Faculty Of Graduate Studies

Mathematics Program

Codes Over Rings

Prepared by
Zainab Abd Alraof

Supervised by
Prof. Mohammad Saleh

M. Sc. Thesis
Birzeit University
Palestine

2016

Codes Over Rings

by
Zainab Abd Alraof Hussain Wahdan

Supervisor
Profesor Mohammad Saleh

Thesis submitted in coding theory of the degree of Master in Mathematics department

At
The faculty of Science
Birzeit University
2016.

Codes Over Rings

Prepared by:
Zainab Wahdan

This thesis was defended successfully on Jun , 4, 2016. And approved by:

Committee members:

1. **Prof. Mohammad Saleh** Head of committee ....
2. **Dr. Hasan Yousef** Internal Examiner ....
3. **Dr. Khaled Al-Takhman** Internal Examiner ....

DEDICATIONS

To the sun of Islam that will never set
To the Prophet Muhammad (pbuh) who is inevitably eminent.

To my teachers and supervisor Professor Muhammad Saleh
For his mentorship and guidance throughout the period of my thesis.

To my great parents
For inspiring me to pursue my higher studies.

To my husband Mahmoud Al-bzour
For his endless care, and encouragement .

To my brother Mouath Wahdan for his valuable counsel through my thesis work.
To my brothers, sisters, and all my family for their support and patience.

ACKNOWLEDGMENTS

First and above all, I thank our God "*Allah*", for reconciling me to the right way which guiding me to this research.

I would thank my Professor Muhammad Saleh for his care, help, and support.

I want also to send my warm and Sincere to my parents, my husband, my sisters and brothers, my family.

Heartiest thanks for my friends, especially my close friends.

Finally, I send my greetings to my teachers, colleagues, department, faculty, and my universities "*BZU*" and "*PTUK*".

Declaration

I certify that this thesis, submitted for the degree of Master of Mathematics to the Department of Mathematics at Birzeit University, is of my own research except where otherwise acknowledged, and that this thesis (or any part of it) has not been submitted for a higher degree to any other university or institution.

Zainab Wahdan
Signature . . . .

Abstract

This humble project aims to study cyclic codes over different Rings. We started our thesis work by providing some basics of coding theory.Afterwards, we Studied codes over the commutative rings Z_4, Z_{p^n}, and finite chain rings. Lastly, we moved towards codes over noncommutative rings.

Keywords:

cyclic codes, Dual code, principal ideal.

الملخص

يهدف هذا المشروع المتواضع لدراسة الترميز على الحلقات الدائرية المختلفة , بدانا بتقديم بعض اساسيات نظرية الترميز, وبعد ذلك درسنا التراميز على الحلقات التبديليه, "Z_4, Z_p^n" .

وفي النهاية انتقلنا الى دراسة التراميز علي الحلقات غير التبديلة .

الكلمات البحث: .cyclic codes, Dual code, principal ideal.

Contents

0.1 Introduction

Codes over rings has experienced tremendous growth since its inception. Progress has been attended in the direction of determining the structural properties of codes over large families of rings.

The study of linear codes over rings was started in 1970 with the investigation of analogs of cyclic codes over integer residue rings in [4], [5], and later on codes over Z_4 was studied in [6], [30], and [34]. The results over Z_4 generalised to Z_{p^m} by Pleas, Qian, Sole and Pramod, and Lopez.

Norton and Salagean extended the structure theorem given in [8], and [23], to cyclic codes over finite chain rings. That paper provided approach which did not require commutative algebra.

In the past few years linear codes over noncommutative rings have received much attention in [24], [10], and [1].

Only to be clear, most of this thesis work is not new. All what we are trying to do is to study what has been done so far and review it in our new way. Hopefully, we could add something with this promising future.

In the first chapter we illustrated introductory material, including basic definitions, facts and theorems in Abstract Algebra and coding Theory that form the building blocks of thesis.

In the second chapter we studied the structure of the cyclic codes. In the third (fourth) chapters we studied the generator matrices for a cyclic code C over the ring Z_4 (Z_{p^n}), the ideals of $Z_4(x)/(f(x))$ $(Z_{p^n}(x)/(f(x)))$, where $f(x)$ is an irreducible factor of $x^n - 1$ and then use these ideals to know the ideals of $Z_4(x)/(x^n - 1)$ $(Z_{p^n}(x)/(x^n - 1))$. Finally, we studed the dual code for the code C.

In the fifth chapter the generalization of the method of chapters [3] and [4] has been studied to obtain cyclic and self dual cyclic codes over finite chain rings with the condition that the length of the code is not divisible by the characteristic of the residue field .

Finally, in the last chapter Cyclic linear codes over arbitrary (not necessarily commutative finite rings) has been investigated and prove that the characterizations in previous chapters to be true for a large class of such codes over these rings.

Notations

Symbol	**definition**
Z_n	The ring of integers modulo n
F_{p^m}	Finite field with p^m elements.
$C[n,k]$	A linear code C over F_{p^m} with length n and dimension k.
$d(C)$	The destance of the code.
$C[n,k,d]$	linear code C over F_{p^m} with length n dimension k and distance $d(C) = d$
$f^*(x)$	The reciprocal polynomial of f(x).
G	Generator matrix for the code C.
H	Parity check matrix for the code C.
$C^{\perp}$	Dual code, the code generated by the parity check matrix.
$Rad(R)$	The radical of the ring R.
$\sum_2(n)$	The permutation $w \to$ 2w (mod n).
$M_n(R)$	Matrix ring, the set of all n by n matrix with element from the ring R.
Z_mC_n	A group ring where C_n is cyclic group generated by g.

Chapter 1

Basics and Preliminaries

This chapter covers the main basic concepts, definitions and theorems from abstract algebra, and coding theory that are used in the following chapters . The proofs of theorems, lemmas and corollaries in this chapter can be found in the references as specified.

1.1 Background of Algebra

Definition 1. *[18] Let R be a ring. A (left)* ***R module*** *is an additive abelian group M together with a function $\theta : R \times M \longrightarrow M$ such that $\theta(r, m) = rm$ for all $r, s \in R$ and $m, m_1, m_2 \in M$:*

1. $r(m_1 + m_2) = rm_1 + rm_2$.
2. $(r + s)m = rm + sm$.
3. $r(sm) = (rs)m$.

If in addition $1m = m$ for all $m \in M$ (1 is the identity element of R), then M is said to be a unitary R module. A right R module is defined similarly via a function $\theta : M \times R \longrightarrow M$ such that $\theta(m, r) = mr$ and satisfying the obvious analogues of $1, 2, 3$.

Definition 2. *[4] The **group ring** RG of a ring R and finite group G is the set of formal sums*

$$\sum_i r_i g^i,$$

$r_i \in R, g^i \in G$ with addition, scalar multiplication and ordinary multiplication defined by

$$\sum_i r_i g^i + \sum_i \acute{r_i} g^i = \sum_i (r_i + \acute{r_i}) g^i$$

$r_i, \acute{r_i} \in R, g^i \in G$

$$r \sum_i r_i g^i = \sum_i (r r_i) g^i,$$

$$(\sum_i r_i g^i).(\sum_j \acute{r_j} g^j) = \sum_i \sum_j r_i \acute{r_j} g^{i+j}$$

Definition 3. *[35] Let R be a commutative ring. A nonempty subset I of R is called an **ideal** if*

- *$a + b$ belong to I, for all $a, b \in I$.*
- *$r.a \in I$, for all $r \in R$ and $a \in I$.*

Definition 4. *[14] Let I be an ideal. We say that I is **maximal** if for every ideal J ,such that $I \subseteq J$, either $J = I$ or $J = R$.*

Definition 5. *[14] Let R be a ring with 1. An element u of R is a **unit** if there is an element $b \in R$ such that $u.b = b.u = 1$.*
*The elemant b is called **multiplicative inverse**.*
*An element a of R is a **zero divisor** if $a \neq 0$ and there is an element $b \in R$, $b \neq 0$ such that $a.b = 0$ or $b.a = 0$.*

Theorem 1.1.1. *[13] Let R be a ring with 1. An element of R cannot be both a unit and zero divisor.*

Theorem 1.1.2. *[13] Let $U(R)$ denotes the units of R, for any $m \geq 2$,*

$$U(Z_m) = U(m) := \{a \in \{1, 2, \cdots, m-1\} : gcd(a, m) = 1\}$$

Definition 6. *[7] The intersection of all maximal ideals of a commutative ring R is called the* ***radical*** *of R, the intersection of all prime ideals of a ring R is called the* ***prime radical*** *of R.*

Definition 7. *[2] A* ***local*** *ring is a ring R that contains a single maximal ideal.*

One property of a local ring R is that the subset $R-m$ is precisely the set of ring units, where m is the maximal ideal. This follows because, in a ring, any nonunit belongs to at least one maximal ideal.

Theorem 1.1.3. *[29] For every finite field F There exists a prime p and positive integer m, such that F has p^m element.*

Definition 8. *[38] The* ***order*** *of a field is the number of elements in the field. If the order is infinite, we call the field* ***an infinite field****.*
And if the order is finite, we call the field a finite field or a ***Galois field****.*

Definition 9. *[38] A finite field with p^m elements is called a Galois field of order p^m and is denoted by F_{p^m} .*

Theorem 1.1.4. *[38] For any prime p and any positive integer m, there exists a finite field, unique up to isomorphism, with p^m elements.*

Lemma 1. *[31] For every element α of a finite field F with p^m elements, we have $\alpha^{p^m} = \alpha$.*

Definition 10. *[38] The order of a nonzero element $\alpha \in F_{p^m}$, denoted by $ord(\alpha)$ or $|\alpha|$ is the smallest positive integer k such that $\alpha^k = 1$.*

Definition 11. *[38] (Primitive Root of Unity) An element α of a field is an n^{th} root of unity if $\alpha^n = 1$, $n = p^m - 1$. It is a primitive n^{th} root of unity if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$.*

An element α in a finite field F_{p^m} is called a primitive element (or a generator) of F_{p^m} if $F_{p^m} = \{0, \alpha, \alpha^2, \cdots, \alpha^{p^m-1}\}$.

Theorem 1.1.5. *[31] The elements of F_{p^m} are precisely the roots of the polynomial $x^{p^m} - x$.*

Definition 12. *[38] Let F be a field and let $K \subseteq F$ be a subring. Then we say K is a subfield of F if K is a field. In this case we also call F an extension field of K and abbreviate this by saying F/K is a field extension.*

Example 1. *The complex numbers is an extension field of both Q and R which is an extension field for Q also.*

Theorem 1.1.6. *[38] Let K be a field and let $f(x) \in K[x]$ be a nonconstant polynomial. Then there exist an extension F of K and $\alpha \in F$ such that $f(\alpha) = 0$.*

Theorem 1.1.7. *[20] For every finite field F_{p^m} the multiplicative group ${F_{p^m}}^*$ of nonzero elements of F_{p^m} is cyclic.*

Theorem 1.1.8. *[30](The fundamental theorem of finite abelian groups) Every finite abelian group G can be expressed as the direct sum of cyclic subgroups of prime power order.*

Definition 13. *[30]Let F be a field. A polynomial $f(x) \in F[x]$ is said to an associate of another polynomial $g(x) \in F[x]$ if*

$$f(x) = cg(x).$$

for some nonzero $c \in F$.

Definition 14. *[3] The ring $R_k = F_{p^m} + uF_{p^m} + u^2F_{p^m} + ... + u^{k-1}F_{p^m}$, where $u^k = 0$ is a commutative chain ring of p^{mk} elements with maximal ideal uR_k Since u is nilpotent with nilpotent index k we have*

$$0 = u^kR_k \subset ... \subset u^2R_k \subset uR_k \subset R_k$$

Moreover $R_k/uR_k \cong F_{p^m}$ is the residue field and

$$|u^iR_k| = p^m|u^{i+1}R_k| = p^{mk-i} \quad ,0 \leq i \leq k-1.$$

Denote $R_1 = F_{p^m}$, $R_2 = F_{p^m} + uF_{p^m}$, $R_3 = F_{p^m} + uF_{p^m} + u^2F_{p^m}$,..., $R_k = F_{p^m} + uF_{p^m} + u^2F_{p^m} + ... + u^{k-1}F_{p^m}$.

1.2 Background of Coding Theory

Let F_{p^m} be the finite field with p^m elements and $(F_{p^m})^n$ be the linear space of all n tuples over F_{p^m}, i.e.,its elements are row vectors.

Definition 15. *[11] Let $k, n \in N$ such that $1 \leq k \leq n$.* ***A linear code*** *C is a k dimensional vector subspace of $(F_{p^m})^n$. We say that C is a linear code over F_{p^m} with length n and dimension k. An element of C is called a word of C*

We denote the linear code C over F_{p^m} with length n and dimension k dy C [n, k] code.

Definition 16. *[11] The Hamming* ***distance*** *$d(u, v)$ between two vectors $u, v \in (F_{p^m})^n$ is the number of coordinates in which u and v differ.*

Example 2. *let u=(110111), v=(101011) be 2 vectors over F_3 then, $d(u, v) = 3$*

Definition 17. *[11] The Hamming* ***weight*** *of a vector $u \in (F_{p^m})^n$ $w(u)$, is the number of its nonzero coordinates, i.e. $w(u) = d(u, 0)$.*

Definition 18. *[11] The* ***distance of a code*** *C is the smallest distance between distinct words:*

$$d(C) = min\{d(c_i, c_j)|c_i, c_j \in C, c_i \neq c_j\}.$$

Theorem 1.2.1. *[11] If C is a linear code, the distance $d(C)$ is the same as the minimum weight of nonzero words: $d(C) = min\{w(c)|c \in C, c \neq 0\}$.*

Proof. $d(u, v) = d(0, u - v) = w(u - v)$, where $u - v \in C$

$$d(C) = min\{d(u, v), u \neq v, u, v \in C\} = min\{w(u - v), u \neq v, u, v \in C\}$$

$$d(C) = min\{w(x) : x \in C\}$$

□

If we know the distance $d(C)$ of an $[n,k]$ code, then we can refer to the code as an $[n,k,d]$ code.

Definition 19. *[11] An $[n,k,d]$ linear code C is **cyclic** if the cyclic shift of a word is also a word, i.e. If $(c_0,...,c_{n-1}) \in C$, then $(c_{n-1},c_0,...,c_{n-2}) \in C$.*

Definition 20. *[6] A linear code of length n over a commutative ring R is **constacyclic** if for some unit $a \in R$, the code is invariant under the automorphism*

$$(c_0,c_1,\cdots,c_{n-1}) \longrightarrow (ac_{n-1},c_0,\cdots,c_{n-2}).$$

In the case $a = 1$, the code is cyclic.

To describe algebraic properties of cyclic codes, we need to introduce the following structure.We construct a bijective correspondence between the vectors of $(F_{p^m})^n$ and the residue classes of polynomials in the ring $F_{p^m}[x]/(x^n-1)$: $v = (v_0,...,v_{n-1}) \leftrightarrow v_0 + v_1x + \ + v_{n-1}x_{n-1}$. We can view linear codes as subsets of the ring $F_{p^m}[x]/(x^n-1)$.
The following theorem points out the algebraic structure of cyclic codes.

Theorem 1.2.2. *[11] Let C be an $[n,k,d]$ code, then C is cyclic if and only if C is an ideal of $F_{p^m}[x]/(x^n-1)$.*

Proof. Multiplying by x modulo x^n-1 corresponds to a cyclic shift:
$(c_0,c_1,...,c_{n-1})$ then $(c_{n-1},c_0,...,c_{n-2})$
$x(c_0 + c_1x + \ + c_{n-1}x_{n-1}) = c_{n-1} + c_0x + \ + c_{n-2}x_{n-2}$. $\square$

Definition 21. *[31] A **generator matrix** for an $[n,k]$ code C is any $k \times n$ matrix G whose rows form a basis for C.*

Example 3. *Consider the linear code C over Z_4, with the generating matrix*

$$G = \begin{bmatrix} 1 & 0 & 0 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 2 & 0 \end{bmatrix}.$$

Since G has 3 rows then the dimension of C is three, and $C[6,3]$ has 4^3 codewords.

In general there are many generator matrices for a code. For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an information set for C. The remaining $r = n - k$ coordinates are termed a redundancy set and r is called the redundancy of C.

Definition 22. *[31] The* ***parity check matrix*** *for the $[n, k]$ code C, defined by*

$$C = \{x \in F_q^n : Hx^T = 0\}.$$

The code C is the kernel of the linear transformation $L : x \to Hx^T$, the matrix H is $(n-k) \times n$ matrix .

Note that the rows of H will also be independent. In general, there are also several possible parity check matrices for C. The next theorem gives one of them when C has a generator matrix in standard form.

Theorem 1.2.3. *[31] If $G = [I_k|A]$ is a generator matrix for the $[n, k]$ code C in standard form, then $H = [-A^T|I_{n-k}]$ is a parity check matrix for C.*

Proof. We clearly have

$$HG^T = -A^T + A^T = O.$$

Thus C is contained in the kernel of the linear transformation $x \mapsto Hx^T$. As H has rank $n - k$, this linear transformation has kernel of dimension k, which is also the dimension of C. The result follows. □

The generator matrix G of an $[n, k]$ code C is simply a matrix whose rows are independent and span the code.

Definition 23. *[31] The rows of the parity check matrix H are independent, hence H is the generator matrix of some code, called the* ***dual*** *or orthogonal of C and denoted $C^\perp$. Notice that $C^\perp$ is an $[n, n-k]$ code. An alternate way to define the dual code is by using inner products.*

Since the ordinary inner product of vectors $x = x_1 \cdots x_n$, $y = y_1 \cdots y_n in$ F_q^n is $x.y = \sum_1^n x_i y_i$.
Therefore, we see that $C^\perp$ can also be defined by

$$C^\perp = \{x \in F_q^n : x.c = 0 \quad for \quad all \quad c \in C\}$$

The generator polynomial for $C^\perp$ can be obtained from the generator polynomial C. To find these, we introduce the concept of the reciprocal polynomial . Let $f(x) = f_0 + f_1 x + ... + f_a x^a$ be a polynomial of degree a in $F_q[x]$. The reciprocal polynomial of $f(x)$ is the polynomial $f^*(x) = x^a f(x^1) = f_a + f_{a1} x + ... + f_0 x^a$. So $f^*(x)$ has coefficients the reverse of those of $f(x)$.

Example 4. *Consider the code $C[6,3]$ over Z_3 generated by*

$$G = \begin{bmatrix} 1 & 0 & 0 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 2 & 0 \end{bmatrix}.$$

Then

$$H = \begin{bmatrix} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Definition 24. *[23] A code is **self orthogonal** if $C \subseteq C^\perp$. A code is **self dual** if $C = C^\perp$.*

Theorem 1.2.4. *[31] Let $a = (a_0, a_1, ..., a_{n1})$ and $b = (b_0, b_1, ..., b_{n1})$ be vectors in $F_{p^m}^n$ with associated polynomials $a(x)$ and $b(x)$. Then a is orthogonal to b and all its shifts if and only if $a(x)b^*(x) = 0$ in R_n.*

Definition 25. *[29] The **characteristic** of the ring is the smallest positive integer n such that*

$$\underbrace{1 + ... + 1}_{n \quad times} = 0$$

if n exist , and Zero otherwise.

Definition 26. *[13] a **matrix ring** is any collection of matrices over some ring R that form a ring under matrix addition and matrix multiplication.*

Definition 27. *[13] The set of all $n \times n$ matrices over an arbitrary ring R, denoted $M_n(R)$ usually referred to as the* ***"full ring of n-by-n matrices"****.*

Definition 28. *[22]* ***division ring****, is a ring in which division is possible. Specifically, it is a nonzero ring in which every nonzero element a has a multiplicative inverse.*

Division rings differ from fields only in that their multiplication is not required to be commutative.

Lemma 2. *[9] If R is a principal ideal domain, then every right ideal of the full matrix ring $M_n(R)$ is principal.*

Definition 29. *[38] A module is called* ***Artinian (Noetherian)*** *if every nonempty set of submodules has a minimal (maximal) element. This is the same as saying that every descending (ascending) sequence of submodules becomes ultimately stationary.*

Theorem 1.2.5. *[38] A module is called Artinian (Noetherian) if and only if every descending (ascending) sequence of submodules becomes ultimately stationary.*

Proof. suppose A is Noetherian, and let $A_1 \subset A_2 \subset ...$ be an ascending sequence of submodules of A. This sequence must have a maximal element A_n, hence

$$A_n = A_{n+1} = ...$$

Conversely, assume every ascending sequence of submodules of A becomes ultimately stationary. Consider any nonempty set of submodules of A and suppose this set has no maximal element. Take any element A_l in the set, since A_l is not maximal, A_l is properly contained in an element A_2 of the set, etc. Thus we get an infinite ascending sequence $A_1 \subset A_2 \subset ....$ contrary to assumption. □

Lemma 3. *[21] Let A be a semisimple ring.*
(i) A is a direct sum of finitely many simple submodules.
(ii) A is artinian and noetherian.

Lemma 4. *[14] Let F be a field. Then $F[x]$ is a principal ideal domain.*

Lemma 5. *[[33],23.7] If R is a finite ring, then for any module ${}_RM$, $Rad_R(M) = Rad(R)M$*

Theorem 1.2.6. *[19](ArtinWedderburns theorem) Any simple left or right Artinian ring is isomorphic to an $n_i \times n_i$ matrix ring over a division ring D, where both n and D are uniquely determined.*

Corollary 1. *[19] every simple ring that is finite dimensional over a division ring is a matrix ring. This is Joseph Wedderburn's original result.*

Theorem 1.2.7. *[17] The group ring RG is semisimple if and only if*

- *R is semisimple group*
- *G is finite*
- *the order of G is a unit in R*

Lemma 6 ([7],Theorem 4.2.3)**.** *Let R be a right Noetherian (Artinian) ring. Then any finitely generated right R module is again Noetherian (Artinian).*

Example 5. *Every finite ring is left and right Artinian.*

Lemma 7 ([7],Theorem 5.3.5)**.** *In any left (or right) Artinian ring R, R is semisimple if and only if it has no nilpotent ideals other than zero.*

Definition 30. *[30] Two codes C_1 and C_2 both of length n are said to be* ***equivalent****, if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates.*

Example 6. *The quaternary linear codes generated by $\begin{pmatrix} 1 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 3 \end{pmatrix}$ are equivalent.*

Definition 31. *[30] Codes differ only by a permutation of coordinates are said to be* ***permutation equivalent****.*

Example 7. *The quaternary linear codes generated by*

$$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, and \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$$

are permutation equivalent.

Definition 32. *[39] The* ***automorphism group*** *$Aut(C)$ of a code C is the group generated by all permutations and sign changes of the coordinates that preserve the set of codewords of C.*

1.3 Galois Ring

Galois rings are finite rings isomorphic to quotient rings $Z_{p^k}[x]/(f)$ where p is a prime and f is a monic polynomial such that $f(mod p)$ is an irreducible polynomial with coefficients in $GF(p)$.

Let $GR(p^k, m)$ denote the Galois ring $Z_{p^k}[x]/f(x)$ where f is monic basic irreducible polynomial over Z_{p^k} of degree m

The elements of $Z_{p^k}[x]/f(x)$ are residue classes of the form

$$a_0 + a_1 x + ... + a_{m-1}x^{m-1} + (f(x)), \quad a_i \in Z_{p^k}.$$

If we write $\zeta = x + f(x)$, then $f(\zeta) = 0$ and every element in $GR(p^k, m)$ can be expressed uniquely in the form

$$a_0 + a_1\zeta + ... + a_{m-1}\zeta^{m-1}, \quad a_i \in Z_{p^k}.$$

The set $T = \{0, \zeta, ..., \zeta p^{m-1}\}$ is Teichmuller set. Every element in $GR(p^k, m)$ can be expressed uniquely in the form

$$a_0 + pz_1 + ... + p^{k-1}z_{k-1}, \quad z_i \in T.$$

Let $F(x) \equiv f(x)(mod p)$. Thus, the polynomial $f(x)$ is linked to $F(x)$ by the homomorphism

$$\mu : Z_{p^k}[x] \rightarrow Z_p[x].$$

If $F(x) \in Z_p[x]$ is monic, irreducible of the form

$$F(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_0.$$

Indeed, in such a case, we have

$$f(x) = x^r + (p^k - p + a_{r-1})x^{r-1} + \cdots + (p^n - p + a_0) \in Z_{p^k}[x].$$

$$GR(p^k, r) = \{\sum_{j=0}^{r-1} b_j \zeta_j : b_j \in Z_{p^k}, 0 \leq j \leq r_1\},$$

with $GR(p, r)(\zeta) = 0$.

Theorem 1.3.1. *Galois rings are local rings with maximal ideal* (p) *and residue field* $GF(p^m)$

Proof. In a finite ring any nonzero element which is not a zero divisor is invertible (theorem1.1.1). Therefore (p) consists of all the zero divisors of R together with the zero element 0 is the only maximal ideal of R and $R/(p)$ is a finite field . Let $\mu : R \longrightarrow R/(p)$ be a homomorphism , $a \in R$ or $R/(p)$, and na denote na the sum of a n times.
Then $p\mu(1) = \mu(p1) = 0$. Therefore $R/(p)$ is of characteristic p and $R/(p) \simeq GF(p^m)$ for some positive integer m.

Let k be the characteristic of R. From $k1 = 0$ we deduce $k\mu(1) = \mu(k1) = 0$. Therefore $p|k$.
Now we use contradiction to prove that $k = p^n$, let $k = p^n l$ where $n, l > 0$ and $(p, l) = 1$ and assume that $l > 1$, then $a = p^n 1$ and $b = l1$ are nonzero elements of R and $ab = 0$. It follows that $l1 \in (p)$ and $l\mu(1) = \mu(l1) = 0 in R/(p)$. But $R/(p)$ is of characteristic p, so $p|l$, which contradicts $(p, l) = 1$. Therefore $l = 1$ and $k = p^n$. ∎

Example 8. *Consider the ring* $Z_9 = Z_{3^2}$

$$F_9 \cong Z_3/(x^2 + 1) = \{a + b\zeta : a, b \in F_3\}, \quad where \zeta^2 = 1$$

$$F_9 = \{0, 1, 2, \zeta, 1+\zeta, 2+\zeta, 2\zeta, 1+2\zeta, 2+2\zeta\}$$

the polynomial x^2+1 *is the primitive polynomial used for the field extension* $F_3 \subset F_9$.
By Hensels lemma

$$f(x) = x^2 + (9-3+0)x + (9-3+1) = x^2 + 6x + 7$$

is a monic basic irreducible over Z_9.
Now we can describe

$$GR(3^2, 2) = \{a_0 + a_1\zeta : a_0, a_1\zeta \in Z_9\}.$$

$|f(x)| = 8^2$, *the maximal ideal is*

$$3GR(3^2, 2) = 3(a_0 + a_1\zeta) : a_0, a_1\zeta \in Z_9.$$

$|GR(3^2, 2)| = 3^2 = 9$

Chapter 2

Cyclic codes

In this chapter the structure of cyclic codes has been studied. Cyclic codes has gained its popularity in controlling errors for several good reasons. Firstly, encoding cyclic code is easy and relatively inexpensive than others. Secondly, cyclic code is considered as the best known codes. Thirdly, cyclic property represents a great deal of algebraic structure, which can be used to predict the error detecting properties of the code and further it discovers codes with appropriate properties.

The main intent of this chapter is to examine carefully the consequences of working over a ring, rather than a finite field.

2.1 The structure of binary cyclic code

Let n be an odd number throw this chapter, let $\omega \in \{0, 1, ...n-1\}$, and the map $\sum_2(n)$:$\omega \longrightarrow 2\omega(modn)$, $\sum_2(n)$ divides the integers $0, 1, \cdots, n-1$ into disjoint cycles.

Example 9. $\sum_2(63)$ =*(0)(1 2 4 8 16 32)(3 6 12 24 48 33)*

(5 10 20 40 17 34)(7 14 28 56 49 35)(9 18 36)
(11 22 44 25 50 37)(13 26 52 35 41 19 38) (15 30 60 57 51 39)
(21 42) (23 46 29 58 53 43) (27 45 54) (31 62 61 59 55 47).

The relation between $x^n - 1$ factors and the cycles of n

Let $x^n - 1 = f_1 f_2 .... f_{i-1}$ be the factorization of $x^n - 1$ into irreducible polynomial over Z_2, let ζ be a primitive n^{th} root of unity. The zeros of $f_i(x)$ in a suitable extension field are $\zeta^{r_1}, \zeta^{r_2}, ..., \zeta^{r_k}$ where $(r_1, r_2, \cdots, r_k)$ is a cycle of $\sum_2(n)$, and each cycle represents in this way the zeros of one of the $f_i(x)$. Hence each $f_i(x)$ with zeros $\zeta^{r_1}, \zeta^{r_2} \cdots \zeta^{r_k}$, is associated with the cycle $(r_1, r_2, \cdots, r_k)$.

Definition 33. *Let* $(a_1,a_2,...,a_s)$ *be a cycle of* $\sum_2(n)$, *the* ***exponent*** *of this cycle is* $e_i := n/r_i$ *where* r_i *is the largest factor of n for which* $a_j | r_i$, *for each j=1,2,...,s*

Example 10.

Cycles						*Exponent*
1	2	4	8	16	32	63
3	6	12	24	33	48	21
5	10	17	20	34	40	63
7	14	28	35	49	56	9
9	18	36				7
11	22	25	37	44	50	63
13	19	26	38	41	25	63
15	30	39	51	57	60	21
21	42					3
23	29	43	46	53	58	63
27	45	54				7
31	47	55	59	61	62	63
0						1

Theorem 2.1.1. *[27] Let* $w_1, w_2, ..., w_t$ *be the cycles of* $\sum_2 n$, *then the number of cyclic codes of length n is* 2^t.

Example 11. *In* $\sum_2 63$ *the number of cyclic codes of length* 63 *is* 2^{13}.

Theorem 2.1.2. *[27] Let* e *be the lest common multiple of the exponent of the cycles contained in the set* S *of cycles. If* $e < n$ *the code associate with* S *has minimum distance* 2*. If* $e = n$ *the minimum distance of the code is at least* 3*.*

Example 12. *in the previous example the code* C *associated with the set* $\{(3 \quad 6 \quad 12 \quad 24 \quad 33 \quad 48), (15 \quad 30 \quad 39 \quad 51 \quad 57 \quad 60)\}$ *has d(C)=2*

Theorem 2.1.3. *[27] Let* S *contains the numbers 1,2,...d-1,d among its cycles, the minimum distance of the code associated with* S *is* $\geq d+1$.

Example 13. *For the code* C *associated with the set*

$$\{(1 \quad 2 \quad 4 \quad 8 \quad 16 \quad 32)(3 \quad 6 \quad 12 \quad 24 \quad 33 \quad 48)\},$$

$d(C) \geq 5$.

Definition 34. *The exponent of a polynomial* $f(x)$ *is the least value of* e *for which* $f(x)$ *divides* $x^e - 1$.

Theorem 2.1.4. *[27]* $g_i(x^r)$ *is exactly divisible by* $f_i(x)$ *if and only if it corresponds to the cycle containing* r.

We can now assign to each factor r_i of n an irreducible factor f_i of $x^n - 1$, which will have exponent $e_i = n/r_i$.

Example 14. *The relation between* $x^{63} - 1$ *factors and the cycles of* 63 $x^{63} - 1 = (1 + x + x^2 + x^5 + x^6)(1 + x^5 + x^6)(1 + x + x^2)(1 + x^2 + x^3 + x^5 + x^6)(1 + x^2 + x^4 + x^5 + x^6)(1 + x + x^4 + x^5 + x^6)(1 + x^3 + x^6)(1 + x + x^3 +$

$x^4 + x^6)(1 + x + x^2 + x^5 + x^6)(1 + x + x^6)(1 + x)(1 + x^2 + x^3)(1 + x + x^3)$

Factors	*Exponents*	*Associated Cycles*
$f_1 = 1 + x + x^2 + x^5 + x^6$	63	$1, 2, 4, 8, 16, 32$
$f_2 = 1 + x^5 + x^6$	63	$11, 22, 25, 37, 44, 50.$
$f_3 = 1 + x + x^2$	3	$21, 42$
$f_4 = 1 + x^2 + x^3 + x^5 + x^6$	63	$5, 20, 17, 20, 34, 40.$
$f_5 = 1 + x^2 + x^4 + x^5 + x^6$	21	$3, 6, 12, 24, 33, 48$
$f_6 = 1 + X + x^4 + x^5 + x^6$	63	$31, 47, 55, 56, 61, 62.$
$f_7 = 1 + x^3 + x^6$	9	$7, 14, 28, 35, 49, 56$
$f_8 = 1 + x + x^3 + x^4 + x^6$	63	$22, 29, 43, 46, 53, 58.$
$f_9 = 1 + x + x^2 + x^5 + x^6$	21	$15, 30, 39, 51, 57, 60.$
$f_{10} = 1 + x + x^6$	36	$13, 19, 26, 38, 41, 52.$
$f_{11} = 1 + x$	1	0
$f_{12} = 1 + x^2 + x^3$	7	$27, 45, 54.$
$f_{13} = 1 + x + x^3$	7	$9, 18, 36$

2.2 Structure of codes over Z_m where m is a product of distinct primes

Theorem 2.2.1. *(Maschkeś theorem)*
Let R be a field G a finite group and suppose the characteristic of R dose not divide the order of G then RG is semisimple

Theorem 2.2.2. *[4] The ring Z_m is semisimple if and only if m is a product of distinct primes*

Proof. Given an integer m which is a direct product of distinct primes p_i, a method is given for constructing codes over the ring of integers modulo m from cyclic codes over Z_{p_i}. Specifically, if we are given a cyclic (n, k_i) code over Z_{p_i}.

Our interest will be with group ring Z_mC_n, where $C_n = (g)$.
From theorem 1.2.7 Z_mC_n is semisimple if and only if Z_m is semisimple, C_n is finite, and n is a unit in Z_m.

From theorem 2.2.2 Z_mC_n is semisimple if and only if m is a product of distinct primes, C_n is finite, and n is a unit in Z_m.
But the units in Z_m is any integer relatively prime to m, if not there exist p s.t. $p^2|m$ $m = p^2k$, m is not a product of distinct primes,a contradiction. $\square$

Corollary 2. *[4] Z_mC_n is semisimple if and only if*

- *m is a product of distinct primes*
- *C_n is finite*
- *$gcd(n, m) = 1$*

Let Z_mC_n be a group ring where C_n is acyclic group generated by g, to each element $a = \sum_{i=0}^{n-1} r_i g^i$ in Z_mC_n, where $r_i \in R$, we associate the n tuple $(r_0, r_1, ...r_{n-1})$. Hence, $(r_{n-1}, r_0, r_1, ..., r_{n-2})$associated with $ga \in Z_mC_n$.

If N is a submodule of Z_mC_n with the property that any cyclic shift of any element in Z_mC_n is also in N, then N is an ideal of Z_mC_n.

The key point in the investigation is the following isomorphism which is an elementary theorem of number theory.

Theorem 2.2.3. *[21] if $m = \prod p_i^{e_i}$, $e_i \geq 1$, p_i distinct primes then*

$$Z_m \cong Z_{{p_1}^{e_1}} \times Z_{{p_2}^{e_2}} \times \cdots \times Z_{{p_1}^{e_1}} = \prod_i Z_{{p_i}^{e_i}}$$

with the isomorphism is exhibited explicitly by

$$\Psi : i \longmapsto (a^1, a^2, \cdots, a^s),$$

where $i \in Z_m$ and $i \equiv a^j (mod p_j^{e_j}), i = 1, \cdots, s$.

the inverse map, Ψ^{-1}, is just the Chinese remainder theorem for integers.

If
$$\Psi : i = j \longmapsto (b^1, b^2, \cdots, b^s)$$
then
$$\Psi : i + j \longmapsto (a^1 + b^1, a^2 + b^2, \cdots, a^s + b^s).$$
Returning to the case where m is a product of distinct primes, we see that Z_m is isomorphic to a direct product of the finite fields Z_{p_i}, $i = 1, \cdots, s$.

The above isomorphism may be used to establish the following isomorphism between the group rings
$$\tau : Z_m C_n \longrightarrow Z_{p_1} C_n \times Z_{p_2} C_n \times \cdots \times Z_{p_1} C_n = \prod_i Z_{p_i} C_n,$$

$$\sum_{i=0}^{n-1} r_i g^i \longmapsto \sum_{i=0}^{n-1} \Psi(r_i) g^i = \sum_{i=0}^{n-1} (a_i^1, a_i^2, \cdots, a_i^s) g^i$$
$$= (\sum_{i=0}^{n-1} a_i^1 g^i, \sum_{i=0}^{n-1} a_i^2 g^i, \cdots, \sum_{i=0}^{n-1} a_i^s g^i)$$
where the two representation of elements in $\Pi_{i=1}^s Z_{p_i}$ are equivalent and used used where convenient. The multiplication and addition in $\Pi_{i=1}^s Z_{p_i}$ are inherited from $Z_m C_n$ under Ψ,i.e.,if
$$a = \sum_0^{n-1} (a_i^1, a_i^2, \cdots, a_i^s) g^i$$
and
$$b = \sum_{j=0}^{n-1} (b_i^1, b_i^2, \cdots, b_i^s) g^i$$
are two arbitrary elements in $\prod_1^s$ then
$$a + b = \sum_{i=0}^{n-1} (a_i^1 + b_i^1, a_i^2 + b_i^2, \cdots, a_i^s + b_i^s) g^i$$

and

$$ab = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(a_i^1 b_i^1, a_i^2 b_i^2, \cdots, a_i^s b_i^s)g^i g^j$$

Now let A be an ideal in $Z_m C_n$ consists of elements $\{(\sum_{i=0}^{n-1} r_i g^i)^{(j)}\}$ where $j \in k$ for some index set k to give successively each elements of A. Let the image of these elements under Ψ be the set

$$\{(\sum_{i=0}^{n-1} a_i^1 g^i, \sum_{i=0}^{n-1} a_i^2 g^i, \cdots, \sum_{i=0}^{n-1} a_i^s g^i)^j\} =$$

$$\{(\sum_{i=0}^{n-1} a_i^1 g^i)^j, (\sum_{i=0}^{n-1} a_i^2 g^i)^j, \cdots, (\sum_{i=0}^{n-1} a_i^s g^i)^j\}$$

again where $j \in k$.

Theorem 2.2.4. *[4] Denote by A_l the set of distinct elements $\{(\sum_{i=0}^{n-1} a_i^l g^i)^j\}$ as $j \in k$, for $l = 1, 2, \ldots, s$, then A_l is an ideal of $Z_{p_l} C_n$ for $l = 1, 2, \ldots, s$,*

Proof. Since A is an ideal in $Z_m C_n$, it is closed under subtraction and multiplication by elements of $Z_m C_n$. it follows that since it also contains the zero element, is closed under subtraction and multiplication by elements of $Z_{p_l} C_n$. □

Definition 35. *[4] If B_l is an ideal in $Z_{p_l} C_n$, $l = 1, ..., s$ then the direct product of ideals $B_1 \times B_2 \times \ldots \times Bs$ in $\prod_{i=1}^{s} Z_{p_i} C_n$ is defined as the set of elements $\{(b^1, b^2, ..., b^s), b^i \in B^i\}$, where all possible combinations of elements are considered and, as before, addition and multiplication are defined component wise. The direct product $\prod_{i=1}^{s} B_i$ is an ideal of $Z_{p_i} C_n$.*

Theorem 2.2.5. *[4] The image of an ideal A in $Z_m C_n$, which we denote by $\tau(A)$, in $\prod_{i=1}^{s} Z_{p_i}$, is a direct product of the ideals A_l , $l = 1, 2, \cdots, s$.*

Proof. Let $a = \sum_{i=0}^{n-1} r_i g^i \in A \longmapsto^{\tau} \sum_{i=0}^{n-1}(a_i^1, a_i^2, \cdots, a_i^s)g^i \in \prod_{i=1}^{s} Z_{p_i} C_n$ then the element $\tau^{-1}(\sum_{i=o}^{n-1}(0, 0, \cdots, a_i^l, \cdots, 0)g^i \in \prod_{l=1}^{s} A_l) \in A$. This follows since the element $r \in Z_m$ such that $\Psi(r) = (0, \cdots, 0, 1, 0, \cdots, 0)$, where the 1 is in the l^{th} position, is such that

$$ra = r(\sum_{i=0}^{n-1} r_i g^i) \longmapsto \tau^{-1}(\sum_{i=o}^{n-1}(0,0,\cdots,a_i^l,\cdots,0)g^i.$$

Thus every ideal A in Z_mC_n is isomorphic to a direct product of ideals A_l of A_l in $Z_{p_l}C_n, l = 1....,s$. Similarly the direct product of ideals A_l in $Z_{p_l}C_n$ is isomorphic to an ideal of Z_mC_n i.e.,if $a \in A$, then $ra \in A$ since A is an ideal, now $\tau(ra) = (\sum_{i=o}^{n-1}(0,0,\cdots,a_i^l,\cdots,0)g^i$. □

Thus there is a one to one correspondence between the ideals of Z_mC_n and the direct product of ideals in $\prod_{i=1}^{s} Z_{p_i}C_n$, and once the ideals of $Z_{p_l}C_n$ are known, every ideal of Z_mC_n may be obtained by taking an appropriate direct product and applying the inverse map τ^{-1}.

Our reasons for restricting attention to the case where m is a product of distinct primes and $gcd(m,n) = 1$ is thus twofold. In the first instance, we can construct any ideal in Z_mC_n from ideals of $Z_{p_i}C_n$ and methods for constructing these ideals are well known. Secondly, in considering ideals of $Z_{p_i}C_n$ it is generally simpler to restrict attention to the case $gcd(p_i,n) = 1$.

Example 15. *Consider the group ring $Z_{15}C_8$ which is isomorphic to $Z_3C_8 \times Z_5C_8$. We take the (8,3) code over Z_3 with generator*

$$g_1(x) = 1 + x + x^2 + 2x^3 + x^5$$

as the ideal A_1 of Z_3C_8 and the $(8,2)$ code over Z_5 with generator

$$g_2(x) = 2 + x + 2x^2 + x^4 + 2x^5 + x^6$$

as the ideal A_2 of Z_5C_8. As an example of code vectors of the ideal $\tau^{-1}(A)$ obtained from (a_1,a_2) corresponding to the respective generator polynomials,i.e.,

$$a_1 = (1,1,1,2,0,1,0,0) \in A_1.$$

$$a_1 = (2,1,2,0,1,2,1,0) \in A_2.$$

The first coefficient of the element in $Z_{15}C_8$ corresponding to the element (a_1, a_2) in $A_1 \times A_2$ is given by $\Psi^{-1}(1,2) = 7$ since(using chines remainder theorem)

$$7 \equiv 1(mod 3)$$

$$7 \equiv 2(mod 5),$$

similarly the second by $\Psi^{-1}(1,2) = 7$,the third by $\Psi^{-1}(1,2) = 7$, etc.,to give the product $a_1 \times a_2 = (7, 1, 7, 5, 6, 7, 6, 0)$.

2.3 Structure of codes over Z_m where $m = \Pi p_i^{e_i}$

In the previous section, we investigated the structure of cyclic codes over the ring Z_m, the integers modulo m, where m is a product of distinct primes. This not include Z_{p^r}. In this section we will study this case.

If $m = \prod_{i=1}^{s} p_i^{e_i}$ then,

$$Z_m C_n \cong \oplus_{i=1}^{s} Z_{p_i^{e_i}} C_n.$$

And every ideal of $Z_m C_n$ is a direct product of ideals of $Z_{p_i^{e_i}} C_n$, i = 1,..., s, where $Z_m C_n$ can be viewed both as a ring and a module over Z_m.
It is sufficient to consider the case $m = p^r$, since a linear code over Z_m as a submodule and a cyclic code as an ideal.

Theorem 2.3.1. *[36] Z_pG can be written as a finite direct product of fields. i.e., $Z_pG \simeq \prod_{i=1}^{N} F_i$.*

Proof. Z_pG is a commutative semisimple ring by (theorem 2.2.1), and so Z_pG can be written as the direct product of fields since every semisimple ring is the (finite) product of simple rings.
A commutative simple ring F must be a field: the zero ring is not simple, and if $a \in F$ is nonzero, then (a) is a (two-sided) ideal hence $(a) = F$ so $a \in F^*$ and F is a field

□

Z_pG is a finite ring of characteristic p, so the same is true for F_i, $i = 1, \cdots, N$. Say F_i has p^{n_i} elements.

Theorem 2.3.2. *[36] Z_pG has 2^N ideals.*

Proof. The multiplicative subgroup of F_i forms a cyclic group from theorem 1.1.7, so there exists an element $\zeta_{m_i} \in F_i$ such that $F_i = Z_p(\zeta_{m_i})$ and ζ_{m_i} is a primitive m_i^{th} root of unity over Z_p, with $(m_i, p) = 1$. So

$$Z_pG \simeq \prod_{i=1}^{N} Z_p(\zeta_{m_i}).$$

This tells us there are N minimal nonzero ideals of Z_pG, namely, $F_1, F_2, \cdots, F_N$. Any direct product of a subset of these ideals gives rise to an ideal of Z_pG.

□

To mimic the above procedure for $Z_{p^n}G$, if $n > 1$, immediately fails. Indeed, $Z_{p^n}G$ is not semisimple, so that $Z_{p^n}G$ is not the direct product of fields. However, we can alter the procedure as follows.

Theorem 2.3.3. *[36] The group ring $Z_{p^n}H$ is the direct product of full matrix rings over local rings for any (not necessarily commutative) finite group H.*

Proof. If H is any finite group of order r with $(r, p) = 1$, then $Z_pG \simeq \prod_{i=1}^{N} Z_p(\zeta_{m_i})$ is replaced by the more general statement (theorem 1.2.6) on semisimple rings .

$$Z_pH = \prod_{i=1}^{k} [Z_p(\zeta_{k_i})]_{n_i},$$

where $[Z_p(\zeta_{k_i})]_{n_i}$ represents the full ring of $n_i \times n_i$ matrices over the field $Z_p(\zeta_{k_i})$.
Z_pH has exactly k minimal nonzero ideals and a total of 2^k ideals.

By the theorem of Spiegel (1976), we can describe $Z_{p^n}H$ in an expression similar to the previous as follow

$$Z_{p^n}H \simeq \prod_{i=1}^{k} [Z_{p^n}(\zeta_{k_i})]_{n_i},$$

i.e., $Z_{p^n}H$ is the direct product of full matrix rings over local rings. $\square$

To describe the ideals , we use the following lemma.

Lemma 8. *[36] Let R be a commutative ring with 1 and $S = M_n(R)$. If I is a two sided ideal of S, then there exists an ideal J of R such that $I = M_n(J)$.*

Proof. Let E_{ij} be the $n \times n$ such that

$$E_{ij} = \begin{cases} 1, & i^{th} row \quad and \quad j^{th} column \\ 0, & Otherwise. \end{cases}$$

Let C_{ij} be the matrix obtained from the identity matrix by the interchange of the i^{th} and j^{th} rows.

For i, j integersIet

$$f_{i,j} : I \to R,$$

$$f_{i,j}(A) = a_{ij}$$

for $A \in I$, where a_{ij} is the entry in the i^{th} row and j^{th} column of A. Then for $A, B \in I$, $f_{ij}(A+B) = f_{ij}(A) + f_{ij}(B)$, and $f_{ij}(rA) = rf_{ij}(A)$ for $r \in R$.

Thus

$$J_{ij} = \{f_{ij}(A) : A \in I\}$$

is an ideal of R.

If $A \in I$, then $C_{ik}AC_{jl} \in I$ and $f_{ij}(A) = f_{kl}(C_{ik}AC_{jl})$, so that $J_{ij} = J_{kl}$ and J_{ij} is independent of i and j.

Let $J = J_{1,1}$. Then I is contained in the full ring of $n \times n$ matrices with coefficients in J.

To prove the required result, it is now sufficient to show that $rE_{ij} \in I$. So let $I_{ij} = \{A \in I :\ f_{kl}(\text{A}) = 0 \text{ if } (k,l) \neq (i,j)\}$.
If $\acute{J}_{ij} = \{f_{ij}(A) : A \in I_{ij}\}$, then $\acute{J}_{ij}$ is again an ideal of R and $\acute{J}_{ij} \subset J_{ij}$.

But if $A \in l$, then $E_{ii}AE_{jj} \in l_{ij}$ and $f_{ij}(A) = f_{ij}(E_{ii}AE_{jj})$, so that

$$\acute{J}_{ij} = J_{ij} = J.$$

Thus if $r \in J$, $rE_{ij} \in I_{ij} \subset I$ and the result follows. □

Theorem 2.3.4. *[36] $Z_{p^n}G$ has $(n+1)^N$ ideals.*

Proof. To each full matrix ring $[Z_{p^n}(\zeta_{K_i})]_{n_i}$, there corresponds exactly $n+1$ ideals, namely,

$$[Z_{p^n}(\zeta_{k_i})]_{n_i}, [pZ_{p^n}(\zeta_{k_i})]_{n_i}, \cdots, [p^n Z_{p^n}(\zeta_{k_i})]_{n_i} = 0.$$

This says that each minimal ideal of Z_pH gives rise to n nonzero ideals of $Z_{p^n}H$, so that there are exactly $(n+1)^k$ ideals of $Z_{p^n}H$.

If G is a finite abelian group of order r and $(r,p)=1$, then we can explicitly find the codes of $Z_{p^n}G$ by the following procedure. We first find the minimal ideals of Z_pG. Say F_1 is one of them, and F_1 is a field of order p^{n_1}. Find a positive integer a_1, such that

$$p^{n_1} \equiv 1 \pmod{a_1}$$

but

$$p^m \neq 1(\text{mod } a_1) \text{ for } 0 < m < n_1.$$

F_1 contains all the roots of the equation

$x^{p^{n_1}-1}=1$, and as $a_1|(p^{n_1}-1)$,

$$\zeta_{a_1}^{a_1} = (\zeta_{a_1}^{a_1})^{(p^{n_1}-1)/a_1} = \zeta_{a_1}^{(p^{n_1}-1)} = 1$$

So $\zeta_{a_1} \in F_1$, and ζ_{a_1} does not belong to any proper subfield of F_1. Then $F_1 = Z_p(\zeta_{a_1})$. Similarly, find $a_2, \cdots, a_N$ so that $F_i = Z_p(\zeta_{a_i})$ and $F_1, \cdots, F_N$ are all the minimal ideals of Z_pG. Then $Z_{p^n}G \simeq \prod_{i=l}^{N} Z_{p^n}(\zeta_{a_i})$. Now all the $(n+1)^N$ ideals of $Z_{p^n}G$ can be seen. $\square$

Codes over Z_m where $m = \prod_{i=1}^{s} p_i^{e_i}$

To determine codes over Z_m, we first write $m = \prod_{i=1}^{s} p_i^{e_i}$ with $e_i \geq 1$ and p_i distinct primes. Let

$$\psi_i : Z_m \to Z_{{p_i}^{e_i}}, i = 1, ..., s$$

be given by $\psi_i(a) = a^{(i)}$ where $a^i \equiv a(\text{mod } Z_{p_i^{e_i}})$. ψ_i is a ring homomorphism.

Define

$$\psi : Z_m \longrightarrow Z_{p_1{}^{e_1}} \times Z_{p_2{}^{e_2}} \times \cdots \times Z_{p_s{}^{e_s}}$$

by

$$\psi(a) = (\psi_1(a), \psi_2(a), ..., \psi_s(a)).$$

Then ψ is a homomorphism. By the Chinese Remainder Theorem ψ is onto, and since both rings in question are finite, ψ is in fact an isomorphism.
For G a finite abelian group of order n, with $(n, m) = 1$, extend ψ to an isomorphism $\bar{\psi}$, by

$$\bar{\psi} : Z_m G \to Z_{p_1^{e_1}} G \times Z_{p_2^{e_2}} G \times \cdots \times Z_{p_s^{e_s}} G,$$

$$\bar{\psi}(\sum_{g\in G} r_g g) = (\sum_{g\in G} \psi_1(r_g)g, \sum_{g\in G} \psi_2(r_g)g, \cdots, \sum_{g\in G} \psi_s(r_g)g)$$

Note that $\bar{\psi}$ is onto from Chinese Remainder Theorem. to prove that $\bar{\psi}$ is one to one, let $\sum_{g\in G} \acute{g}g \in ker\bar{\psi}$

$$\bar{\psi}(\sum_{g\in G} \acute{g}g) = (\sum_{g\in G} \psi_1(r_g), \sum_{g\in G} \psi_2(r_g), \cdots, \sum_{g\in G} \psi_s(r_g)) = (0, 0, ..., 0)$$

since $(n, m) = 1$, $r_g = 0$. Hence, $ker\bar{\psi} = 0$.

If I is an ideal of $Z_m G$, then $\{\sum_{g\in G} \psi_1(r_g)g | \sum_{g\in G} r_g g \in I\}$ is an ideal of $Z_{p_i^{e_i}} G$, while if A_i is an ideal of $Z_{p_i^{e_i}} G$ for $i = 1, 2, ..., s$, then

$$\bar{\psi}^{-1}\{(a_1, \cdots, a_s) | a_i \in A_i\}$$

is an ideal of $Z_m G$. Thus knowledge of the ideals, and hence codes of $Z_m G$ is equivalent to knowledge of the codes of $Z_{p_i^{e_i}} G$ for $i = 1, ..., s$. Using the results of the previous section, we can determine the codes of $Z_{p_i^{e_i}} G$ from the codes of $Z_{p_i} G$.[36]

Chapter 3

Quaternary codes

In this chapter, the generator matrices has been studied for a code C over the ring Z_4, the ideals of $Z_4(x)/(f(x))$, where $f(x)$ is an irreducible factor of $x^n - 1$ and then use these ideals to know the ideals of $Z_4(x)/(x^n - 1)$. Finally, the dual code for the code C has been studied.

3.1 Generator Matrices

Definition 36. *[39] The* ***type*** *of the group : Let G be a group of p^m elements, and let G be a direct sum of m_1 cyclic subgroups of order p^{e_1}, $\cdots$, m_r cyclic subgroups of order p^{e_r}. Then we say that the group is of* ***type*** *$(p^{e_1})m_1 \cdots (p^{e_r})m_r$. And the group consisting of the identity element alone is of type p_0.*

Example 16. *[39] Let n be the length of the code,*

$$Z_4^n = \oplus_{i=1}^n \{(0, \cdots, 0, x_i, 0, \cdots, 0) | x_i \in Z_4\}$$

where each

$$\{(0, ..., 0, x, 0, ..., 0) | x \in Z_4\}$$

is a cyclic subgroup of order 2^2. Hence, Z_4^n is of type $(2^2)^m$,

Theorem 3.1.1. *[39] Any Z_4 linear code C containing some nonzero codewords is permutation equivalent to a Z_4 linear code with a generator matrix of the form*

$$\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{pmatrix} \tag{3.1}$$

where I_{k_1} denote the $k_1 \times k_1$ identity matrix, and I_{k_2} also denote the $k_2 \times k_2$ identity matrix, A and C are Z_2 matrices, and B is a Z_4 matrix.

Then C is an abelian group of type $4^{k_1}2^{k_2}$, and C contains $2^{2k_1+k_2}$ codewords.

Proof. We apply induction on the code length n . We distinguish the following two cases:

1. There is a codeword of order 4 in C.

   After permuting the coordinates of the codeword and (if necessary) multiplying the codeword by -1 , we can assume that the codeword of order 4 is of the form

   $$(1, c_2, \cdots, c_n).$$

   Let

   $$C' = \{(0, x_2, ..., x_n) \in C\}.$$

   C' is also a Z_4 linear code and can be regarded as a code of length $n-1$ by deleting the first coordinate.

   By induction hypothesis, C' has a generator matrix of the form

   $$\begin{pmatrix} 0 & I_{k_1-1} & A_1 & B_1 \\ 0 & 0 & 2I_{k_2} & 2 \end{pmatrix},$$

   where A_l and C are Z_2 matrices and B_1 is a Z_4 matrix.

Then C has a generator matrix of the form

$$\begin{pmatrix} 1 & c_2, \cdots, c_{k_1} & c_{k_2+1} \cdots c_{k_1+k_2} & c_{k_1+k_2+1} \cdots c_n \\ 0 & I_{k_1-1} & A_1 & B_1 \\ 0 & 0 & 2I_{k_2} & 2C \end{pmatrix}$$

After adding a certain linear combination of the last $k_1 + k_2 - 1$ rows of the above matrix to the first row, we can assume that it is carried into a matrix of the form in theorem .

2. There is no codeword of order 4 in C. Then all nonzero codewords in C are of order 2. Since $C \neq 0^n$, there is a codeword of order 2 in C.

   As in (1) we can assume that this codeword is of the form

$$(2, 2c_2, \cdots, 2c_2)$$

   Define C' as in (1). Then C' is also a Z_4 linear code without codewords of order 4. C' can be regarded as a code of length $n - 1$.

   By induction hypothesis, C' has a generator matrix of the form

$$\begin{pmatrix} 0 & 2I_{k_2-1} & 2C_1 \end{pmatrix}$$

   where C_1 is a Z_2 matrix. Then C has a generator matrix of the form

$$\begin{pmatrix} 2 & 2C_2 \cdots 2C_{k_2} & 2C_{k_2+1} \cdots 2C_n \\ 0 & 2I_{k_2-1} & 2C_1 \end{pmatrix}$$

   After adding a certain linear combination of the last $k_2 - 1$ rows of the above matrix to the first row, we can assume that it is carried into a matrix of the form

$$\begin{pmatrix} 2I_{k_2} & 2C \end{pmatrix}$$

   which is a matrix of the form in theorem with $k_1 = 0$.

□

Let $u_1, \cdots, u_{k_1} \in Z_4$ and $u_{k_1+1}, \cdots, u_{k_1+k_2} \in Z_2$. We may regard $u_1, \cdots, u_{k_1}, u_{k_1+1}, \cdots, u_{k_1+k_2}$ as information symbols. Then encoding is carried out by matrix multiplication

$$(u_1, \cdots, u_{k_1}, u_{k_1+1}, \cdots, u_{k_1+k_2})G.$$

Theorem 3.1.2. *[39] The dual code $C^{\perp}$ of the Z_4 linear code C with generator matrix (3.1) has generator matrix*

$$\begin{pmatrix} -B^t - C^t A^t & C^t & I_{n-k_1-k_2} \\ 2A^t & 2I_{k_2} & 0 \end{pmatrix} \tag{3.2}$$

where n is the code length of C. $C^{\perp}$ is an abelian group of type $4^{n-k_1-k_2}2^{k_2}$ and $C^{\perp}$ contains $2^{2n-2k_1-k_2}$ codewords.

Proof. Denote the Z_4 linear code with generator matrix 3.2 by C' Clearly $C' \subset C^{\perp}$.

Let $c = (c_1, c_2, \cdots, c_n) \in C^{\perp}$.

After adding a certain linear combination of the first $n - k_1 - k_2$ rows of 3.2 to c, we can obtain a codeword of $C^{\perp}$, which is of the form

$$c' = (c_1, \cdots, c_{k_1}, c_{k_1+1}, \cdots, c_{k_1+k_2}, 0, \cdots, 0).$$

Since c' is orthogonal to the last k_2 rows of 3.1 , each of $c_{k_1}, c_{k_1+1}, \cdots, c_{k_1+k_2}$ is 0 or 2.

After adding a certain linear combination of the last k_2 rows of (3.2) to c' we can obtain a codeword of $C^{\perp}$, which is of the form

$$c'' = (c_1, \cdots, c_k, 0, ..., 0).$$

Since c'' is orthogonal to the first k_1 rows of 3.1, $c_1 = \cdots = c_k = 0$. Therefore $c \in C'$. □

Definition 37. *The codes over F_2 with generator matrix*

$$\begin{pmatrix} I_{k_1} & A & \overline{B} \end{pmatrix} \tag{3.3}$$

where $\overline{B}$ is the reduction modulo 2 of B is the ***residue code.***

The codes over F_2 with generator matrix

$$\begin{pmatrix} I_{k_1} & A & \overline{B} \\ 0 & I_k & C \end{pmatrix} \tag{3.4}$$

is the ***torsion code .***

Corollary 3. *[39] Any self dual Z_4 code of length n contains 2^n codewords.*

Proof. Let C be a self dual Z_4 code of length n with generator matrix (3.1).

$|C| = 2^{2k_1+k_2}$ and $|C^\perp| = 2^{2n-2k_1-k_2}$.

Since $C^\perp = C$, we have $2^{2n-2k_l-k_2} = 2^{2k_1+k_2}$.

Therefore $n = 2k_1 + k_2$ and $|C| = 2^n$. □

3.2 The ideals of $Z_4(x)/(f(x))$

Definition 38. *[6] A code over Z_4 or a Z_4 code is a set C of n tuples over Z_4.*
a linear code over Z_4 or a quaternary code is a Z_4 module.

Definition 39. *[6] A polynomial $f(x) \in Z_4[x]$ is* ***irreducible*** *in Z_4 if whenever $f(x) = g(x)h(x)$ for two polynomials $g(x)$ and $h(x)$ in $Z_4[x]$, one of $g(x)$ or $h(x)$ is a unit.*

Let $\mu : Z_4[x] \to Z_2[x]$ be the map which sends a to a(mod 2) and x to x.
And $\mu : Z_{p^n} \to Z_p[x]$ be the map which sends a to a(mod p) and x to x in

general.
The ring homomorphism.

$$\mu : Z_4[x] \longrightarrow Z_2[x]$$
$$a_0 + a_1x + \cdots + a_nx^n \longrightarrow \mu a_0 + \mu a_1x + \cdots + \mu a_nx^n \tag{3.5}$$

Definition 40. *[20] A polynomial $f(x) \in Z_{p^m}[x]$ is **basic** irreducible if its $\mu(f(x))$ is irreducible in $Z_p[x]$.*

Definition 41. *[8] An ideal I of a ring Z_4 is called **a primary** ideal provided $ab \in I$ implies that either $a \in I$ or $b^r \in I$ for some positive integer r.*

Definition 42. *[30] A polynomial $f(x) \in Z_4[x]$ is primary if the principal ideal*

$$(f(x)) = \{f(x)g(x) : g(x) \in Z_4[x]\}$$

is primary ideal.

Definition 43. *[8] Let $f(x)$ and $g(x)$ be polynomials over the ring R: If*

$$gcd(f(x), g(x)) = 1,$$

we say that $f(x)$ and $g(x)$ are relatively prime (over R). In particular, $f(x)$ and $g(x)$ are relatively prime if and only if there exist polynomials $a(x)$ and $b(x)$ over R for which

$$a(x)f(x) + b(x)g(x) = 1.$$

Theorem 3.2.1. *[20] If $f(x)$ is a basic irreducible polynomial, then $f(x)$ is primary*

Proof. Suppose $g(x)h(x) \in (f(x))$. Since $\mu f(x)$ is irreducible,

$$d = gcd(\mu g(x), \mu f(x))$$

is either 1 or $\mu f(x)$.

If $d = 1$, then by definition there exist polynomials $a(x)$ and $b(x)$ in $Z_4[x]$ such that

$$\mu(a(x))\mu(g(x)) + \mu(b(x))\mu(f(x)) = 1.$$

Hence

$$a(x)g(x) + b(x)f(x) = 1 + 2s(x)$$

for some $s(x) \in Z_4[x]$. Therefore

$$a(x)g(x)h(x)(1+2s(x))+b(x)f(x)h(x)(1+2s(x)) = h(x)(1+2s(x))^2 = h(x),$$

implying that $h(x) \in (f(x))$.

Suppose now that $d = \mu(f(x))$. Then there exists $a(x) \in Z_4[x]$ such that

$$\mu(g(x)) = \mu(f(x))\mu(a(x))$$

implying that

$$g(x) = f(x)a(x) + 2s(x)$$

for some $s(x) \in Z_4[x]$. Hence

$$g(x)^2 = (f(x)a(x))^2 \in (f(x)).$$

Thus $f(x)$ is a primary polynomial. □

Definition 44. *[8] Two polynomials f and g in $R[x]$ are called coprime, or relatively prime if $R[x] = (f) + (g)$*

Lemma 9. *[30] Let $f(x)$ and $g(x)$ be polynomials in $Z_4[x]$. Then $f(x)$ and $g(x)$ are coprime if and only if $\mu(f(x))$ and $\mu(g(x))$ are coprime polynomials in $F_2[x]$.*

Proof. If $f(x)$ and $g(x)$ are coprime, then

$$a(x)f(x) + b(x)g(x) = 1$$

for some $a(x)$ and $b(x)$ in $Z_4[x]$.

Then

$$\mu(a(x))\mu(f(x)) + \mu(b(x))\mu(g(x)) = \mu(1) = 1,$$

implying that $\mu(f(x))$ and $\mu(g(x))$ are coprime.
Conversely, suppose that $\mu(f(x))$ and $\mu(g(x))$ are coprime. Then there exist $a(x)$ and $b(x)$ in $Z_4[x]$ such that

$$\mu(a(x))\mu(f(x)) + \mu(b(x))\mu(g(x)) = 1.$$

Thus

$$a(x)f(x) + b(x)g(x) = 1 + 2s(x)$$

for some $s(x) \in Z_4[x]$ since 1+2s(x) is invertible, then $1 \in Z_4[x]$ by definition (44) showing that $f(x)$ and $g(x)$ are coprime.
Or

$$a(x)(1 + 2s(x))f(x) + b(x)(1 + 2s(x))g(x) = (1 + 2s(x))^2 = 1$$

showing that $f(x)$ and $g(x)$ are coprime. □

Theorem 3.2.2. *[39] Let $f(x)$ be a monic polynomial of degree ≥ 1 in $Z_4[x]$, then*

- *$f(x) = g_1(x)...g_k(x)$, where $g_1(x), ..., g_k(x)$ are pairwise coprime monic primary polynomials.*
- *Let*

$$f(x) = g_1(x)...g_k(x) = h_1(x)...h_s(x) \tag{3.6}$$

be two factorization of $f(x)$ into pairwise coprime monic primary polynomials, then $k = s$ and after renumbering, $g_i(x) = h_i(x)$, $i = 1, ..., k$.

Theorem 3.2.3. *(Hensel's lemma)[26]*
Let $f(x) \in R[x]$ where R is a chain ring, let $\mu : R \to R/(a)$ where (a) is the maximal ideal.
Suppose $\mu(f(x)) = h_1(x)h_2(x)...h_k(x)$, where $h_1(x)h_2(x)\cdots h_k(x)$ are pairwise coprime polynomials in $R[x]/(a)$.
Then there exist $g_1(x), g_2(x), \cdots, g_k(x)$ in $R[x]$ such that:
1- $\mu(g_i(x)) = h_i(x) for 1 \leq i \leq k$,
2- $g_1(x), g_2(x), ..., g_k(x)$ are pairwise coprime, and
3- $f(x) = g_1(x)g_2(x)g_k(x)$, deg $g_i(x)$ =deg $h_i(x)$.

Theorem 3.2.4. *[30] Let n be a positive odd integer. Then the polynomial $x^n - 1$ over Z_4 can be factored into a product of finitely many pairwise coprime basic irreducible polynomials over Z_4 , say*

$$x^n - 1 = g_1(x), g_2(x), ..., g_k(x) \tag{3.7}$$

Moreover, $g_1(x), g_2(x), ..., g_k(x)$ are uniquely determined up to a rearrangement.

Proof. Over Z_2, we have the unique factorization

$$x^n - 1 = h_1(x)h_2(x) \cdots h_k(x),$$

where $h_1(x)h_2(x) \cdots h_k(x)$ are irreducible polynomials over Z_2. Since n is odd, $h_1, (x)h_2(x), \cdots, h_k(x)$ are pairwise coprime.

By Hensel's lemma, there are monic polynomials $g_1(x), g_2(x), ..., g_k(x)$ over Z_4 such that $\mu g_i(X) = h_i(X)$ and $deg\ g_i(X) = deg\ h_i(X)$ for $i = 1, 2, ..., k$, that $g_1(X), g_2(X), \cdots, g_k(X)$ are pairwise coprime, and that

$$x^n - 1 = g_1(X)g_2(X)...g_r(X),$$

Since $\mu g_i(X) = h_i(x)$, $i = 1, 2, ..., k$, are irreducible over Z_2,

$$g_1(X), g_2(X), ..., g_k(X)$$

are basic irreducible. By lemma 9 $g_i(X)$, $i = 1, 2, ..., k$, are primary.

Then the uniqueness of (3.7) follows from Theorem 3.2.2 □

Theorem 3.2.5. *[30] If $f(x)$ is in Z_4 and is basic irreducible, then the only ideals of $Z_4/(f(x))$ are $(0), (1)$ and (2).*

Proof. Suppose I is a nonzero ideal of the ring $Z_4/(f(x))$ and $g(x) + (f(x)) \in I$ for some $g(x)$ which is not belong $(f(x))$. Since

$gcd(\mu g(x), \mu f(x)) = 1$ or $\mu f(x)$.

If $gcd(\mu f(x), \mu g(x)) = 1$, then there exist $a(x)$,$b(x) \in Z_4[x]$ such that

$$\mu a(x)\mu f(x) + \mu b(x)\mu g(x) = 1$$

$$a(x)f(x) + b(x)g(x) = 1 + 2s(x),$$

$s(x) \in Z_4[x]$, multiply both sides by $(1 + 2s(x))$

$$a(x)f(x)(1 + 2s(x)) + b(x)g(x)(1 + 2s(x)) = 1,$$

$$a(x)f(x)(1 + 2s(x)) + ((g(x))(b(x)(1 + 2s(x)))) = 1$$

$$(b(x)(1 + 2s(x)) + (f(x)))(g(x) + (f(x))) = 1 + (f(x)).$$

Hence, $g(x) + (f(x))$ is invertible.

$$I = Z_4[x]/(f(x)) = (1).$$

If $gcd(\mu f(x), \mu g(x)) = \mu f(x)$, then there exists $a(x), b(x), s(x) \in Z_4$ such that

$$\mu a(x)\mu f(x) + \mu g(x)\mu b(x) = \mu f(x)$$

$$a(x)f(x) + b(x)g(x) = f(x) + 2s(x)$$

$$2a(x)f(x) + 2b(x)g(x) = 2f(x)$$

$$2b(x)g(x) + (f(x)) = 2 + (f(x)).$$

Hence,$2 + (f(x)) \in I$

$$(2 + (f(X))) \subseteq I$$

From the ring homomorphism (3.5) because

$$(Z_4[x]/(f(X)))/(2 + (f(X))) \approx Z_2[X]/(\mu f(X)),$$

which is a field, $(2 + (f(X)))$ is a maximal ideal of $Z_4[x]/(f(X))$. Hence $I = (2 + (f(X)))$. □

3.3 The ideals of $Z_4[x]/(x^n - 1)$

Lemma 10. *[39] Let $f_1(X), f_2(X), ..., f_k(X)$ be k pairwise coprime polynomials over Z_4 and Let $\hat{f}_i(X)$ denote the product of all $f_j(X)$ except $f_i(X)$, Then $\hat{f}_i(X)$ and $f_i(X)$ are coprime for $i = 1, 2, ..., k$.*

Proof. By Lemma 9 the coprimeness of $f_i(X)$ and $f_j(X)$ for $i \neq j$ implies the coprimeness of $\mu f_i(X)$ and $\mu f_j(X)$. But $\mu f_1(X), \mu f_2(X), ..., \mu f_k(X)$ are polynomials over Z_2. So $\mu \hat{f}_i(X) = \mu f_1(X)...\mu f_{i-1}(X), \mu f_{i+1}(X)...\mu f_k(X)$ and $\mu f_i(X)$ are coprime. Again by Lemma 9, $f_i\hat{(}X)$ and $f_i(X)$ are coprime. □

Lemma 11. *[39] Let $f_1(X), f_2(X), ..., f_k(X)$ be k pairwise coprime polynomials in $Z_4[X]$, then*

$$(f_1(X)f_2(X)...f_k(X)) = (f_1(X)) \cap (f_2(X)) \cap ... \cap (f_k(X)).$$

Proof. Clearly, $(f_1(X), f_2(X), ..., f_k(X)) \in (f_i(X))$ for every i. Therefore

$$(f_1(X)f_2(X)...f_k(X)) \subseteq (f_1(X)) \cap (f_2(X)) \cap ... \cap (f_k(X)).$$

It remains to prove that

$$(f_1(X)f_2(X)...f_k(X)) \supseteq (f_1(X)) \cap (f_2(X)) \cap ... \cap (f_k(X)).$$

We apply induction on k . The case $k = 1$ is trivial. Let $k > 1$ and assume that it's holds for $k - 1$. That is, we have

$$(f_1(X)f_2(X)...f_{k-1}(X)) = (f_1(X)) \cap (f_2(X)) \cap ... \cap (f_{k-1}(X)).$$

Let

$$g(X) \in (f_1(X)) \cap (f_2(X)) \cap ... \cap (f_k(X)),$$

then

$$g(X) \in (f_1(X)f_2(X)...f_{k-1}(X)) \cup (f_k(X)).$$

Thus there are polynomials $q_1(X)$, $q_2(X) \in Z_4[X]$ such that

$$g(x) = q_1(X)f_1(X)f_2(X)...f_{k-1}(X) = q_2 f_k(x).$$

By lemma 10 $f_1(X)f_2(X)...f_{k-1}(X)$ and $f_k(x)$ are coprime. Then there are polynomials $h_1(X)$, $h_2(X) \in Z4[X]$ such that

$$h_1(X)f_1(X)f_2(X)...f_{k-1}(X) + h_2(X)f_k(x) = 1.$$

Multiplying the last equation by $g(X)$, we obtain

$$g(x)h_1(X)f_1(X)f_2(X)...f_{k-1}(X) + g(x)h_2(X)f_k(x) = g(x)$$

$$g(x) = (q_2h_1(X) + q_1(X)h_2(X))f_1(X)f_2(X)...f_{k-1}(X)f_k(x).$$

Thus $g(x) \in (f_1(X)f_2(X)...f_{k-1}(X)f_k(x))$. Which compleat the proof. □

Theorem 3.3.1. *[39] (Sun Zi Theorem) Let $f_1(X), f_2(X), ..., f_k(x)$ be k pairwise coprime polynomials of degree ≥ 1 over Z_4 and $a_1(X), a_2(X), ..., a_k(X)$ be any k polynomials over Z_4. Then the simultaneous congruences*

$$x \equiv a_1(X)(mod f_1(X))$$

$$x \equiv a_2(X)(mod f_2(X))$$

$$\vdots$$

$$x \equiv a_K(X)(mod f_k(X)).$$

has a solution in $Z_4[X]$.
Moreover, the solution is unique $mod f_1(X)f_2(X)\cdots f_k(x)$, i.e., if $g(X)$ and $h(X)$ are two solutions , then

$$g(X) \equiv h(X)(mod f_1(X)f_2(X)...f_k(x)).$$

Proof. By Lemma 10 $\hat{f}_i(X)$ and $f_i(X)$ are coprime, $i = 1, 2, ..., k$. Then there are polynomials $b_i(X)$ and $q_i(X)$ over Z_4 such that

$$b_i(X)\hat{f}_i(X) + q_i(X)f_i(X) = 1. \tag{3.8}$$

It is easy to verify that

$$a_1 b_1 \hat{f}_1(X) + a_2 b_2 \hat{f}_2(X) + \cdots + a_k b_k \hat{f}_k(X) \tag{3.9}$$

is a solution of the system.

Now let $g(X)$ and $h(X)$ be two solutions of the system.
Then $g(X) \equiv h(X)(mod f_i(X))$, $i = 1, 2, ..., k$.
That is, $g(X) - h(X) \in (f_i(X))$, $i = 1, 2, ..., k$. By Lemma 11

$$g(X) - h(X) \in f_1(X) f_2(X) ... f_k(x)$$

That is,

$$g(X) \equiv h(X)(mod f_1(X) f_2(X) ... f_k(x)).$$

□

Theorem 3.3.2. *[39] Let $f_1(X), f_2(X), ..., f_k(x)$ be k pairwise coprime polynomials of degree ≥ 1 over Z_4 and $f(x) = f_1(X) f_2(X) ... f_k(x)$. Denote the residue class ring $Z_4[X]/(f(X))$ by R. For $i = 1, 2, ..., k$, let*

$$e_i = b_i(X) \hat{f}_i(X) + (f(X)), \tag{3.10}$$

where $b_i(X)$ is the polynomial $b_i(X)$ appearing in (3.8). Then

- *$R_i = Re_i$ is an ideal of R, and e_i is the identity of R_i, $i = 1, 2, ..., k$.*
- *$R = R_1 \oplus R_2 \oplus ... \oplus R_k$.*

Corollary 4. *[39] Let $f_1(X), f_2(X), ..., f_k(x)$ be k pairwise coprime monic polynomials of degree≥ 1 over Z_4 and $f(x) = f_1(X) f_2(X) ... f_k(x)$, Then for any $i = 1, 2, ..., k$, the map*

$$Z_4[X]/f_i(X) \longrightarrow (Z_4[X]/(f(X))e_i = Re_i \tag{3.11}$$

$$k(X) + (f_i(X)) \longrightarrow (k(X) + (f(X)))e_i$$

is an isomorphism of rings.

Corollary 5. *[39] Let $f_1(X), f_2(X), ..., f_k(x)$ be k pairwise coprime monic polynomials of degree≥ 1 over Z_4 and $f(x) = f_1(X)f_2(X)...f_k(x)$, Then*

$$Z_4(x)/(f(x)) \simeq Z_4(x)/(f_1(X)) \oplus Z_4(x)/(f_2(X)) \oplus \cdots \oplus Z_4(x)/(f_k(X)).$$

Lemma 12. *[30] Let n be an odd positive integer and $x^n-1 = f_1(X)f_2(X)...f_k(x)$ be the unique factorization of $x^n - 1$ into basic irreducible polynomials over Z_4. Then under the isomorphism (3.11), the ideals (0), $(1 + (f_i(X)))$, and $(2 + (f_i(X)))$ of $Z_4[X]/(f_i(X))$ are mapped into (0), $(\hat{f}_i(X) + (x^n - 1))$ and $(2\hat{f}_i(X) + (x^n - 1))$ of $R_i = Re_i$, respectively.*

Proof. Under the isomorphism (3.11), we have

$$1 + (f_i(X)) \longrightarrow (1 + (x^n - 1))e_i.$$

By (3.10), $e_i = b_i(X)\hat{f}_i(X) + (x^n - 1)$. Therefore

$$1 + (f_i(X)) \longrightarrow b_i(X)\hat{f}_i(X) + (x^n - 1).$$

Clearly,

$$b_i(X)\hat{f}_i(X) + (x^n - 1) \in (\hat{f}_i(X) + (x^n - 1)).(*)$$

Multiplying both sides of (3.8) by $\hat{f}_i(X)$, we obtain

$$b_i(X)\hat{f}_i(X)\hat{f}_i(X) + C_i(X)(x^n - 1) = \hat{f}_i(X).$$

Then

$$b_i(X)\hat{f}_i(X)\hat{f}_i(X) + (x^n - 1) = \hat{f}_i(X) + (x^n - 1),$$

which implies

$$\hat{f}_i(X) + (x^n - 1) \in (b_i(X)\hat{f}_i(X) + (x^n - 1))(**).$$

Therefore

$$(b_i(X)\hat{f}_i(X) + (x^n - 1)) = (\hat{f}_i(X) + (x^n - 1)), (by * and **)$$

and the image of $(1 + (f_i(X)))$ under (3.11) is $(\hat{f}_i(X) + (x^n - 1))$. Similarly, we can prove that the image of $(2 + (f,(X)))$ under (3.11) is $(2\hat{f}_i(x) + (x^n - 1))$. □

Theorem 3.3.3. *[30] Let $x^n - 1 = f_1 f_2 \dots f_k$, be a product of basic irreducible and pairwise coprime polynomials for odd n. Then any ideal in the ring R_n is a sum of ideal $(\hat{f}_i)$ and $(2\hat{f}_j)$*

Proof. By theorem (3.2.4) the factorization of $x^n - 1$ exists and is unique. By corollary 5

$$R_n = Z_4[x]/(f_1) \oplus Z_4[x]/(f_2) \oplus Z_4[x]/(f_3) \oplus \cdots \oplus Z_4[x]/(f_k).$$

if I is an ideal of R_n, then

$$I \simeq I_1 \oplus I_2 \oplus \cdots \oplus I_k$$

[[15]p135], where I_i is an ideal of the ring $Z_4[x]/(f_i)$, for $i = 1, 2, \cdots, k$. By theorem (3.2.5),

$$I_i = 0, Z_4[x]/(f_i) \quad or \quad (2 + (f_i)).$$

By theorem (12) $I_i = Z_4[x]/(f_i)$, then it corresponds to the ideal $(\hat{f}_i)$ in the ring R_n, if $I_i = (2 + (f_i))$, then it corresponds to the ideal $(2\hat{f}_j)$. In any case, the ideal I is a sum of $(\hat{f}_i)$ and $(2\hat{f}_j)$. □

Theorem 3.3.4. *[30] Suppose C is a Z_4 cyclic code of odd length n. Then there exist unique monic polynomials f, g and h such that $x^n - 1 = fgh$ and $C = (fh) \oplus (2fg)$: Furthermore, C has type $4^{degg} 2^{degh}$.*

When $h = 1$, $C = (f)$ and $|C| = 4^{n-degf}$

When $g = 1$, $C = (2f)$ and $|C| = 2^{n-degf}$.

Proof. We know that $x^n - 1$ has a unique factorization such that

$$x^n - 1 = f_1 f_2 \cdots f_r,$$

where thef_i are basic irreducible and pairwise coprime, We also know, by the previous theorem , that C is a sum of $(\hat{f}_i)$ and $(2\hat{f}_j)$. By permuting the subscripts of f_i, we can suppose that C is a sum of

$$(\hat{f}_{k+1}), (\hat{f}_{k+2}), \cdots, (\hat{f}_{k+l}), (2\hat{f}_{k+l+1}), (2\hat{f}_{k+l+2}), \cdots, (2\hat{f}_r),$$

Then

$$C = (f_1 f_2 \cdots f_k f_{k+l+1} f_{k+l+2} \cdots f_r, 2 f_1 f_2 \cdots f_k f_{k+1} \cdots f_{k+l}) = (fh, 2fg),$$

where $f = f_1 f_2 \cdots fk$, $g = f_{k+1} f_{k+2} \cdots f_{k+l}$ or 1 if $l = 0$

and

$h = f_{k+l+1} f_{k+l+2} \cdots f_r$ or $1 if k + l = r$.

When$h \neq 1$ fh and g are coprime, $(fh) \bigcap (2fg) = 0$. Therefore

$$|C| = |fh||2fg| = 4^{n-ged(f)-deg(h)} 2^{n-deg(f)-deg(g)}.$$

When $h = 1$, the above identity is still true because in this case $C = (f)$ and

$$|C| = |fh||2fg| = 4^{n-ged(f)-deg(h)} 2^{n-ged(f)-deg(g)} = 4^{n-ged(f)}.$$

When $g = 1$, the above identity is still true because in this case $C = (2f)$ and

$$|C| = |fh||2fg| = 4^{n-ged(f)-deg(h)} 2^{n-ged(f)-deg(g)} = 2^{n-ged(f)}.$$

□

3.4 The dual codes

Theorem 3.4.1. *[30] Let $C = (fh, 2fg)$ be a Z_4 cyclic code of odd length n where f, g and h are monic polynomials such that $fgh = x^n - 1$.*
Then $C^\perp$ is also a Z_4 cyclic code $C^\perp = (g^* h^*, 2g^* f^*)$, and $|C^\perp| = 4^{degf} 2^{degh}$.

Proof.

$$fh(g^*h^*)^* = fghh = 0 \quad in \quad Z_4/(x^n - 1),$$
$$2fg(g^*h^*)^* = 2fghg = 0 \quad in \quad Z_4/(x^n - 1).$$

So, $g^*h^* \in C^{\perp}$.

$$fh(2g^*f^*)^* = 2fghf = 0 \quad in \quad Z_4/(x^n - 1)$$
$$Also \quad 2fg(2g^*f^*)^* = 0 \quad Z_4/(x^n - 1).$$

Thus $2g^*f^* \in C^{\perp}$, $(g^*h^*, 2g^*f^*) \subseteq C^{\perp}$. Since C has type $4^{degg}2^{degh}$, $C^{\perp}$ has type $4^{n-degg-degh}2^{degh} = 4^{degf}2^{degh}$ from theorem (3.3.4).

Since $x^n - 1 = f^*g^*h^*$, $(g^*h^*, 2g^*f^*)$ has type $4^{degf^*}2^{degh^*} = 4^{degf}2^{degh}$. Thus $C^{\perp} = (g^*h^*, 2g^*f^*)$.

□

Corollary 6. *[31] Let* n *be odd. Assume* $x^n - 1$ *is a product of* k *irreducible polynomial in* $Z_4[x]$*.Then there are* $(3)^k$ *cyclic codes over* Z_4 *of length* n*.*

Proof. Let $x^n - 1 = g_1(x)g_2(x)...g_k(x)$ be the factorization of $x^n - 1$ into monic irreducible polynomials. If C is a cyclic code, by the pervious theorem $C = (f(x)g(x)) \oplus (2f(x)h(x))$ where $x^n - 1 = f(x)g(x)h(x)$. Each $g_i(x)$ is a factor of exactly one of $f(x), g(x), or h(x)$. □

Example 17. *[31]* $x^7-1 = (x-1)(x^3+2x^2+x-1)(x^3-x^2+2x-1)$ *let* $x^7-1 = g_1(x)g_2(x)g_3(x)$ *let* $g_1(x), g_2(x)$*and* $g_3(x)$ *equal* $(x-1), (x^3+2x^2+x-1)$ *and* $(x^3 - x^2 + 2x - 1)$ *respectively are the monic irreducible factors of* $x^7 - 1$*.*

By the previous corollary there are $3^3 = 27$ *cyclic codes over* Z_4 *of length* 7*. In the table we give the generator polynomials of the* 25 *nontrivial cyclic codes of length* 7 *as described in the theorem*

Code number	*generator polynomials*	*type*	*dual polynomial*
1	2	2^7	2
2	f_1	4^6	f_2f_3
3	f_2	4^4	f_1f_2
4	f_3	4^4	f_1f_3
5	f_1f_2	4^3	f_2
6	f_2f_3	4	f_1
7	f_1f_3	4^3	f_3
8	$2f_1$	2^6	$(f_2f_3, 2f_1)$
9	$2f_2$	2^4	$(f_1f_2, 2f_3)$
10	$2f_3$	2^4	$(f_1f_3, 2f_2)$
11	$2f_2f_3$	2	$(f_1, 2f_2f_3)$
12	$2f_1f_2$	2^3	$(f_2, 2f_1f_3)$
13	$2f_1f_3$	2^3	$(f_3, 2f_1f_2)$
14	$(f_1, 2f_2f_3)$	$4^6.2$	$2f_2f_3$
15	$(f_2, 2f_1f_3)$	$4^4.2^3$	$2f_1f_2$
16	$(f_3, 2f_1f_2)$	$4^4.2^3$	$2f_1f_3$
17	$(f_1f_2, 2f_3)$	$4^3.2^4$	$2f_2$
18	$(f_1f_3, 2f_2)$	$4^3.2^4$	$2f_3$
19	$(f_2f_3, 2f_1)$	4.2^6	$2f_1$
20	$(f_1f_2, 2f_1f_3)$	$4^3.2^3$	$(f_2f_3, 2f_1f_2)$
21	$(f_1f_2, 2f_2f_3)$	$4^3.2$	$(f_1f_2, 2f_2f_3)$
22	$(f_1f_3, 2f_1f_2)$	$4^3.2^3$	$(f_2f_3, 2f_1f_3)$
23	$(f_1f_3, 2f_3f_2)$	$4^3.2$	$(f_1f_3, 2f_3f_2)$
24	$(f_2f_3, 2f_1f_2)$	4.2^3	$(f_1f_2, 2f_1f_3)$
25	$(f_2f_3, 2f_1f_3)$	4.2^3	$(f_1f_3, 2f_1f_2)$

Example 18. *[31] If $C = (f(x)h(x)) \oplus (2f(x)g(x))$, as in the theorem , we can easy write down a generator matrix G for C.*

Consider $C = (g_1g_3, 2g_2)$ in the table Since $g_1(x)g_3(x) = 1 + x + 3x^2 + 2x^3 + x4$ and $2g_2(x) = 2 + 2x + 2x^3$; then the generator matrix for this code *is*

$$C = \begin{pmatrix} 1 & 1 & 3 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 3 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 3 & 2 & 1 \\ 2 & 2 & 0 & 2 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 & 2 \end{pmatrix}$$

Chapter 4

Codes over Z_{p^n}

In this chapter, the code C over the ring Z_{p^n} has been studied. The ideals of $Z_{p^n}(x)/(f(x))$, where $f(x)$ is an irreducible factor of $x^n - 1$ and then use these ideals to know the ideals of $Z_{p^n}(x)/(x^n - 1)$. Finally, we steady the dual code for the code C.

Definition 45. *A polynomial f in the ring R is called regular if it is not a zero divisor, i.e., if for $g \in R$, $fg = 0$ implies $g = 0$.*

4.1 The ideals of $Z_{p^m}[x]/(f(x))$

Lemma 13. *[23] Let $f(x)$ and $g(x)$ be regular polynomials in $Z_{p^n}[x]$. Then $f(x)$ and $g(x)$ are coprime if and only if $\mu(f(x))$ and $\mu(g(x))$ are coprime polynomials in $F_p[x]$.*

Proof. If $f(x)$ and $g(x)$ are coprime, then

$$a(x)f(x) + b(x)g(x) = 1$$

for some $a(x)$ and $b(x)$ in $Z_{p^n}[x]$.

Then

$$\mu(a(x))\mu(f(x)) + \mu(b(x))\mu(g(x)) = \mu(1) = 1,$$

implying that $\mu(f(x))$ and $\mu(g(x))$ are coprime. Conversely, suppose that $\mu(f(x))$ and $\mu(g(x))$ are coprime. Then there exist $a(x)$ and $b(x)$ in $Z_{p^n}[x]$ such that

$$\mu(a(x))\mu(f(x)) + \mu(b(x))\mu(g(x)) = 1.$$

Thus

$$a(x)f(x) + b(x)g(x) = 1 + p^k s(x)$$

for some $s(x) \in Z_{p^n}[x]$,and positive integer k. Since since $1 + p^k s(x)$ is invertible, then $1 \in Z_{p^k}[x]$ by definition 44 this showing that $f(x)$ and $g(x)$ are coprime.

□

Theorem 4.1.1. *[25] Let $f(x)$ be a regular polynomial in $Z_{p^k}[x]$, then*

- *$f(x) = ug_1(x)...g_k(x)$, where $g_1(x), ..., g_k(x)$ are regular pairwise coprime primary polynomials.*
- *Let*
$$f(x) = ug_1(x)...g_k(x) = vh_1(x)...h_s(x) \tag{4.1}$$
where u and v are units be two factorization of $f(x)$ into regular pairwise coprime primary polynomials, then $k = s$ and after renumbering, $g_i(x) = h_i(x)$, $i = 1, ..., k$.

Theorem 4.1.2. *[25] Let n be a positive integer and p does not divides n. Then the polynomial $x^n - 1$ over Z_{p^m} can be factored into a product of finitely many pairwise coprime regular, primary polynomials over Z_{p^k} , say*

$$x^n - 1 = g_1(x), g_2(x), ..., g_k(x) \tag{4.2}$$

Moreover, $g_1(x), g_2(x), ..., g_k(x)$ are uniquely determined up to a rearrangement.

Theorem 4.1.3. *[23] If $f(x) \in Z_{p^m}[x]$ is a basic irreducible polynomial then the ideals of $Z_{p^m}[x]/(f(x))$ are precisely (0), $(1 + (f(x)))$, $(p + (f(x)))$,..., $(p^{m-1} + (f(x)))$.*

Proof. Suppose I is a nonzero ideal of the ring $Z_{p^m}[x]/(f(x))$ and $g(x) + (f(x)) \in I$ for some $g(x)$ which is not belong $(f(x))$. Since $\mu f(x)$ is irreducible in $Z_p[x]$

$gcd(\mu g(x), \mu f(x)) = 1$ or $\mu f(x)$.

If $gcd(\mu f(x), \mu g(x)) = 1$, then there exist $a(x)$,$b(x) \in Z_{p^m}[x]$ such that

$$\mu a(x)\mu f(x) + \mu b(x)\mu g(x) = 1$$

$$a(x)f(x) + b(x)g(x) = 1 + p^k s(x),$$

for some positive integer k $s(x) \in Z_{p^m}[x]$. Since since $1+p^k s(x)$ is invertible, then $1 \in Z_{p^k}[x]$ by definition 44 this showing that $f(x)$ and $g(x)$ are coprime. There exists $u(x)$ and $v(x)$ such that $1 = f(x)u(x) + g(x)v(x)$.
But then $(g(x) + (f(x)))(v(x) + (f(x))) = 1 + (f(x))$.
Therefore $g(x) + (f(x))$ is invertible. Hence, $g(x) + (f(x))$ is invertible.

$$I = Z_{p^m}[x]/(f(x)) = (1).$$

If $gcd(\mu f(x), \mu g(x)) = \mu f(x)$,then $\mu f(x)|\mu g(x)$.
Hence there exists $a(x), b(x) \in Z_{p^m}$ such that

$$g(x) = a(x)f(x) + p^k b(x)$$

where $gcd(\mu f(x), \mu b(x)) = 1$.
Hence $g(x) + (f(x)) \in (p^k + (f(x))$

$$I \subseteq (p^k + (f(x)). \tag{4.3}$$

Also $p^k + (f(x) \in I$ where $gcd(\mu f(x), \mu b(x)) = 1$. But the by lemma 13 $f(x)$ and $b(x)$ are coprime. Hence there exist $p(x)$, $q(x) \in Z_{p^m}[x]$ such that

$$1 = p(x)f(x) + q(x)b(x)$$

$$p^k + (f(x))) = (q(x)p^k + (f(x)))(b(x)p^k + (f(x))) \in I$$

$$(p^k + (f(x))) \in I. \tag{4.4}$$

From (4.3) and (4.4) $I = (p^k + (f(x)))$

□

4.2 The ideals of $Z_{p^m}[x]/(x^n - 1)$

Lemma 14. *Let $f_1(X), f_2(X), ..., f_k(X)$ be k pairwise coprime polynomials over Z_{p^m} and Let $\hat{f}_i(X)$ denote the product of all $f_j(X)$ except $f_i(X)$, Then $\hat{f}_i(X)$ and $f_i(X)$ are coprime for $i = 1, 2, ..., k$.*

Proof. By Lemma 13 the coprimeness of $f_i(X)$ and $f_j(X)$ for $i \neq j$ implies the coprimeness of $\mu f_i(X)$ and $\mu f_j(X)$. But $\mu f_1(X), \mu f_2(X), ..., \mu f_k(X)$ are polynomials over Z_2. So $\mu \hat{f}_i(X) = \mu f_1(X)...\mu f_{i-1}(X), \mu f_{i+1}(X)...\mu f_k(X)$ and $\mu f_i(X)$ are coprime. Again by Lemma 13, $\hat{f_i(X)}$ and $f_i(X)$ are coprime. □

Lemma 15. *Let $f_1(X), f_2(X), ..., f_k(X)$ be k pairwise coprime polynomials in $Z_{p^m}[X]$, then*

$$(f_1(X)f_2(X)...f_k(X)) = (f_1(X)) \cap (f_2(X)) \cap ... \cap (f_k(X)).$$

Proof. Clearly, $(f_1(X), f_2(X), ..., f_k(X)) \in (f_i(X))$ for every i. Therefore

$$(f_1(X)f_2(X)...f_k(X)) \subseteq (f_1(X)) \cap (f_2(X)) \cap ... \cap (f_k(X)).$$

It remains to prove that

$$(f_1(X)f_2(X)...f_k(X)) \supseteq (f_1(X)) \cap (f_2(X)) \cap ... \cap (f_k(X)).$$

We apply induction on k . The case $k = 1$ is trivial. Let $k > 1$ and assume that it's holds for $k - 1$. That is, we have

$$(f_1(X)f_2(X)...f_{k-1}(X)) = (f_1(X)) \cap (f_2(X)) \cap ... \cap (f_{k-1}(X)).$$

Let

$$g(X) \in (f_1(X)) \cap (f_2(X)) \cap ... \cap (f_k(X)),$$

then

$$g(X) \in (f_1(X)f_2(X)...f_{k-1}(X)) \cup (f_k(X)).$$

Thus there are polynomials $q_1(X)$, $q_2(X) \in Z_{p^m}[X]$ such that

$$g(x) = q_1(X)f_1(X)f_2(X)...f_{k-1}(X) = q_2 f_k(x).$$

By lemma 14 $f_1(X)f_2(X)...f_{k-1}(X)$ and $f_k(x)$ are coprime. Then there are polynomials $h_1(X)$, $h_2(X) \in Z_p^m[X]$ such that

$$h_1(X)f_1(X)f_2(X)...f_{k-1}(X) + h_2(X)f_k(x) = 1.$$

Multiplying the last equation by $g(X)$, we obtain

$$g(x)h_1(X)f_1(X)f_2(X)...f_{k-1}(X) + g(x)h_2(X)f_k(x) = g(x)$$

$$g(x) = (q_2h_1(X) + q_1(X)h_2(X))f_1(X)f_2(X)...f_{k-1}(X)f_k(x).$$

Thus $g(x) \in (f_1(X)f_2(X)...f_{k-1}(X)f_k(x))$. Which compleat the proof. $\square$

Theorem 4.2.1. *Let $f_1(X), f_2(X), ..., f_k(x)$ be k pairwise coprime polynomials of degree ≥ 1 over Z_{p^k} and $a_1(X), a_2(X), ..., a_k(X)$ be any k polynomials over Z_{p^k}. Then the simultaneous congruences*

$$x \equiv a_1(X)(mod f_1(X))$$

$$x \equiv a_2(X)(mod f_2(X))$$

$$\vdots$$

$$x \equiv a_K(X)(modf_k(X)).$$

has a solution in $Z_{p^k}[X]$.
Moreover, the solution is unique $modf_1(X)f_2(X)\cdots f_k(x)$, *i.e., if* $g(X)$ *and* $h(X)$ *are two solutions , then*

$$g(X) \equiv h(X)(modf_1(X)f_2(X)...f_k(x)).$$

Proof. By Lemma 14 $\hat{f}_i(X)$ and $f_i(X)$ are coprime, $i = 1, 2, ..., k$. Then there are polynomials $b_i(X)$ and $q_i(X)$ over Z_{p^k} such that

$$b_i(X)\hat{f}_i(X) + q_i(X)f_i(X) = 1. \tag{4.5}$$

It is easy to verify that

$$a_1b_1\hat{f}_1(X) + a_2b_2\hat{f}_2(X) + \cdots + a_kb_k\hat{f}_k(X) \tag{4.6}$$

is a solution of the system.

Now let $g(X)$ and $h(X)$ be two solutions of the system.
Then $g(X) \equiv h(X)(modf_i(X))$, $i = 1, 2, ..., k$.
That is, $g(X) - h(X) \in (f_i(X))$, $i = 1, 2, ..., k$. By Lemma 15

$$g(X) - h(X) \in f_1(X)f_2(X)...f_k(x)$$

That is,

$$g(X) \equiv h(X)(modf_1(X)f_2(X)...f_k(x)).$$

□

Theorem 4.2.2. *Let* $f_1(X), f_2(X), ..., f_k(x)$ *be* k *pairwise coprime polynomials of degree* ≥ 1 *over* Z_{p^k} *and* $f(x) = f_1(X)f_2(X)...f_k(x)$. *Denote the residue class ring* $Z_{p^k}/(f(X))$ *by* R. *For* $i = 1, 2, ..., k$, *let*

$$e_i = b_i(X)\hat{f}_i(X) + (f(X)), \tag{4.7}$$

where $b_i(X)$ *is the polynomial* $b_i(X)$ *appearing in (4.5). Then*

- $R_i = Re_i$ *is an ideal of* R*, and* e_i *is the identity of* R_i*,* $i = 1, 2, ..., k$*.*
- $R = R_1 \oplus R_2 \oplus ... \oplus R_k$*.*

Corollary 7. *Let* $f_1(X), f_2(X), ..., f_k(x)$ *be* k *pairwise coprime monic polynomials of degree*≥ 1 *over* Z_{p^k} *and* $f(x) = f_1(X)f_2(X)...f_k(x)$*, Then for any* $i = 1, 2, ..., k$*, the map*

$$Z_{p^k}[X]/f_i(X) \longrightarrow (Z_{p^k}[X]/(f(X))e_i = Re_i \tag{4.8}$$

$$k(X) + (f_i(X)) \longrightarrow (k(X) + (f(X)))e_i$$

is an isomorphism of rings.

Corollary 8. *Let* $f_1(X), f_2(X), ..., f_k(x)$ *be* k *pairwise coprime monic polynomials of degree*≥ 1 *over* Z_{p^k} *and* $f(x) = f_1(X)f_2(X)...f_k(x)$*, Then*

$$Z_{p^k}(x)/(f(x)) \simeq Z_{p^k}(x)/(f_1(X)) \oplus Z_{p^k}(x)/(f_2(X)) \oplus \cdots \oplus Z_{p^k}(x)/(f_k(X))$$

Lemma 16. *Let* n *be an odd positive integer and* $x^n - 1 = f_1(X)f_2(X)...f_k(x)$ *be the unique factorization of* $x^n - 1$ *into basic irreducible polynomials over* Z_{p^k}*. Then under the isomorphism (4.8), the ideals* (0)*,* $(1 + (f_i(X)))$*, and* $(p^k + (f_i(X)))$ *of* $Z_{p^k}[X]/(f_i(X))$ *are mapped into* (0)*,* $(\hat{f}_i(X) + (x^n - 1))$ *and* $(p^k\hat{f}_i(X) + (x^n - 1))$ *of* $R_i = Re_i$*, respectively.*

Proof. Under the isomorphism (4.8), we have

$$1 + (f_i(X)) \longrightarrow (1 + (x^n - 1))e_i.$$

By (4.7), $e_i = b_i(X)\hat{f}_i(X) + (x^n - 1)$. Therefore

$$1 + (f_i(X)) \longrightarrow b_i(X)\hat{f}_i(X) + (x^n - 1).$$

Clearly,

$$b_i(X)\hat{f}_i(X) + (x^n - 1) \in (\hat{f}_i(X) + (x^n - 1)).(*)$$

Multiplying both sides of (4.5) by $\hat{f}_i(X)$, we obtain

$$b_i(X)\hat{f}_i(X)\hat{f}_i(X) + C_i(X)(x^n - 1) = \hat{f}_i(X).$$

Then

$$b_i(X)\hat{f}_i(X)\hat{f}_i(X) + (x^n - 1) = \hat{f}_i(X) + (x^n - 1),$$

which implies

$$\hat{f}_i(X) + (x^n - 1) \in (b_i(X)\hat{f}_i(X) + (x^n - 1)).(**)$$

Therefore

$$(b_i(X)\hat{f}_i(X) + (x^n - 1)) = (\hat{f}_i(X) + (x^n - 1)), (by * and **)$$

and the image of $(1 + (f_i(X)))$ under (4.8) is $(\hat{f}_i(X) + (x^n - 1))$.
Similarly, we can prove that the image of $(p^k + (f, (X)))$ under (4.8) is $(p^k \hat{f}_i(x) + (x^n - 1))$. □

Theorem 4.2.3. *[23] Let p be a prime such that p dose not divide n. Let $x^n - 1 = f_1 f_2 \dots f_k$, be a product of basic irreducible and pairwise coprime polynomials in $Z_{p^m}[x]$. Then any ideal in the ring $Z_{p^m}[x]/(x^n - 1)$ is a sum of ideal $(p^j \hat{f}_i) + (x^n - 1)$, where $0 \le j \le m - 1$.*

Proof. By theorem (3.2.4) the factorization of $x^n - 1$ exists and is unique. By corollary 8

$$Z_{p^k}[x]/(x^n-1) = Z_{p^k}[x]/(f_1) \oplus Z_{p^k}[x]/(f_2) \oplus Z_{p^k}[x]/(f_3) \oplus \cdots \oplus Z_{p^k}[x]/(f_k).$$

if I is an ideal of $Z_{p^k}[x]/(x^n - 1)$, then

$$I \simeq I_1 \oplus I_2 \oplus \cdots \oplus I_k,$$

where I_i is an ideal of the ring $Z_{p^k}[x]/(f_i)$, for $i = 1, 2, \cdots, k$. By theorem (3.2.5),

$$I_i = 0, Z_{p^k}[x]/(f_i) or (p^k + (f_i)).$$

By theorem (16) $I_i = Z_{p^k}[x]/(f_i)$, then it corresponds to the ideal $(\hat{f}_i)$ in the ring $Z_{p^k}[x]/(x^n - 1)$, if $I_i = (p^k + (f_i))$, then it corresponds to the ideal $(p^k \hat{f}_j + (x^n - 1))$. In any case, the ideal I is a sum of $(\hat{f}_i + (x^n - 1))$ and $(p^k \hat{f}_j + (x^n - 1))$. □

Corollary 9. *[31] Let p be a prime that dose not divide n . Assume $x^n - 1$ is a product of k basic irreducible parwise coprime polynomials in $Z_{p^m}[x]$. Then there are $(m + 1)^k$ cyclic codes over Z_{p^k} of length n.*

Proof. Let $x^n - 1 = g_1(x)g_2(x)...g_k(x)$ be the factorization of $x^n - 1$ into monic basic irreducible polynomials. If C is a cyclic code, by the previous theorem $C = (p^{i_1}\hat{g_1}) \oplus ... \oplus (p^{i_k}\hat{g_k})$ where $i_i \in [0, m]$. Hence there is $(m+1)^k$ cyclic codes. $\square$

4.3 $Z_{p^m}[x]/x^n - 1$ is a principal ideal ring

The following theorem is generalization for theorem 3.3.4

Theorem 4.3.1. *[23] Let p be a prime such that p dose not divide n, and C is a Z_{p^m} acyclic code, then there exist a collection of pairwise coprime polynomials $F_0, F_1, ..., F_m$ such that $C = (\hat{F_1}, p\hat{F_2}, ..., p^{m-1}\hat{F_m})$ where $x^n - 1 = F_0F_1...F_m$, and $|c| = p^{\sum_{i=0}^{m-1}(m-i)degF_{i+1}}$*

Proof. We know that $x^n - 1$ has a unique factorization such that

$$x^n - 1 = f_1 f_2 \cdots f_r,$$

where thef_i are unique basic irreducible and pairwise coprime. Since $x^n - 1$ is monic $f_i s$ may be chosen to be monic, We also know, by the previous theorem, that C is a sum of ideals of the type $(p^j\hat{f_i}) + (x^n - 1)$. By permuting the subscripts of f_i, we can suppose that C is a sum of

$$(\hat{f}_{k_1+1}), (\hat{f}_{k_1+2}), \cdots, (\hat{f}_{k_1+k_2}), (p\hat{f}_{k_1+k_2+1}), (p\hat{f}_{k_1+k_2+2}), \cdots,$$

$$(p\hat{f}_{k_1+k_2+k_3}), \cdots, (p^{m-1}\hat{f}_{k_1+k_2+...+k_m+1}), ..., (p^{m-1}\hat{f}_r).$$

Then

$$C = (f_1 f_2 \cdots f_{k_1} f_{k_1+k_2+1} f_{k_1+k_2+2} \cdots f_r; p f_1 f_2 \cdots f_{k_1} f_{k_1+1}$$

$$\cdots f_{k_1+k_2} f_{k_1+k_2+k_3+1}, \cdots, f_r; \cdots; p^{m-1} f_1 f_2, \cdots, f_{k_1+k_2+...+k_m}).$$

For $0 \leq i \leq m$, let

$$F_i = f_{k_1+k_2+...+k_i+1} ... f_{k_1+k_2+...+k_{i+1}}.$$

Hence

$$C = (\hat{F}_1, p\hat{F}_2, ..., p^{m-1}\hat{F}_m).$$

Since F_is are pairwise coprime thus

$$C = \hat{F}_1 \oplus p\hat{F}_2 \oplus ... \oplus p^{m-1}\hat{F}_m.$$

Therefor,

$$|C| = |\hat{F}_1||p\hat{F}_2|...|p^{m-1}\hat{F}_m|$$
$$= p^{m(n-deg\hat{F}_1)}p^{(m-1)(n-deg\hat{F}_2)}...p^{(n-deg\hat{F}_m)}$$
$$= p^{\sum_{i=0}^{m-1}(m-i)degF_{i+1}}$$

□

Theorem 4.3.2. *[23][7] Let p be a prime such that p dose not divide n, and C any Z_{p^m} acyclic code, then C has the form*

$$C = (f_0, pf_1, p^2f_2, ..., p^{m-1}f_{m-1})$$

where the f_is satisfying

$$f_{m-1}|f_{m+2}|...|f_0|x^n - 1$$

Proof. With the notations of Theorem 4.3.1

$$C = (\hat{F}_1, p\hat{F}_2, ..., p^{m-1}\hat{F}_m).$$

For $0 \leq i \leq m-2$, let $f_i = F_0F_{i-2}...F_m$ and $f_{m-1} = F_0$. Then

$$f_{m-1}|f_{m-2}|...|f_0|x^n - 1.$$

Also for all $0 \leq i \leq m-1$ $p_i\hat{F}_{i+1} = p^iF_0F_1...F_iF_{i+2}...F_m = p^if_iF_1F_2...F_i$. Hence,

$$C \subseteq (f_0, pf_1, ..., p^{m-1}f_{m-1}).$$

To prove the reverse inclusion first observe that $f_0 \in C$. As F_1 and F_2 are coprime, there exist polynomials $a(x)$, $b(x) \in Z_{p^m}[x]$ such that

$$1 = a(x)F_1(x) + b(x)F_2(x).$$

Thus,

$$pf_1 = pF_0F_3...F_m = pa(x)F_0F_1F_3...F_m + pb(x)f_0 = pa(x)\hat{F}_2 + pb(x)f_0 \in C.$$

Proceeding like this we get $p^i f_i \in C$ for all i, $0 \leq i \leq m-1$. Thus,

$$C = (f_0, pf_1, ..., p^{m-1}f_{m-1})$$

$\square$

Corollary 10. *[23][7] If p is a prime not dividing n then $Z_{p^m}/(x^n-1)$ is a principal ideal ring.*

Proof. With the notations of Theorem 4.3.1,$C = (\hat{F}_1, p\hat{F}_2, ..., p^{m-1}\hat{F}_m)$. Let $G = \hat{F}_1 + p\hat{F}_2 + ... + p^{m-1}\hat{F}_m$. We shall prove that $C = (G)$. First observe that $\hat{F}_i\hat{F}_j = 0$ in $Z_{p^n}/(x^n-1)$ for $0 \leq i, j \leq m$, and $i \neq j$.
Also, since $\hat{F}_i, F_i$ are coprime polynomials for all i such that $1 \leq i \leq m$, there exist q_i, r_i such that $q_i\hat{F}_i + r_iF_i = 1$. It follows that, for all k such that $1 \leq k \leq m$, $\prod_{i=1}^{k}(q_i\hat{F}_i + r_iF_i) = 1$. Therefore, for all k, there exist polynomials $a_{k0}, a_{k1}, ..., a_{kk}$ such that

$$a_{k0}F_1F_2...F_k + a_{k1}\hat{F}_1F_2...F_k + a_{k2}F_1\hat{F}_2...F_k... + a_{kk}F_1F_2...\hat{F}_k = 1.$$

Multiplying by $p^{m-1}\hat{F}_m$ on both sides of the version of the above equation with $k = m-1$, we obtain

$$p^{m-1}\hat{F}_m = p^{m-1}a_{m-1}F_1F_2...F_{m-1}\hat{F}_m.$$

On the other hand,

$$F_1F_2...F_m - 1G = p^{m-1}F_1F_2...F_{m-1}\hat{F}_m.$$

Consequently, $p^{m-1}\hat{F}_m \in (G)$ and, thus, $H = \hat{F}_1 + p\hat{F}_2 + ... + p^{m-2}\hat{F}_{m-1} \in (G)$. A similar argument yields

$$p^{m-2}\hat{F}_{m-1} = p^{m-2}a_{m-2}F_1F_2...F_{m-2}\hat{F}_{m-1}$$

and

$$F_1F_2...F_{m-2}H = p^{m-2}F_1F_2...F_{m-2}\hat{F}_{m-1}.$$

So, we get $p^{m-2}\hat{F}_{m-1} \in (G)$ and, hence,

$$\hat{F}_1 + p\hat{F}_2 + ... + p^{m-3}\hat{F}_{m-2} \in (G).$$

Continuing on like this, we conclude that

$$\hat{F}_1, p\hat{F}_2, p^2\hat{F}_3, ..., p^{m-1}\hat{F}_m \in (G).$$

This completes the proof. □

4.4 Dual cyclic code

Lemma 17. *[8] The number of elements in any nonzero linear code C over Z_{p^m} is of the form p^k. And the dual code has p^l codewords were $k + l = mn$*

Theorem 4.4.1. *[23][7] Let p be a prime such that p dose not divide n, and $C = (\hat{F}_1, p\hat{F}_2, ..., p^{m-1}\hat{F}_m)$ where $x^n - 1 = F_0F_1...F_m$, then*

$$C^{\perp} = (\hat{F_1}^*, p\hat{F_m}^*, p^2\widehat{F_{m-1}}^* ..., p^{m-1}\hat{F_2}^*)$$

Proof. let

$$C_1 = (\hat{F_1}^*, p\hat{F_2}^*, ..., p^{m-1}\hat{F_m}^*),$$

we will prove that

$$C_1 = C^{\perp}$$

for $0 \leq i, j \leq m - 1$,

$$\begin{cases} (p^i\hat{F}_{i+1}) \quad (p^j\hat{F}^*_{m-j+1})^* \quad \textit{is} \quad \textit{divisible} \quad \textit{by} \quad x^n - 1, & \text{i+1} \neq m - j + 1 \\ (p^i\hat{F}_{i+1}) \quad (p^j\hat{F}^*_{m-j+1})^* \quad \textit{is} \quad \textit{divisible} \quad \textit{by} \quad p^n, & \text{i+1} = m - j + 1. \end{cases}$$

In any case $(p^i\hat{F}_{i+1})(p^j\hat{F}^*_{m-j+1})^* \equiv 0 \bmod (x^n - 1)$. That is $C_1 \subseteq C^{\perp}$.

On the other hand $|C_1| = p^{mdegF_0^*} p^{(m-1)degF_m^*} ... p^{degF_2^*} = p^{\sum_{i=1}^{m} idegF_{i+1}^*}$. But $degF = degF^*$, so

$$|C_1| = p^{\sum_{i=1}^{m} idegF_{i+1}^*}.$$

And

$$|C^\perp| = p^l$$

where

$$l = mn - \sum_{i=0}^{m-1} (m-i)degF_{i+1}$$

$= mn - (mdegF_1 + (m-1)degF_2 + (m-2)degF_3 + ... + (m-(m-1))degF_m)$.

$= m(n - degF_1 - degF_2 - ... - degF_m) + degF_2 + 2degF_3 + 3degF_4 + ... + mdegF_{m+1}$.

$$= \sum_{i=1}^{m} idegF_{i+1}.$$

Hence $C_1 = C^\perp (C_1 \subseteq C^\perp, |C_1| = |C^\perp|)$. □

Theorem 4.4.2. *[23] Let p be a prime such that p dose not divide n, and*

$$C = (\hat{F_1}, p\hat{F_2}, ..., p^{m-1}\hat{F_m})$$

where $x^n - 1 = F_0 F_1 ... F_m$, then C is self dual if and only if for $0 \leq i, j \leq m$, $i + j \equiv 1 (mod \quad m+1)$, then F_i is an associate of F_j^* .

Proof. Assume C is self dual, for $0 \leq i, j \leq m$, if $i + j \equiv 1 (mod \quad m+1)$ let $g_i = F_j^*$

$$x^n - 1 = F_0 F_1 ... F_m,$$

$$(x^n - 1)^* = (F_0 F_1 ... F_m)^* = g_0 g_1 ... g_m.$$

Hence

$$x^n - 1 = -g_0 g_1 ... g_m = F_0 F_1 ... F_m,$$

and

$$C^\perp = (\hat{g}_1, p\hat{g}_2, p^2\hat{g}_3, ..., p^{m-1}\hat{g}_m)$$

Not that $g_0 = F_1^*$, $g_2 = F_m^*$,...$\hat{g}_i = \hat{F}_i$, $0 \leq i \leq m$.
Hence F_i is an associate F_j^*.

To prove the other direction assume that for $0 \leq i, j \leq m$, if $i + j \equiv 1(mod \quad m+1)$, then $c_i F_i = F_j^*$,where $c_i \in Z_{p^n}$

$$C^{\perp} = (\hat{F_0}^*, p\hat{F_m}^*, ..., p^{m-1}\hat{F_2}^*)$$

$$= (c_1\hat{F}_1, pc_2\hat{F}_2, p^2c_3\hat{F}_3, ..., p^{m-1}c_{m-1}\hat{F}_m)$$
$$= (\hat{F}_1, p\hat{F}_2, ..., p^{m-1}\hat{F}_m) = C.$$

Hence, C is self orthogonal. $\square$

Chapter 5

Codes over finite chain ring

In this chapter, the the generalization of the methods of chapters [2.2] and [4] has been studied to obtain cyclic and self dual cyclic codes over finite chain rings with the condition that the length of the code is not divisible by the characteristic of the residue field .

5.1 The ideals of $R[x]/(f(x))$

Theorem 5.1.1. *[12] For a finite commutative ring R the following are equivalent:*
1. R is a local ring and the maximal ideal is principal.
2. R is a local principal ideal ring.
3.R is a chain ring.

Proof. (1) $\rightarrow$ (2) Let I be an ideal of R, if $I = R$ then $1 \in I$ and $I = R = (1)$. If $I \neq R$, then $I \subseteq (a)$ where (a) is the maximal principal ideal. Therefor

$I = a^k$ for some positive integer k.

(2) $\rightarrow$ (3) Let R be a local principal ideal ring with the maximal ideal (a) A and B be proper ideals of R. then $A = (a^i)$ and $B = (b^j)$ for some positive integers i and j less than the nilpotency of a. Hence $A \subseteq B$ or $B \subseteq A$.
Thus R is a chain ring.

(3) $\rightarrow$ (1) Assume R is a finite chain ring, then R has unique maximal ideal hence R is a local ring, to prove that the maximal ideal is principal suppose that the maximal ideal contains a and b in the generating set of it. Hence, b does not belong to the ideal aR and a does not belong to the ideal aR, aR not a subset of bR and bR not a subset of aR and this implies that R is not a chain.

$\square$

Let $\mu : R[x] \rightarrow R[x]/(a)$ be the map which sends r to $r + (a)$, and x to x, where (a) is the maximal ideal ring.

$$r_0+r_1x+...+r_{m-1}x^{m-1}+(f(X)) \longrightarrow \mu r_0+\mu r_1x+\cdots+\mu r_{m-1}x^{m-1}+(\mu f(X)), \tag{5.1}$$

Theorem 5.1.2. *[12] Let R be a finite chain ring with the maximal ideal (a), and t be the nilpotency of a , If $f(x) \in Z_{p^m}[x]$ is a basic irreducible polynomial then the ideals of the chain ring $R[x]/(f(x))$ are precisely (0), $(1 + (f(x)))$, $(a + (f(x)))$,..., $(a^{t-1} + (f(x)))$.*

Proof. Suppose I is a nonzero ideal of the ring $R[x]/(f(x))$ and $g(x) + (f(x)) \in I$ for some $g(x)$ which is not belong $(f(x))$. Since $\mu f(x)$ is irreducible in $R[x]/(a)$
$gcd(\mu g(x), \mu f(x)) = 1$ or $\mu f(x)$.
If $gcd(\mu f(x), \mu g(x)) = 1$, then there exist $d(x)$,$b(x) \in R[x]$ such that

$$\mu d(x)\mu f(x) + \mu b(x)\mu g(x) = 1$$

$$d(x)f(x) + b(x)g(x) = 1 + as(x),$$

$s(x) \in R[x]$. Since $1 + as(x)$ is invertible, then $1 \in R[x]$ by definition 44 this showing that $f(x)$ and $g(x)$ are coprime.*
There exists $u(x)$ and $v(x)$ such that $1 = f(x)u(x) + g(x)v(x)$.
But then $(g(x) + (f(x)))(v(x) + (f(x))) = 1 + (f(x))$.
Therefore $g(x) + (f(x))$ is invertible. Hence, $g(x) + (f(x))$ is invertible.

$$I = R[x]/(f(x)) = (1).$$

If $gcd(\mu f(x), \mu g(x)) = \mu f(x)$,then $\mu f(x)|\mu g(x)$.
Hence there exists $d(x), b(x) \in R$ such that

$$g(x) = d(x)f(x) + ab(x)$$

where $gcd(\mu f(x), \mu b(x)) = 1$.
Hence $g(x) + (f(x)) \in (a + (f(x))$

$$I \subseteq (a + (f(x)). \tag{5.2}$$

Also $a + (f(x)) \in I$ where $gcd(\mu f(x), \mu b(x)) = 1$. Hence, $f(x)$ and $b(x)$ are coprime in R from *.
So there exist $p(x)$, $q(x) \in R[x]$ such that

$$1 = p(x)f(x) + q(x)b(x)$$

$$a + (f(x))) = (q(x)a + (f(x)))(b(x)a + (f(x))) \in I$$

$$(a + (f(x))) \in I. \tag{5.3}$$

From (5.2) and (5.3) $I = (a + (f(x)))$

□

5.2 The ideals of $R[x]/(x^n - 1)$

Lemma 18. *[38]* ***Chinese remainder theorem***
Let R be a commutative ring. If $I_1, ..., I_k$ are pairwise coprime ideals of R,

then the product I of these ideals equal to there intersection, and the quotient ring R/I is isomorphic to $R/I_1 \times ... \times R/I_k$ via the following map:

$$f : R/I \to R/I_1 \times \cdots \times R/I_k \tag{5.4}$$
$$f(x + I) = (x + I_1, \ldots, x + I_k) \tag{5.5}$$

Theorem 5.2.1. *[26] If f is a monic polynomial over the chain ring R such that μf is a square free, then f factors uniquely as a product of monic basic irreducible pairwise coprime polynomial.*

Theorem 5.2.2. *[23] Let $< a >$ be the maximal ideal of the finite chain ring R, and t the nilpotency of a. Let $x^n - 1 = f_1 f_2 \ldots f_k$, be a product of basic irreducible and pairwise coprime polynomials in $R[x]$. Then any ideal in the ring $R[x]/(x^n - 1)$ is a sum of ideal $(a^j \hat{f}_i) + (x^n - 1)$, where $0 \leq j \leq t$.*

Proof. By theorem (5.2.1) the factorization of $x^n - 1$ exists and is unique. By theorem 18

$$R[x]/(x^n - 1) = R[x]/(f_1) \oplus R[x]/(f_2) \oplus R[x]/(f_3) \oplus \cdots \oplus R[x]/(f_k).$$

if I is an ideal of $R[x]/(x^n - 1)$, then

$$I \simeq I_1 \oplus I_2 \oplus \cdots \oplus I_k,$$

where I_i is an ideal of the ring $R[x]/(f_i)$, for $i = 1, 2, \cdots, k$. By theorem (5.1.2),

$$I_i = 0, \quad or \quad (a^r + (f_i)). \quad r \in \{1, 2, ..., t - 1.\}$$

Since $I_i = (a^r + (f_i))$ corresponds to the ideal $(a^r \hat{f}_i + (x^n - 1))$ in the ring $R[x]/(x^n - 1)$. Consequently I is a sum of ideals of the form $(a^j \hat{f}_i) + (x^n - 1)$. ☐

Corollary 11. *[12] Let $< a >$ be the maximal ideal of the finite chain ring R, and t the nilpotency of a. Let $x^n - 1 = f_1 f_2 \ldots f_k$, be a product of basic irreducible and pairwise coprime polynomials in $R[x]$.*
Then there are $(t + 1)^k$ cyclic codes over R of length n.

Proof. Let $x^n - 1 = f_1(x) f_2(x) ... f_k(x)$ be the factorization of $x^n - 1$ into monic basic irreducible polynomials. If C is a cyclic code, by the previous theorem $C = (a^{i_1} \hat{f}_1) \oplus ... \oplus (a^{i_k} \hat{f}_k)$ where $i_i \in \{0, .., t\}$. Hence there are $(t + 1)^k$ cyclic codes. ☐

5.3 $R[x]/(x^n - 1)$ is a principal ideal ring

Theorem 5.3.1. *[12] Let (a) be the maximal ideal of the finite chain ring R, and t the nilpotency of a. Let C be a acyclic code over R , then there exist a unique collection of pairwise coprime polynomials $F_0, F_1, ..., F_t$ such that*

$$C = (\hat{F}_1, a\hat{F}_2, ..., a^{t-1}\hat{F}_t)$$

where $x^n - 1 = F_0F_1...F_t$, and

$$|C| = |R/(a)|^{\sum_{i=0}^{t-1}(t-i)degF_{i+1}}$$

Proof. We know that $x^n - 1$ has a unique factorization such that

$$x^n - 1 = f_1f_2 \cdots f_r,$$

where thef_i are unique basic irreducible and pairwise coprime. Since $x^n - 1$ is monic f_is may be chosen to be monic, We also know, by the previous theorem, that C is a sum of ideals of the type $(a^j\hat{f}_i) + (x^n - 1)$. By permuting the subscripts of f_i, we can suppose that C is a sum of

$$(\hat{f}_{k_1+1}), (\hat{f}_{k_1+2}), \cdots, (\hat{f}_{k_1+k_2}), (a\hat{f}_{k_1+k_2+1}), (a\hat{f}_{k_1+k_2+2}), \cdots,$$
$$(a\hat{f}_{k_1+k_2+k_3}), \cdots, (a^{m-1}\hat{f}_{k_1+k_2+...+k_t+1}), ..., (t^{m-1}\hat{f}_r).$$

Then

$$C = (f_1f_2 \cdots f_{k_1}f_{k_1+k_2+1}f_{k_1+k_2+2} \cdots f_r; af_1f_2 \cdots f_{k_1}f_{k_1+1}$$
$$\cdots f_{k_1+k_2}f_{k_1+k_2+k_3+1}, \cdots, f_r; \cdots; a^{t-1}f_1f_2 \cdots f_{k_1+k_2+...+k_t}).$$

For $0 \leq i \leq t$, let

$$F_i = f_{k_1+k_2+...+k_i+1} ... f_{k_1+k_2+...+k_{i+1}}.$$

Hence

$$C = (\hat{F}_1, p\hat{F}_2, ..., p^{t-1}\hat{F}_t).$$

Since F_is are pairwise coprime thus

$$C = \hat{F}_1 \oplus p\hat{F}_2 \oplus ... \oplus p^{t-1}\hat{F}_t.$$

Therefor,

$$|C| = |\hat{F}_1||a\hat{F}_2|...|a^{t-1}\hat{F}_t|$$
$$= |R/(a)|^{t(n-deg\hat{F}_1)}|R/(a)|^{(t-1)(n-deg\hat{F}_2)}...|R/(a)|^{(n-deg\hat{F}_t)}$$
$$= |R/(a)|^{\sum_{i=0}^{t-1}(t-i)degF_{i+1}}$$

□

Corollary 12. *[32] Suppose C is a acyclic code of length n over the ring $F_p + uF_p + ... + u^{k-1}F_p$, p is not devisable by n, then there exist a unique collection of pairwise coprime polynomials $F_0, F_1, ..., F_k$ such that*

$$C = (\hat{F}_1, u\hat{F}_2, ..., u^{k-1}\hat{F}_k)$$

where $x^n - 1 = F_0F_1...F_k$, and

$$|C| = p^{\sum_{i=0}^{k-1}(k-i)degF_{i+1}}$$

Theorem 5.3.2. *[12] Let (a) be the maximal ideal of the finite chain ring R, and t the nilpotency of a, and C any R cyclic code, then C has the form*

$$C = (f_0, af_1, a^2f_2, ..., a^{m-1}f_{m-1})$$

where the f_is satisfying

$$f_{m-1}|f_{m-2}|...|f_0|x^n - 1$$

Proof. With the notations of Theorem 5.3.1

$$C = (\hat{F}_1, a\hat{F}_2, ..., a^{m-1}\hat{F}_m).$$

For $0 \leq i \leq t-2$, let $f_i = F_0F_{i-2}...F_t$ and $f_{t-1} = F_0$. Then

$$f_{m-1}|f_{m-2}|...|f_0|x^n - 1.$$

Also for all $0 \leq i \leq m-1$ $a_i\hat{F}_{i+1} = a^iF_0F_1...F_iF_{i+2}...F_m = a^if_iF_1F_2...F_i$. Hence,

$$C \subseteq (f_0, af_1, ..., a^{m-1}f_{m-1}).$$

To prove the reverse inclusion first observe that $f_0 \in C$. As F_1 and F_2 are coprime, there exist polynomials $g(x)$, $b(x) \in R[x]$ such that

$$1 = g(x)F_1(x) + b(x)F_2(x).$$

Thus,

$$af_1 = aF_0F_3...F_m = ag(x)F_0F_1F_3...F_m + ab(x)f_0 = ag(x)\hat{F}_2 + ab(x)f_0 \in C.$$

Proceeding like this we get $a^i f_i \in C$ for all i, $0 \leq i \leq m-1$. Thus,

$$C = (f_0, af_1, ..., a^{m-1}f_{m-1})$$

□

Corollary 13. *[3] Suppose C is a acyclic code of length n relatively prime to q over the ring $F_q + uF_q + ... + u^{k-1}F_q$, which has (u) as a maximal ideal ring and k is a nilpotent index of then C has the form*

$$C = (f_0, uf_1, u^2f_2, ..., u^{k-1}f_{k-1})$$

where the f_is satisfying

$$f_{k-1}|f_{k-2}|...|f_0|x^n - 1$$

Corollary 14. *[12] $R[x]/(x^n-1)$ is a principal ideal ring.*

Proof. With the notations of Theorem 5.3.1, $C = (\hat{F}_1, a\hat{F}_2, ..., a^{t-1}\hat{F}_t)$. Let $G = \hat{F}_1 + a\hat{F}_2 + ... + a^{t-1}\hat{F}_t$. We shall prove that $C = (G)$. First observe that $\hat{F}_i\hat{F}_j = 0$ in $R[x]/(x^n-1)$ for $0 \leq i, j \leq t$, and $i \neq j$.
Also, since $\hat{F}_i, F_i$ are coprime polynomials for all i such that $1 \leq i \leq t$, there exist q_i, r_i such that $q_i\hat{F}_i + r_iF_i = 1$. It follows that, for all k such that $1 \leq k \leq t$, $\prod_{i=1}^{k}(q_i\hat{F}_i + r_iF_i) = 1$. Therefore, for all k, there exist polynomials $g_{k0}, g_{k1}, ..., g_{kk}$ such that

$$g_{k0}F_1F_2...F_k + g_{k1}\hat{F}_1F_2...F_k + g_{k2}F_1\hat{F}_2...F_k... + g_{kk}F_1F_2...\hat{F}_k = 1.$$

Multiplying by $a^{t-1}\hat{F}_t$ on both sides of the version of the above equation with $k = t-1$, we obtain

$$a^{t-1}\hat{F}_t = a^{t-1}g_{t-1,0}F_1F_2...F_{t-1}\hat{F}_t.$$

On the other hand,

$$F_1F_2...F_{t-1}G = a^{t-1}F_1F_2...F_{t-1}\hat{F}_t.$$

Consequently, $a^{t-1}\hat{F}_t \in (G)$ and, thus, $H := \hat{F}_1 + a\hat{F}_2 + ... + a^{t-2}\hat{F}_{t-1} \in (G)$. A similar argument yields

$$a^{t-2}\hat{F}_{t-1} = a^{t-2}a_{t-2}F_1F_2...F_{t-2}\hat{F}_{t-1}$$

and

$$F_1F_2...F_{m-2}H = a^{t-2}F_1F_2...F_{t-2}\hat{F}_{t-1}.$$

So, we get $a^{t-2}\hat{F}_{t-1} \in (G)$ and, hence,

$$\hat{F}_1 + a\hat{F}_2 + ... + a^{t-3}\hat{F}_{t-2} \in (G).$$

Continuing on like this, we conclude that

$$\hat{F}_1, a\hat{F}_2, a^2\hat{F}_3, ..., a^{t-1}\hat{F}_t \in (G).$$

This completes the proof. □

Corollary 15. *[3] The ring*

$$F_q[x] + uF_q[x] + ... + u^{k-1}F_q[x]/(x^n - 1)$$

is a principal ideal ring.

5.4 Dual cyclic code

Lemma 19. *[26] Let R be a finite commutative chain ring, with maximal ideal (a), let t be the nilpotency then*
1. The characteristic of R and $R/(a)$ are powers of p where p is some prime, and $|R| = p^k$, $|R/(a)| = p^l$ for some integers k, l and $k \geq l$.
2. $|R| = |R/(a)|^t$ i.e. $k = lt$.

Lemma 20. *[8] Let R be a finite commutative chain ring of order p^{ι}. The number of elements in any nonzero linear code C of length n over R is of the form p^k where $k \in \{1, 2, ..., \iota n\}$. And the dual code has p^l codewords were $k + l = \iota n$.*

Theorem 5.4.1. *[12] Let (a) be the maximal ideal of the finite chain ring R, and t the nilpotency of a, and*

$$C = (\hat{F}_1, a\hat{F}_2, ..., a^{t-1}\hat{F}_t)$$

where $x^n - 1 = F_0F_1...F_t$, then

$$C^{\perp} = (\hat{F_1}^*, a\hat{F_t}^*, ..., a^{t-1}\hat{F_2}^*)$$

$$|C| = |R/(a)|^{\sum_{i=0}^{t-1} degiF_{i+1}}$$

Proof. let

$$C_1 = (\hat{F_1}^*, a\hat{F_t}^*, ..., a^{t-1}\hat{F_2}^*),$$

we will prove that

$$C_1 = C^{\perp}$$

$$\begin{cases} (a^i\hat{F}_{i+1}) \quad (a^j\hat{F}^*_{t-j+1})^* \quad is \quad divisible \quad by \quad x^n - 1, & \text{i+1} \neq t - j + 1 \\ (a^i\hat{F}_{i+1}) \quad (a^j\hat{F}^*_{m-j+1})^* \quad is \quad divisible \quad by \quad a^t, & \text{i+1} = m - j + 1. \end{cases}$$

In any case $(a^i\hat{F}_{i+1})(a^j\hat{F}^*_{m-j+1})^* \equiv 0 \quad in \quad R[x]/(x^n-1)$. That is $C_1 \subseteq C^{\perp}$.

On the other hand

$$|C_1| = |\hat{F}^*_0||a\hat{F}^*_{t-1}|...|a^{t-1}\hat{F}^*_2|$$

$$|R/(a)|^{tdegF^*_0}|R/(a)|^{(t-1)degF^*_t}...|R/(a)|^{degF^*_2}$$

$$|C_1| = |R/(a)|^{\sum_{i=1}^{t} idegF_{i+1}} = p^{\iota\sum_{i=1}^{t} idegF_{i+1}}.$$

And

$$|C^{\perp}| = p^l$$

where

$$l = tn - \sum_{i=0}^{t-1}(t-i)degF_{i+1}$$

$= \iota tn - \iota(tdegF_1 + (t-1)degF_2 + (t-2)degF_3 + ... + (t-(t-1))degF_t)$.
$= t\iota(n - degF_1 - degF_2 - ... - degF_t) + \iota degF_2 + 2\iota degF_3 + 3\iota degF_4 + ... + t\iota degF_{t+1}$.

$$= \iota\sum_{i=1}^{t} idegF_{i+1}.$$

Hence $C_1 = C^{\perp}(C_1 \subseteq C^{\perp}, |C_1| = |C^{\perp}|)$. □

Theorem 5.4.2. *[12] Let*

$$C = (\hat{F}_1, a\hat{F}_2, ..., a^{t-1}\hat{F}_t)$$

where $x^n - 1 = F_0F_1...F_t$, then C is self dual if and only for $0 \leq i, j \leq t$, if $i + j \equiv 1(mod \quad t+1)$, then F_i is an associate of F_j^* .

Proof. Assume C is self dual, for $0 \leq i, j \leq t$, if $i + j \equiv 1(mod \quad m+1)$ let $g_i = F_j^*$

$$x^n - 1 = F_0F_1...F_t,$$

$$(x^n - 1)^* = (F_0F_1...F_t)^* = g_0g_1...g_t.$$

Hence

$$x^n - 1 = -g_0g_1...g_t = F_0F_1...F_t,$$

and

$$C^{\perp} = (\hat{g}_1, a\hat{g}_2, a^2\hat{g}_3, ..., a^{t-1}\hat{g}_t)$$

Not that $g_0 = F_1^*$, $g_2 = F_t^*$,...$\hat{g}_i = \hat{F}_i$, $0 \leq i \leq t$.
Hence F_i is an associate F_j^*.

To prove the other direction assume that for $0 \leq i, j \leq t$, if

$$i + j \equiv 1(mod \quad m+1),$$

then $c_iF_i = F_j^*$,where $c_i \in R$

$$C^{\perp} = (\hat{F_0}^*, a\hat{F_t}^*, ..., a^{t-1}\hat{F_2}^*)$$

$$= (c_1\hat{F}_1, ac_2\hat{F}_2, a^2c_3\hat{F}_3, ..., a^{t-1}c_{t-1}\hat{F}_t)$$

$$= (\hat{F}_1, a\hat{F}_2, ..., a^{t-1}\hat{F}_t) = C.$$

Hence, C is self orthogonal. $\square$

Chapter 6

Codes over noncommutative rings

In the previous chapters the cyclic codes has been characterized in terms of the factors of polynomial $x^n - 1$. This chapter investigates cyclic linear codes over arbitrary (not necessarily commutative) finite rings and prove that the characterizations in previous chapters to be true for a large class of such codes over these rings.

Definition 46. *A R* ***module*** *M is* ***free*** *if there exists a subset B of M, called a basis, such that every element in M is uniquely expressible as a linear combination of the elements in B.*

Definition 47. *[18] A submodule S of a left R module M is a direct summand of M if there exists a submodule T of M with $M = S \oplus T$. The submodule T is called a complement of S.*

Theorem 6.0.3. *Let R be a ring. The following are equivalent*

- *R is left simisimple*
- *every left R module is projective*

- *every finitely generated left R module is projective*
- *all cyclic left R module are projective.*

Theorem 6.0.4. *Let R module M is projective iff M is a direct summand of a free left R module*

Definition 48. *[24] A linear left code C of length n over a finite ring R is a submodule of ${}_RR^n$. We call C splitting if it is a direct summand of ${}_RR^n$*

Definition 49. *[24] A cyclic linear left code C of length n over a ring R is a left ideal of $R[x]/(x^n - 1)$. C is called splitting if it is a direct summand of ${}_R(R[x]/(x^n - 1))$.*

Theorem 6.0.5. *[25] Let R be a finite dimensional algebra, then either R has a zero divisor or every finite dimensional left R module is free.*

6.1 Divisors of $x^n - 1$ generate splitting codes

Lemma 21. *[24] Let R be a finite ring, and let $gh = x^n - 1$ for some $g, h \in R[x]$, then:*
(a) g and h commute, i.e. $hg = x^n - 1$.
(b)${}_R(R[x]h)$ is a free module.
(c)$R[x]g$ is a direct summand of ${}_RR[x]$.

Proof. (a) $h(gh - (x^n - 1)) = hgh - h(x^n - 1) = 0$
$hgh = h(x^n - 1)$.
Hence $hg = x^n - 1$.
(b)For the constant coefficients g_0, h_0 of g and h, respectively, we have $g_0h_0 = -1$ and hence g_0 and h_0 are units of R, since R is finite.
From theorem 1.1.1 we get that $fh = 0$ implies $f = 0$ for all $f \in F[x]$. This leads to the $R[x]$ isomorphy and hence to the R isomorphy of $R[x]$ and $R[x]h$ which proves this module to be free from theorem 6.0.5.
(c)Consider the map

$$R[x] \longrightarrow R[x]h/(x^n - 1)$$

Its kernel is $R[x]g$, and since $R[x](x^n-1)$ is a direct summand of the free module ${}_RR[x]h$, we know $R[x]h/(x^n-1)$ to be a projective R-module. This shows R[x]g to be a direct summand of ${}_RR[x]$ since $R[x](x^n-1) = R[x]g(x)h(x)$. $\square$

Corollary 16. *[24] For a finite ring R every divisor of $x^n - 1$ in $R[x]$ generates a cyclic splitting code of length n.*

Proof. Let g be a divisor of x^n-1 in $R[x]$, then by Lemma 2.1 we know $R[x]g$ to be a direct summand of ${}_RR[x]$ which contains the submodule $R[x](x^n-1)$. Hence we obtain $R[x]g/(x^n-1)$ to be a direct summand in ${}_R(R[x]/x^n-1)$ which proves our claim. $\square$

6.2 Characterization of all cyclic splitting codes

Theorem 6.2.1. *[24]*
(a) For a semisimple ring $S := R/Rad(R)$, the polynomial ring $S[x]$ is a (left and right) principal ideal ring.
(b)If R is a finite ring, then $Rad(R)[x]$ is a small submodule of ${}_RR[X]$, i.e. for any submodule U of ${}_RR[X]$ with $Rad(R)[x] + U = R[x]$ it follows that $U = R[x]$.

Proof. (a) From lemma (3) and Wedderburn's theorem S is isomorphic to an $n \times n$ matrix ring over a division ring (skew field) F, so let $S = M_n(f)$. Hence we wont to prove that $M_n(f)$[x] is a principal ideal ring. Not that $M_n(f)$[x] isomorphic to the matrix ring $M_n(F[x])$. From lemma (4) $F[x]$ is principal ideal domain, lemma (2) implies that $M_n(F[x])$ is a matrix
(b)From lemma 5 its clear that $Rad_R(M)$ is a small submodule of ${}_RM$. Now choose $M = R[x]$, together with $Rad(R)[x] = Rad(R)R[x]$ it follows that $Rad(R)[x]$ is a small submodule of ${}_RR[X]$ $\square$

Theorem 6.2.2. *[24] For a cyclic linear left code of length n over a finite ring R the following are equivalent:*

(a) C is a splitting code.
(b) There exists a divisor g of $x^n - 1$ in $R[x]$ such that $C = R[x]g/(x^n - 1)$.

Proof. $(a) \to (b)$ Assume C is a splitting cyclic linear code, that is C a direct summand of ${}_R(R[x]/(x^n - 1))$, let T be the complement of C, i.e., $T \oplus C = R[x]$ and $T \cap C = R[x](x^n - 1)$.
Define $T' := T \cap (R \oplus Rx \oplus Rx^2 \oplus ... \oplus Rx^{n-1})$, then T' is a complement of C in ${}_R R[x]$.
Now consider the natural map $\mu :_R R[x] \to_s S[x]$, let $\mu(C) = \overline{C}$.
From theorem (6.2.1) $S[x]$ is a principal ideal. Hence, there exist $g \in C$ such that $\overline{g} = \overline{C}$, define $C_0 =< g >$. Then $C_0 \leq C$ and $C_0 \cap T' = 0$ whereas $C_0 + T' + Rad(R)[x] = R[x]$. Theorem (6.2.1) yields $C_0 \oplus T' = R[x]$ and thus $C_0 = C$. Hence $C =< g >$ and because of $(x^n - 1) \leq C$ we obtain a polynomial $h \in R[x]$ such that $hg = x^n - 1$.

□

6.3 F_{p^2} Linear Map

A non commutative ring, denoted by $\omega_{p^2} + v_p\omega_{p^2}$, v_p an involution in $M_2(F_p)$, that is isomorphic to $M_2(F_p)$ is constructed through a unital embedding τ from F_{p^2} to $M_2(F_p)$. The elements of ω_{p^2} come from $M_2(F_p)$ such that $\tau(F_{p^2}) = \omega_{p^2}$.

The structure theorems used the transformation of the non commutative ring $\omega_{p^2} + v_p\omega_{p^2}$ to $\omega_{p^2} + u_p\omega_{p^2}$ by introducing a matrix $i_P \in M_2(F_p)$ such that $u_p = i_p + v_p$, where u_p^2 is a zero matrix.

The unital embedding τ come from a characterization of F_p in terms of an irreducible polynomial $f(x) = x^2 + x + (p - 1) \in F_p[x]$. The property of this polynomial restricts our study to case where $p \equiv 2$ or $3 \bmod 5$.

Lemma 22. *Let $p \equiv 2$ or $3 \bmod 5$ then the polynomial $f(x) = x^2+x+(p-1)$ is irreducible over F_p*

Theorem 6.3.1. *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in F_q[x]$ be a monic irreducible polynomial. Then mapping $\pi : F_q[x] \to M_n(F_q)$, $g(x) \to g(X)$ induces a unital embedding of $F_q[x]$ into $M_n(F_q)$ where*

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Corollary 17. *Let $F_{p^2} = F_p[\varpi]$ where $\varpi^2 + \varpi + (p-1) = 0$ then*

$$\tau : F_{p^2} \to M_2(F_p)$$

defined by $a + b\varpi \longmapsto \begin{pmatrix} a & b \\ b & a+(p-1)b \end{pmatrix}$ *is an embedding.*

Theorem 6.3.2. *If ϖ is a root of $f(x) = x^2 + x + (p-1)$ then*

$$\varpi^p \equiv (p-1)\varpi + (p-1) mod(\varpi^2 + \varpi + (p-1)).$$

Theorem 6.3.3. *$(p-1)\varpi + (p-1)$ is a root of f(x) since*

$$f((p-1)\varpi + (p-1))$$

$$\begin{aligned} &= ((p-1)\varpi + (p-1))^2 + (p-1)\varpi + (p-1) + (p-1) \\ &= [(p-1)^2\varpi^2 + 1] + [(p-1)\varpi + (p-1)] + (p-1) \\ &= \varpi^2 + 2\varpi + 1 - \varpi - 2 \\ &= \varpi^2 + \varpi + (p-1) \\ &= 0. \end{aligned}$$

By division algorithm, there exist $g(x)$ and r_1x+r_2 such that $x^p = g(x)f(x)+(r_1x+r_2)$ where r_1x+r_2 is the remainder when x^p is divided by $f(x)$. Since ϖ and $(p-1)\varpi+(p-1)$ are roots of $f(x)$ then we have $\varpi^p = r_1\varpi + r_2$ and

$$[(p-1)\varpi + (p-1)]p = r_1[(p-1)\varpi + (p-1)] + r_2$$

or equivalently,

$$(p-1)\varpi^p + (p-1) = r_1(p-1)\varpi + r_1(p-1) + r_2.$$

Since the characteristic of F_p is p,

$$[(p-1)\varpi + (p-1)]^p = [(p-1)\varpi]^p + (p-1)^p = [(p-1)^p\varpi^p] + (p-1)^p.$$

from fermat's Little theorem,

$$[(p-1)^p\varpi^p] + (p-1)^p = (p-1)\varpi^p + (p-1).$$

Adding $\varpi^p = r_1\varpi + r_2$ and $(p-1)\varpi^p + (p-1) = r_1[(p-1)\varpi + (p-1)] + r_2$ modulo p, then $(p-1) = r_1(p-1) + 2r_2$ or equivalently $r_1 + (p-2)r^2 = 1$. since the $gcd(1, p-2) = 1$, and $1 = (p-1)-(p-2) = (p-1)+(p-2)(p-1)$. $r_1 = p-1$ and $r_2 = p-1$. Hence $\varpi^p \equiv (p-1)\varpi+(p-1) mod(\varpi^2+\varpi+(p-1))$.

Theorem 6.3.4.

$$\tau^p(\varpi) = \begin{pmatrix} p-1 & p-1 \\ p-1 & 0 \end{pmatrix}.$$

Proof. τ is a homomorphism hence $\tau^p(\varpi) = \tau(\varpi^p)$

$$\begin{aligned} \tau^p(\varpi) &= \tau(\varpi^p) = \tau((p-1)\varpi + (p-1)) \\ &= \tau(p-1)\tau(\varpi) + \tau(p-1) \\ &= \begin{pmatrix} p-1 & 0 \\ 0 & p-1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & p-1 \end{pmatrix} + \begin{pmatrix} p-1 & 0 \\ 0 & p-1 \end{pmatrix} \\ &= \begin{pmatrix} p-1 & p-1 \\ p-1 & 0 \end{pmatrix}. \end{aligned}$$

□

Theorem 6.3.5. *Let F_p be the set of all scalar matrices in $M_2(F_p)$, $p \equiv 2$ or 3 mod 5, $\tau(F_p^2) = \omega_{p^2}$ and $v_p = \begin{pmatrix} 0 & 1 \\ 1 & p-1 \end{pmatrix}$, then $v_p\tau(\varpi) = \tau^p(\varpi)v_p$, $\omega_p[\tau(\varpi)] = \omega_{p^2}$ and $M_2(F_p) = \omega_{p^2} + v_p\omega_{p^2}$.*

Proof. Note that $\tau^2(\varpi) + \tau(\varpi) + \tau(p-1) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, hence its easy to prove that $v_p\tau(\varpi) = \tau^p(\varpi)v_p$ and $\omega_p[\tau(\varpi)] = \omega_{p^2}$.

$$\omega_{p^2} + v_p\omega_{p^2} = \{\begin{pmatrix} a+b & b+d \\ b-c-d & a-b-c \end{pmatrix} : a,b,c,d \in F_p\}$$

$$= M_2F_p.$$

□

6.4 The ideals of $M_2(F_p)(x)/(f(x))$

Let $p \equiv 2$ or $3 \pmod 5$, $i_p = \begin{pmatrix} p-1 & 0 \\ 0 & 1 \end{pmatrix}$ and $u_p = v_p + i_p$. Then $u_{p^2} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and

$$\omega_{p^2} + u_p\omega_{p^2} = \{\begin{pmatrix} a & b \\ b-c & a-b-d \end{pmatrix} : a,b,c,d \in F_p\}.$$

We have a natural homomorphic map from $\omega_{p^2} + u_p\omega_{p^2}$ to its field ω_{p^2}. For any $a \in \omega_{p^2} + u_p\omega_{p^2}$, let $\hat{a}$ denote the polynomial reduction modulo u_p. Now define a polynomial reduction mapping $\mu : \omega_{p^2} + u_p\omega_{p^2}[x] \to \omega_{p^2}[x]$ such that

$$f(x) = \sum_{i=0}^{r} a_i x^j \mapsto \sum_{i=0}^{r} \hat{a}_i x^j.$$

A monic polynomial f over $\omega_{p^2} + u_p\omega_{p^2}[x]$ is said to be basic irreducible if $\mu(f)$ is irreducible over $\omega_{p^2}[x]$.

Theorem 6.4.1. *[10] Let A_p denote $\omega_{p^2} + u_p\omega_{p^2}$, if $f(x)$ is an irreducible polynomial over ω_{p^2}, then the only right A modules of the non commutative chain ring $A[x]/(f(x))$ are $(\tau(0))$, $(\tau(1))$ and (u_p).*

Proof. Suppose I is a nonzero ideal of the ring $A[x]/(f(x))$ and $g(x) + (f(x)) \in I$ for some $g(x)$ which is not belong $(f(x))$. Since

$$gcd(\mu g(x), \mu f(x)) = \tau(1) \text{ or } \mu f(x).$$

If $gcd(\mu f(x), \mu g(x)) = 1$, then there exist $a(x)$, $b(x) \in \omega_{p^2}[x]$ such that

$$\mu a(x)\mu f(x) + \mu b(x)\mu g(x) = 1$$
$$a(x)f(x) + b(x)g(x) = 1 + us(x),$$

$s(x) \in \omega_{p^2}[x]$, multiply both sides by $(1 + us(x))$

$$a(x)f(x)(1 + us(x)) + b(x)g(x)(1 + us(x)) = \tau(1),$$
$$a(x)f(x)(1 + us(x)) + ((g(x))(b(x)(1 + us(x)))) = \tau(1)$$
$$(b(x)(1 + us(x)) + (f(x)))(g(x) + (f(x))) = \tau(1) + (f(x)).$$

Hence, $g(x) + (f(x))$ is invertible.

$$I = A[x]/(f(x)) = (\tau(1)).$$

If this never happens

$$I \subseteq (u + (f(X)))$$

to proof the other inclusion $gcd(\mu f(x), \mu g(x)) = \mu f(x)$, then there exists $a(x), b(x), s(x) \in \omega_{p^2}$ such that

$$\mu a(x)\mu f(x) + \mu g(x)\mu b(x) = \mu f(x)$$
$$a(x)f(x) + b(x)g(x) = f(x) + u_p s(x)$$
$$u_p a(x)f(x) + u_p b(x)g(x) = u_p f(x)$$
$$u_p b(x)g(x) + (f(x)) = u_p + (f(x)).$$

Hence, $u_p + (f(x)) \in I$

$$(u_p + (f(x))) \subseteq I.$$

Hence $I = (u_p + (f(x)))$. ∎

Corollary 18. *[1] If $f(x)$ is an irreducible polynomial over ω_4 , then the only right A modules of the non commutative chain ring $A[x]/(f(x))$ are (0), (1) and (u).*

6.5 The ideals of $M_2(F_p)(x)/(x^n-1)$

Theorem 6.5.1. *[40] Let $f_1(x), f_2(x), ..., f_k(x)$ be submodules of the R module M, then the following are equivalent*
(1) The canonical map

$$p : M \to \prod_{i\leq k} M/(f_i(x))$$

$$m \to (m+f_i)_{i\leq k}$$

is epimorphisms and monomorphisms

(2)for every $i \leq n$ we have $f_j + \cap_{i\neq j} f_i = M$ and $\cap_{i\leq n} f_i = 0$.

Proof. Let p be epimorphisms and $m \in M$. For $j \leq n$ we form the element $(..., 0, m+f_j, 0, ...) \in \prod_{i\leq n} M/(f_i(X))$ and choose a pre image $m_0 \in M$ under p. Then $m_0 - m_2 \in f_i$ and $m_0 \in \cap_{i\neq j} f_i$ i.e. $m \in f_j + \cap_{i\neq j} f_i$.

Now consider $(m+f_i)_{i\leq n} \in \prod_{i\leq n} M/(f_i(X))$. By (2), we can find $k_j \in F_j$ and $\tilde{k_j} \in \cap_{i\neq j} f_i$ with $m_j = k_j + \tilde{k_j}$ For the element $m = \tilde{k_1} + \tilde{k_2} + ... + \tilde{k_n} \in M$, we get

$$(m)p\pi_j = m + f_j = \tilde{k_i} + f_j = m_j + f_j \quad forall j \leq n.$$

Since kernel p $=\cap_{i\leq n} f_i$, the map is monic if and only if $\cap_{i\leq n} f_i = 0$.

□

Corollary 19. *[1] Let $x^n - 1 = f_1(X)f_2(X)...f_k(X)$ where $f_i(x)$ are irreducible polynomials over ω_4, as right modules we have the expansion*

$$A[x]/(x^n-1) = A[x]/f_1(X) \oplus A[x]/f_2(X) \oplus ... \oplus A[x]/f_k(X)$$

Theorem 6.5.2. *[10] Let $x^n - 1 = f_1 f_2 \dots f_k$, be a product of irreducible polynomials over ω_{p^2}. Then any ideal in the ring $A[x]/(x^n-1)$ is a sum of ideals of the form $(u\hat{f_i})$, and $(\hat{f_j})$*

Proof. The factorization of x^n-1 exists and is unique over ω_{p^2} . By corollary 19

$$A[x]/(x^n-1) = A[x]/(f_1) \oplus A[x]/(f_2) \oplus A[x]/(f_3) \oplus \cdots \oplus A[x]/(f_k).$$

If I is an ideal of $A[x]/(x^n-1)$, then

$$I \simeq I_1 \oplus I_2 \oplus \cdots \oplus I_k,$$

where I_i is an ideal of the ring $A[x]/(f_i)$, for $i = 1, 2, \cdots, k$. By theorem (6.4.1),

$$I_i = \tau(0), \quad (u_p + (f_i)) \quad , or \quad (\tau(1) + (f_i))$$

Since $I_i = (\tau(1) + (f_i))$ or $I_i = (u_p + (f_i))$, corresponds to the ideals $(\hat{f}_i + (x^n-1))$ or $(u_p\hat{f}_i + (x^n-1))$ respectively in the ring $A[x]/(x^n-1)$.
Consequently I is a sum of ideals of the form $(u_p\hat{f}_i)$, and $(\hat{f}_j)$. □

Theorem 6.5.3. *[10] Suppose C is a cyclic code of length n over $A_p = \omega_{p^2} + u_p\omega_{p^2}$ where n dose not divides p. Then there are monic polynomials F_0, F_1, F_2 such that $C = (\hat{F}_1, u_p\hat{F}_2)$ where $F_0F_1F_2 = x^n - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and $|C| = p^{4degF_1+2degF_2}$*

Proof. We know that $x^n - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has a unique factorization such that

$$x^n - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = f_1f_2\cdots f_r,$$

where thef_i are irreducible, We also know, by the previous theorem, that C is a sum of $(\hat{f}_i)$ and $(u_p\hat{f}_j)$. By permuting the subscripts of f_i, we can suppose that C is a sum of

$$(\hat{f}_{k+1}), (\hat{f}_{k+2}), \cdots, (\hat{f}_{k+l}), (u_p\hat{f}_{k+l+1}), (u_p\hat{f}_{k+l+2}), \cdots, (u_p\hat{f}_r),$$

Then

$$C = (f_1f_2\cdots f_kf_{k+l+1}f_{k+l+2}\cdots f_r, u_pf_1f_2\cdots f_kf_{k+1}\cdots f_{k+l}) = (F_0F_2, u_pF_0F_1),$$

where $F_0 = f_1f_2\cdots fk$, $F_1 = f_{k+1}f_{k+2}\cdots f_{k+l}$ or 1 if $l = 0$

and
$F_2 = f_{k+l+1} f_{k+l+2} \cdots f_r$ or 1 $\quad if \quad k+l=r.$

To calculate the order of C, note that

$$C = (\hat{F_1}) \oplus (u_p \hat{F_2}).$$

Hence,

$$|C| = (p^2)^{2(n-deg\hat{F_1})} (p^2)^{2(n-deg\hat{F_2})} = p^{4degF_1+2degF_2}.$$

□

Corollary 20. *[1] Suppose C is a A cyclic code of odd length n over $M_2[F_2]$. Then there exist f, g and h such that $x^n - 1 = fgh$, 3 pairwise coprime factors over ω_4 such that*

$$C = (fh) \oplus u(fg).$$

and $|C| = 4^{(2degF_1+degF_2)}$

Proof. Follow directly from the previous theorem (choose p=2) □

Bibliography

[1] Alamadhi,A., Sboui,H., Sole,P., and Yemn,O., "*Cyclic Codes Over $M_2(F_2)$*", arXiv:1201.6533v1, 2012.

[2] Atiyah,M. F. and Macdonald,I. G. "*Introduction to Commutative Algebra*". Reading, MA: Addison-Wesley, 1969.

[3] Al-Ashker,M., and Chen,J., "*Cyclic codes of arbitrary codes over $F_q + uF_q + u^2F_q + ... + u^{k-1}F_q$*", Palestine journal of mathmatics, Vol. 2(1), 72-80, 2013.

[4] Blake,I., "*Codes over certain ring*", Department of electrical engineering, University of wateloo, Canada, 1972.

[5] Blake,I., F., "*Codes over integer residue ring*", Inform. Contor.29, 295-300, 1975.

[6] Blackford,T, "*Cyclic codes over Z_4 of oddly even length*", Discreat Applide mathmatics, 128, 27-46, 2003.

[7] Cohn,P.M., "*Basic algebra groups rings and fields*", Springer-Verlag London Berlin Heidelberg, 2003.

[8] Calderbank,A. R. and Sloane, N. J. A., "*Modular and p-adic cyclic codes, Designs Codes Cryptogr*", 6, 2135, 1995.

[9] Cohn,P.M., "*Algebra*", Vol. 1, second edition, Wiley, Chichester, 1985.

[10] Dixie,F., Falcunit,Jr., and Virgilio,P., "*SisonCyclic codes over the matrix ring $M_2(F_p)$ and their Isometric images Over $F_{p^2} + UF_{p^2}$*", ETH-Zrich, 2014.

[11] Daniel,A., Emanuele,B., and Emmanuela,O., *" An Introduction to Linear and Cyclic Codes"*, Grbner Bases, Coding, and Cryptography, 2009.

[12] Dinh,H.,Q., Lpez-permouth,S.,R., "*Cyclic and negacyclic codes over finite chain ring*", IEEE Transactions on Information theory , 50(8), 2004.

[13] Eric,J., "*Associative algebra*", 2014.

[14] Gallian,J.,A., "*Contemporary Abstract Algebra*", 7^{th} ed. Brooks/Cole, Belmont, 2009.

[15] Hungerford,T., "Algebra". New York:springer-Verlag, 1974.

[16] Hansraj,G., "*Euler totient functionand its invers*", Indianj. pure appl. Math., 12(1):22-30, January 1981.

[17] lambek,j., Duman,O., "*Lectures on rings and modules*", Ginn and Blaisdell, New York, 1966.

[18] Joseph,J.R., "*An introduction to homological algebra*", 2^{nd} ed. , Springer Science Business Media, 2009.

[19] John,A., "*Introductory Lectures on Rings and Modules*". Cambridge University Press. p. 156. ISBN 978-0-521-64407-5, 1999.

[20] Lidl,R., and Niederreiter,H., "*Introduction to finite fields and their applications*", Addison Wesley, Reading, MA, 1983.

[21] Lang,S., "*Algebra*", Addison Wesley, Reading, Ma, 1971.

[22] Lam,T., "*A first course in noncommutative rings*". Graduate Texts in Mathematics 131 (2^{nd} ed.). Springer. ISBN 0-387-95183-0, 2001.

[23] Lopez-permouth,S.r., Kanwar, P., "*Cyclic codes over the integrs modulo p^m*", Finite Fields Appl. 334-352, 1997.

[24] Greferath,M., "*Cyclic codes over finite rings*", Discrete Math. 177, 273-277, 1997.

[25] Mines,R., Richman,F., and Ruitenburg,W., "*A course in constructive algebra*", Springer Verlag, p234, 1988.

[26] McDoonald,B.,R., "*Finite rings with identity*", Pure and Applide mathmatics. New York: Marcel Dekker, vol.28, 1974.

[27] Macwilliams,J., *"The structure and properties of binary cyclic alphabets"*, Byll syst. Teach. j .44, 303-332, 1965.

[28] Norton,G. H., Salagean,A., *" On the Hamming distance of linear codes over a finite chain ring"*, IEEE Trans. Inf. Theory, Vol. 46(3), 1060-1067, 2000.

[29] Pless,V., *"Introduction to the theory of error correcting codes"*, canada, 1998.

[30] Pless,V. and Qian,Z., *"Cyclic codes and quadratic codes over Z_4"*, IEEE Trans. Inform. Theory 42, 1594-1600, 1996.

[31] Pless,V., and Huffman,w.c., "*Fundumentals of error correcting codes*", Cambridge, U.K.CambridgeUniv. Press, 2003.

[32] Qian,J., Zhang,L., and Zhu,S., "*Cyclic codes over $F_p + uF_p + ... + u^k F_p$*", IEICE Trans. Fundamentals, vol E88-A, No.3, pp779-795, 2005.

[33] R.Wisbauer, "*Foundations of Module and Ring Theory*", Gordon and Breach, Reading , 1991.

[34] Roger Hammons, A., Kumar, A. R., Calderbank, N. J. A., Sloane,N., and P. Sole, "*The Z_4 linearity of Kerdock, Preparata, Goethals, and related codes*", IEEE Trans. Inform. Theory 40, 301-319, 1994.

[35] San,l., Chaoping, x., "*Coding Theory A first Course*", Cambridge University press, 2004.

[36] Spiegel,E., "*Codes over Z_m*", University of Connecticut, Informtion and control 35, 48-51, 1977.

[37] Sabouh,S., "*A family Of Cyclic Codes Over Finite Chain Rings*",(Master thesis). Islamic University Gaza, Palistine, 2008.

[38] Vijay,k., "*Acourse in abstract Algebra*", University of Dulhi, 2^{nd} Revised Editon, 1998.

[39] Wan,Z., "*Quaternary codes*", World scientific Publishing, 1997.

[40] Wisbauer,R., "*Foundations of module and ring theory*", Gordon and Breach, 1991.