 1.$$

We see that $gcd(x^n - 1, x^{n-1} + x^{n-2} + \cdots + x + c) \neq 1$ for all $c \in \mathbb{F}_2$. By Proposition 2.7.5, we get that $x^{n-1} + x^{n-2} + \cdots + x + 1$ is irreducible over $\mathbb{F}_2$ where the coefficient of x^{n-2} is $1 \neq 0$. By Theorem 2.5.8, we have $x^{n-1} + x^{n-2} + \cdots + x + 1$ is a 0-normal polynomial over $\mathbb{F}_2$. □

Remark 4.2.2. We keep the notations as in Proposition 4.2.1. For $q = 2$ and $q^{n-1} - 1 = 2^{n-1} - 1$ is a prime and by Theorem 2.4.9, we have $x^{n-1} + x^{n-2} + \cdots + x + 1$ is a primitive normal polynomial over $\mathbb{F}_2$.

Example 4.2.3. For $q = 2$ and $n = 5 = 2^2 + 1$. By constructing of 2-cycles mod 5, we have $(0), (1, 2, 3, 4)$ are 2-cycles mod 5. Consequently, by Proposition 4.2.1 $f(x) = x^4 + x^3 + x^2 + x^1 + 1$ is a primitive 0-normal polynomial over $\mathbb{F}_2$.

Proposition 4.2.4. Let q be a power of prime and n be a positive integer with $gcd(q, n) = 1$. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exist primitive nth roots of unity in $\mathbb{F}_{q^m}$). Assume that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length l. Then its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a 0-normal polynomial over $\mathbb{F}_q$ if and only if $\{\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}}\}$ is linearly independent over $\mathbb{F}_q$.

Proof. Recall that $l|m$ and so $\mathbb{F}_{q^l}$ is a subfield of $\mathbb{F}_{q^m}$. By constructing of q-cycles, $\alpha^{a_0} = (\alpha^{a_0})^{q^l}$. By Corollary 2.1.22, $\alpha^{a_0} \in \mathbb{F}_{q^l}$. Assume that $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$ is a 0-normal polynomial over $\mathbb{F}_q$. Then $\{\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}}\}$ is a normal basis of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$. Therefore $\{\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}}\}$ is linearly independent over $\mathbb{F}_q$. □

Remark 4.2.5. We keep the notations as in Proposition 4.2.4. For $q = 2$ and $q^l - 1 = 2^l - 1$ is a prime and by Theorem 2.4.9, $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$ is a primitive normal polynomial over $\mathbb{F}_2$ if and only if $\{\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}}\}$ is linearly independent over $\mathbb{F}_2$.

Example 4.2.6. Factorize the polynomial $x^7 - 1$ into a product of irreducible polynomial over $\mathbb{F}_2$. Frist, partition the 7 numbers $0, 1, 2, 3, 4, 5, 6$ into 2-cycles mod 7. Then $(0), (1, 2, 4), (3, 6, 5)$ are 2-cycles mod 7 of length $1, 3$ and 3, respectively. The correspondence of each 2-cycle is a monic irreducible factor of $x^7 - 1$ over $\mathbb{F}_2$. The order of 2 in $\mathbb{Z}_7^*$ is $m = 3$. We choose $f(x) = x^3 + x + 1$ an irreducicle polynomial over $\mathbb{F}_2$ to construct the finite field $\mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3 + x + 1)$. Let $\alpha = \overline{x} \in \mathbb{F}_{2^3}$ be a root of $f(x)$. Thus α is a primitive 7th root of unity over $\mathbb{F}_2$. Then monic irreducible factors of $x^7 - 1$ over $\mathbb{F}_2$ are

$$\begin{aligned} f_0(x) &= (x - \alpha^0) \\ f_1(x) &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^4) \\ f_2(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^5). \end{aligned}$$

Thus the complete factorization of $x^7 - 1$ over $\mathbb{F}_2$ is

$$x^7 - 1 = f_0(x) f_1(x) f_2(x).$$

By considering $\alpha = \overline{x}$ as a root of $x^3 + x + 1$, we get the explicit terms of $f_0(x), f_1(x), f_2(x) \in \mathbb{F}_2[x]$.

$$\begin{aligned} f_0(x) &= x - 1 \\ f_1(x) &= x^3 + x + 1 \\ f_2(x) &= x^3 + x^2 + 1. \end{aligned}$$

First, for 2-cycle mod 7, (0), $f_0(x) = x - \alpha^0 = x - 1$. We known that $\{\alpha^0 = 1\}$ is linearly independent and it is a normal over $\mathbb{F}_2$. Then $f_0(x) = x - 1$ is

a 0-normal polynomial over $\mathbb{F}_2$.

Next, for 2-cycle mod 7, $(1, 2, 4)$, we get that

$$f_1(x) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1$$

and $\{\alpha, \alpha^2, \alpha^4 = \alpha^2 + \alpha\}$ is not linearly independent. By Proposition 4.2.4, $f_1(x)$ is not 0-normal polynomial over $\mathbb{F}_2$.

Note that the 2-cycle mod 7, $(3, 6, 5)$, has 3 as the leading element and its correspondence polynomial $f_2(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5)$. Consider the set $\{\alpha^3 = \alpha+1, \alpha^6 = \alpha^2+1, \alpha^5 = \alpha^2+\alpha+1\}$. We will show that $\{\alpha+1, \alpha^2+1, \alpha^2+\alpha+1\}$ is linearly independent over $\mathbb{F}_2$. Assume that $a, b, c \in \mathbb{F}_2$. Then

$$\begin{aligned} a(\alpha+1) + b(\alpha^2+1) + c(\alpha^2+\alpha+1) &= 0, \\ a\alpha + a + b\alpha^2 + b + c\alpha^2 + c\alpha + c &= 0, \\ (c+b)\alpha^2 + (a+c)\alpha + (a+b+c) &= 0, \\ a = b = c &= 0. \end{aligned}$$

Therefore $\{\alpha+1, \alpha^2+1, \alpha^2+\alpha+1\}$ is linearly independent over $\mathbb{F}_2$. By Theorem 4.2.4, $f(x)$ is a 0-normal polynomial over $\mathbb{F}_2$ and thus $f(x)$ is a primitive normal polynomial over $\mathbb{F}_2$.

Theorem 4.2.7. Let n be a positive integer such that $gcd(n, q) = 1$ where q is a power of prime p. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exist primitive nth roots of unity in $\mathbb{F}_{q^m}$). Assume that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length $l = p^e$ for some $e \in \mathbb{N}$. Then its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a 0-normal polynomial over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$.

Proof. Assume that $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$, where a_0 is the leading element of q-cycle mod n, $(a_0, a_1, \ldots, a_{l-1})$ of length $l = p^e$ for some $e \in \mathbb{N}$, by Theorem 2.7.2, we

have its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a monic irreducible factor of $x^n - 1$ in $\mathbb{F}_q[x]$. From Theorem 2.2.31, we get $\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}} \in \mathbb{F}_{q^l} \backslash \mathbb{F}_q$. Since dimension $l = p^e$ and $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$, α^{a_0} is a 0-normal element of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$ by Theorem 2.5.4, so all conjugates of α^{a_0} are 0-normal elements of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$ by Theorem 2.6.4. Therefore

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a 0-normal polynomial over $\mathbb{F}_q$. Conversely, let

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

be a 0-normal polynomial $\mathbb{F}_q$. Then its all roots of $f(x)$ are 0-normal elements of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$. By Theorem 2.5.4, hence $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$. □

Remark 4.2.8. We keep notations as in Theorem 4.2.7. For $q = 2$ and $q^l - 1 = 2^l - 1$ is a prime and by Theorem 2.4.9, $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$ is a primitive normal polynomial over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$.

Example 4.2.9. Factorize the polynomial $x^5 - 1$ over $\mathbb{F}_2$ into product of irreducible polynomial over $\mathbb{F}_2$. First, partition the 5 numbers $0, 1, 2, 3, 4$ into 2-cycles mod 5. Then (0) and $(1, 2, 3, 4)$ are 2-cycles mod 5 of length 1 and 4, respectively. For each of the 2-cycle, there is an irreducible factor of $x^5 - 1$ over $\mathbb{F}_2$. The order of 2 in $\mathbb{Z}_5^*$ is $m = 4$. We choose an irreducible polynomial $f(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$ to construct the finite field $\mathbb{F}_2[x]/(x^4 + x^3 + 1)$. Let $\alpha = \overline{x}$ be a root of $f(x)$. Then α is a primitive 5th root of unity over $\mathbb{F}_2$. Then monic irreducible factors of $x^5 - 1$ over $\mathbb{F}_2$ are

$$\begin{aligned} f_0(x) &= (x - \alpha^0) \\ f_1(x) &= (x - \alpha^1)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4). \end{aligned}$$

The complete factorization of $x^5 - 1$ over $\mathbb{F}_2$ is

$$x^5 - 1 = f_0(x)f_1(x),$$

and so

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

Since $Tr_{\mathbb{F}_{2^4}/\mathbb{F}_4}(\alpha) \neq 0$ and by Theorem 4.2.7, we have $f_1(x) = x^4 + x^3 + x^2 + x + 1$ is a 0-normal polynomial over $\mathbb{F}_q$.

Theorem 4.2.10. Let n be a positive integer such that $gcd(n, q) = 1$ where q is a power of prime p. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exist primitive nth roots of unity in $\mathbb{F}_{q^m}$). Assume that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length l where l is a prime different from p and q is a primitive element modulo l. Then its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a 0-normal polynomial over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$.

Proof. Let $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$. Since $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length l where l is a prime different from p and q is a primitive element modulo l and by Theorem 2.7.2, we have that its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a monic irreducible factor of $x^n - 1$ in $\mathbb{F}_q[x]$. From Theorem 2.2.31, we get that $\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}} \in \mathbb{F}_{q^l} \backslash \mathbb{F}_q$. Since l is a prime different from p and $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$, α^{a_0} is a 0-normal element of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$ by Theorem 2.5.5, so $\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}}$ are 0-normal elements of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$ by Theorem 2.6.4. Therefore its correspondence polynomial $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$ is a 0-normal polynomial over $\mathbb{F}_q$. Now, assume that $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$ is a 0-normal polynomial over $\mathbb{F}_q$. Then all its roots of $f(x)$ are 0-normal elements of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$. By Theorem 2.5.5, we get $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$. □

Remark 4.2.11. We keep notations as in Theorem 4.2.10. For $q^l - 1 = 2^l - 1$ is a prime and by Theorem 2.4.9, $f(x) = (x-\alpha^{a_0})(x-\alpha^{a_1})\cdots(x-\alpha^{a_{l-1}})$ is a primitive normal polynomial over $\mathbb{F}_2$ if and only if $Tr_{\mathbb{F}_{2^l}/\mathbb{F}_2}(\alpha^{a_0}) \neq 0$.

Theorem 4.2.12. Let n be a positive integer such that $gcd(n,q) = 1$ where q is a power of prime p. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exist primitive nth roots of unity in $\mathbb{F}_{q^m}$). Assume that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length $l = q^e - 1$ where e is a positive integer.

(1) $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$ if and only if its correspondence polynomial

$$f(x) = (x-\alpha^{a_0})(x-\alpha^{a_1})\cdots(x-\alpha^{a_{l-1}})$$

is a 0-normal polynomial over $\mathbb{F}_q$.

(2) $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) = 0$ if and only if its correspondence polynomial

$$f(x) = (x-\alpha^{a_0})(x-\alpha^{a_1})\cdots(x-\alpha^{a_{l-1}})$$

is a 1-normal polynomial over $\mathbb{F}_q$.

Proof. Let $(a_0, a_1, \ldots, a_{l-1})$ be a q-cycle mod n of length l where $l = q^e - 1$ for some e is positive integer. By Theorem 2.7.2, its correspondence polynomial

$$f(x) = (x-\alpha^{a_0})(x-\alpha^{a_1})\cdots(x-\alpha^{a_{l-1}})$$

is a monic irreducible factor of $x^n - 1$ in $\mathbb{F}_q[x]$. By Theorem 2.2.31, we get that $\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}} \in \mathbb{F}_{q^l} \backslash \mathbb{F}_q$.

(1) Assume that $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$. By Theorem 4.1.15.(2), we get that α^{a_0} is a 0-normal element of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$, so $\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}}$ are 0-normal elements of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$ by Theorem 2.6.4. Therefore its correspondence polynomial

$$f(x) = (x-\alpha^{a_0})(x-\alpha^{a_1})\cdots(x-\alpha^{a_{l-1}})$$

is a 0-normal polynomial $\mathbb{F}_q$. Now, we assume that

$$f(x) = (x-\alpha^{a_0})(x-\alpha^{a_1})\cdots(x-\alpha^{a_{l-1}})$$

is a 0-normal polynomial over $\mathbb{F}_q$. Then all its roots of $f(x)$ are 0-normal elements of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$. By Theorem 4.1.15.(2), we obtain $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$.

(2) Suppose that $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) = 0$. By Theorem 4.1.15.(1), we obtain that α^{a_0} is a 1-normal element of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$, so $\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}}$ are 1-normal elements of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$ by Theorem 2.6.4. Therefore its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a 1-normal polynomial over $\mathbb{F}_q$. Now, we suppose that

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a 1-normal polynomial over $\mathbb{F}_q$. Then all its roots of $f(x)$ are 1-normal elements of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$. By Theorem 4.1.15.(1), $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$. □

Example 4.2.13. For $q = 2, n = 7$, $(0), (1,2,4), (3,6,5)$ are 2-cycles mod 7 of length $1, 3$ and 3, respectively. In Example 4.2.6, we consider $\mathbb{F}_2[x]/(x^3 + x + 1)$ and $\alpha = \overline{x}$ is a root of $f(x)$. For 2-cycle mod 7, $(3,6,5)$, its correspondence polynomial is

$$f_2(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^5) = x^3 + x^2 + 1.$$

Consider the element $\alpha^3 = \alpha + 1$. We have

$$\begin{aligned} Tr_{\mathbb{F}_{2^3}/\mathbb{F}_3}(\alpha^3) &= \alpha^3 + (\alpha^3)^2 + (\alpha^3)^{2^2} \\ &= (\alpha + 1) + (\alpha^2 + 1) + (\alpha^2 + 1) \\ &= 1. \end{aligned}$$

From Theorem 4.2.10, we obtain that $f_2(x) = x^3 + x^2 + 1$ is a 0-normal polynomial over $\mathbb{F}_2$, that is, $f_2(x)$ is a primitive normal polynomial over $\mathbb{F}_2$. In the same way, the 2-cycle mod 7 of length $3 = 2^2 - 1$, $(1,2,4)$, its correspondence polynomial is

$$f_1(x) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1.$$

Consider the element α. We see that

$$\begin{aligned} Tr_{\mathbb{F}_{2^3}/\mathbb{F}_3}(\alpha) &= \alpha + \alpha^2 + \alpha^{2^2} \\ &= \alpha + \alpha^2 + \alpha^2 + \alpha \\ &= 0. \end{aligned}$$

From Theorem 4.2.12, we get that $f_1(x) = x^3 + x + 1$ is a 1-normal polynomial over $\mathbb{F}_2$.

Theorem 4.2.14. Let $\mathbb{F}_q$ be a finite field with q elements and n be a positive integer such that $gcd(q, n) = 1$. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exist primitive nth roots of unity in $\mathbb{F}_{q^m}$). Assume that (a_0, a_1) is a q-cycle mod n of length $l = 2$. Then $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1})$ is a 1 - normal polynomial over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha^{a_0}) = 0$.

Proof. Suppose that $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha^{a_0}) = 0$. Since (a_0, a_1) is a q-cycle mod n of length $l = 2$, by Theorem 2.7.2, we have $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1})$ is a monic irreducible factor of $x^n - 1$ in $\mathbb{F}_q[x]$. From Theorem 2.2.31, we get that $\alpha^{a_0}, \alpha^{a_1} \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. By assumption and Theorem 4.1.3, α^{a_0} is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, so α^{a_1} is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Therefore $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1})$ is a 1-normal polynomial over $\mathbb{F}_q$. Now, assume that $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1})$ is a 1-normal polynomial over $\mathbb{F}_q$. Then all its roots of $f(x)$ are 1-normal elements of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. By Theorem 4.1.3, we have $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha^{a_0}) = 0$. □

Example 4.2.15. Factorize the polynomial $x^8 - 1$ into a product of irreducible polynomial over $\mathbb{F}_3$. Frist, partition the 8 numbers $0, 1, 2, 3, 4, 5, 6, 7$ into 3-cycles mod 8. Then $(0), (1, 3), (2, 6), (4), (5, 7)$ with length $1, 2, 2, 1$ and 2, respectively. The correspondence of each 3-cycle mod 8 is an irreducible factor of $x^8 - 1$ over $\mathbb{F}_3$. From the order of 3 in $\mathbb{Z}_8^*$ is $m = 2$. We choose $f(x) = x^2 + x + 2$ an irreducicle polynomial over $\mathbb{F}_3$ and consider the finite field $\mathbb{F}_{3^2} \cong \mathbb{F}_3[x]/(x^2 + x + 2)$. Let $\alpha = \overline{x}$ be a root of $f(x)$. Thus α is a primitive 8th root of unity over $\mathbb{F}_2$. Then monic

irreducible factors of $x^8 - 1$ over $\mathbb{F}_3$ are

$$\begin{aligned} f_0(x) &= (x - \alpha^0) \\ f_1(x) &= (x - \alpha^1)(x - \alpha^3) \\ f_2(x) &= (x - \alpha^2)(x - \alpha^6) \\ f_3(x) &= (x - \alpha^4) \\ f_4(x) &= (x - \alpha^5)(x - \alpha^7). \end{aligned}$$

Then we have the complete factorization of $x^8 - 1$ over $\mathbb{F}_3$

$$x^8 - 1 = f_0(x)f_1(x)f_2(x)f_3(x)f_4(x).$$

To express $f_0(x), f_1(x), f_2(x), f_3(x), f_4(x)$ as polynomial with coeffcients in $\mathbb{F}_2$, we use $\alpha = \overline{x}$ as a root of $x^2 + x + 2$. Then

$$\begin{aligned} f_0(x) &= x - 1 \\ f_1(x) &= x^2 + 2x + 2 \\ f_2(x) &= x^2 + 1 \\ f_3(x) &= x + 1 \\ f_4(x) &= x^2 + x + 2. \end{aligned}$$

For the 3-cycle mod 8, $(2, 6)$, its correspondence polynomial is

$$f_2(x) = (x - \alpha^2)(x - \alpha^6) = x^2 + 1.$$

Consider

$$\begin{aligned} Tr_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha^2) &= \alpha^2 + (\alpha^2)^3 \\ &= (2\alpha + 1) + (\alpha + 2) = 0. \end{aligned}$$

By theorem 4.2.14, we get that $f_2(x) = x^2 + 1$ is a 1-normal polynomial over $\mathbb{F}_3$.

CHAPTER VI

CONCLUSIONS

In this chapter, we conclude all main results that we found in this research.

1. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exists a primitive nth root of unity in $\mathbb{F}_{q^m}$). Suppose that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length l and $ord(\alpha) = q^l - 1$. Then its correspondence polynomial $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$ is a primitive polynomial over $\mathbb{F}_q$ if and only if $gcd(a_0, q^l - 1) = 1$.

2. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exists a primitive nth root of unity in $\mathbb{F}_{q^m}$). Suppose that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length l and $ord(\alpha) = q^l - 1$. Then we have if $q^l - 1$ is a prime number where $q = 2$, then its correspondence polynomial $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$ is primitive over $\mathbb{F}_2$.

3. Let $\alpha \in \mathbb{F}_{q^2}^*$. If 1 is the unique root in $\mathbb{F}_{q^2}$ of $g_\alpha(x)$, then α is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

4. Let $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Then $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = 0$ if and only if α is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

5. Let $\alpha, \beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. If α and β are 1-normal elements of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ with $\alpha + \beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, then $\alpha + \beta$ is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

6. Let $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. If α is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, then α^{-1} is a 1-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

7. Let $\alpha, \beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. If α and β are 0-normal elements of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ with $\alpha + \beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ and $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta) \neq 0$ in $\mathbb{F}_q$, then $\alpha + \beta$ is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

8. Let $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. If α is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, then α^{-1} is a 0-normal element of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$.

9. Let $n = q^m - 1$ where m is a positive integer and $\alpha \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q$. Then

(1) α is a 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$.

(2) α is a 0-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$.

10. Let $n = q^m - 1$ where m is a positive integer and $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ be an irreducible polynomial over $\mathbb{F}_q$. Then $f(x)$ is a 1-normal polynomial over $\mathbb{F}_q$ if and only if $a_1 = 0$.

11. Let $n = q^m - 1$ where m is a positive integer and $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ be an irreducible polynomial over $\mathbb{F}_q$. Then $f(x)$ is a 0-normal polynomial over $\mathbb{F}_q$ if and only if $a_1 \neq 0$.

12. Let $\alpha \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q$. If $x^{n-1} + x^{n-2} + \cdots + x + 1$ is irreducible over $\mathbb{F}_q$ and $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$, then α is a 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

13. Let $e \in \mathbb{N}$ and $n = 2^e + 1$. If the number of 2-cycles mod n is equal to 2, then $f(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$ is a 0-normal polynomial over $\mathbb{F}_2$.

14. Let q be a power of prime and n be a positive integer with $gcd(q, n) = 1$. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exist primitive nth roots of unity in $\mathbb{F}_{q^m}$). Assume that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length l. Then its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a 0-normal polynomial over $\mathbb{F}_q$ if and only if $\{\alpha^{a_0}, \alpha^{a_1}, \ldots, \alpha^{a_{l-1}}\}$ is linearly independent over $\mathbb{F}_q$.

15. Let n be a positive integer such that $gcd(n, q) = 1$ where q is a power of prime p. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exist primitive nth roots of unity in $\mathbb{F}_{q^m}$). Assume that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length $l = p^e$ for some $e \in \mathbb{N}$. Then its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a 0-normal polynomial over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$.

16. Let n be a positive integer such that $gcd(n, q) = 1$ where q is a power of prime p. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exist primitive nth roots of unity in $\mathbb{F}_{q^m}$). Assume that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length l where l is a prime different from p and q is a primitive element modulo l. Then its correspondence polynomial $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$ is a 0-normal polynomial over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$.

17. Let n be a positive integer such that $gcd(n, q) = 1$ where q is a power of prime p. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exist primitive nth roots of unity in $\mathbb{F}_{q^m}$). Assume that $(a_0, a_1, \ldots, a_{l-1})$ is a q-cycle mod n of length $l = q^e - 1$ where e is a positive integer.

(1) $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) \neq 0$ if and only if its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a 0-normal polynomial over $\mathbb{F}_q$.

(2) $Tr_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha^{a_0}) = 0$ if and only if its correspondence polynomial

$$f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{l-1}})$$

is a 1-normal polynomial over $\mathbb{F}_q$.

18. Let $\mathbb{F}_q$ be a finite field with q elements and n be a positive integer such that $gcd(q,n) = 1$. Let α be a primitive nth root of unity (if the order of q in $\mathbb{Z}_n^*$ is m, then there exist primitive nth roots of unity in $\mathbb{F}_{q^m}$). Assume that (a_0, a_1) is a q-cycle mod n of length $l = 2$. Then $f(x) = (x - \alpha^{a_0})(x - \alpha^{a_1})$ is a 1 - normal polynomial over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha^{a_0}) = 0$.

REFERENCES

REFERENCES

[1] Blake, I., Gao, X.H., Mullin, R.C., Vanstone, S.A., & Yaghoobian, T. (1993). *Applications of finite fields.* Boston, Dordrecht, Lancaster: Kluwer Academic Publishers.

[2] Lenstra, H.W., & Schoof, R.J. (1987). Primitive normal bases for finite fields. *Mathematics of Computation, 48*(17), 217-231.

[3] Carlitz, L. (1952). Primitive roots in finite fields. *Transactions of the American Mathematical Society, 73*, 373-382.

[4] Cohen, S. D. (2008). Gauss sums and a sieve for generators of galois fields. *Publicationes Mathematicae Debrecen, 56*, 293-312.

[5] Cohen, S. D., & Hachenberger, D. (2000). Primitivity freeness norm and trace. *Discrete Mathematics, 214*, 135-144.

[6] Cohen, S. D. (2003). The orders of related elements of a finite field. *The Ramanujan Journal, 7*, 196-183.

[7] Cohen, S. D. (2006). Primitive polynomials with a prescribed coefficient. *Finite Fields and Their Applications, 12*, 425-491.

[8] Cohen, S. D. (2012). Primitive cubics and quartics with zero trace and prescribed norm. *Finite Fields and Their Applications, 18*, 1156-1168.

[9] Fitzgerald, R. W. (2003). A characterization of primitive polynomials over finite fields. *Finite Fields and Their Applications, 9*, 117-121.

[10] Friedberg, S. H., Insel, A.J., & Specnce ,L.E. (2017). *Linear algebra.* Cambridge: Prentice Hall.

[11] Galois, E. (1830). Sur la theéorie des nombres. *Bulletin des Sciences Mathématiques, physiques et chimiques, 13*, 428-435.

[12] Hensel, K. (1888). *Über* die darstellung der zahlen eines gattungsbereiches für einen beliebigen primdivisor. *Journal Für Die Reine und Angewandte Mathematik, 103*, 230-237.

[13] Huczynska, S., Mullen, G.L., Panario, D., & David, T. (2013). Existence and properties of k - normal elements over finite fields. *Finite Fields and Their Applications, 24*, 170-183.

[14] Jungnickle, D., & Vanstone, S. A. (1989). On primitive polynomials over finite fields. *Journal of Algebra, 2*(124), 337-353.

[15] Laohakosol, V., & Pintoptant, U. (2008). A modification of Fitzgerald's characterization of primitive polynomials over finite fields. *Finite Fields and Their Applications, 14*, 85-91.

[16] Liao, Q. Y., Keli, P., & Jiyou, Li. (2016). On the existence for some special primitive elements in finite fields. *Chinese Annals of Mathematics, 37B*(2), 259-266.

[17] Lidl, R., & Niederreiter, H. (1997). *Finite fields, volume 20 of encyclopedia of mathematics and its applications.* Cambridge: Cambridge University.

[18] Moreno, O. (1982). On primitive elements of trace equal to 1 in $GF(2^m)$. *Discrete Mathematics, 41*, 53-56.

[19] Pintoptang, U., Tadee, S., & Laohakosol, V. (2014). The concept of q-cycle and applications. *International Journal of Discrete Mathematics, Art., 823567*, 9.

[20] Thomas, W. H. (1997). *Abstract algebra, an introduction*(2nd ed.). United States of America: Cengage Learning.

[21] Wan, Z.X. (2012). *Finte fields and galois rings.* Singapore: World Scientific.

[22] Wang, P., Cao, X., & Feng, R. (2012). On the existence of some speciffic elements in finite fields of characteristic 2. *Finite Fields and Their Applications, 18*(4), 800-813.