Chapter 1

Introduction and Review of Literature

Coding theory is the study of sending information from one place to another correctly. In this process we first encode a message in a digital sequence of symbols and in the next step it is transmitted through a channel. In the third and last step we decode the received signals (digital sequence) into message. Sometimes it is observed that the channel may be noisy because of lightening, folds in a magnetic tape, meteor showers, competing telephone messages or many other things and therefore, the information received may be erroneous. Coding theory deals with the problems of detecting and correcting transmission errors. Basically, the subject of error correcting codes came into existence in response to a practical problem in the reliable communication of digitally encoded information and was developed as a branch of Information theory, a discipline in electrical engineering in the late forties. The ignition that initiated the subject was the paper ‘A Mathematical Theory of Communication’, by Shannon [96] in 1948. Since then algebraic coding theory has developed many connections with algebra and combinatorics and has become an interesting and fascinating topic for the mathematicians. Mathematical techniques from Linear Algebra, Number theory, Group theory, Group rings proved themselves to be very efficient tools that helped the mathematician in the construction of very useful varieties of codes. Hamming [50] was the first coding theorist whose work attracted widespread interest. Interestingly Hamming and Shannon both were connected with the fundamental problem of communication over noisy channels but there was a clear cut difference between the combinatorial constructive viewpoint of Hamming and the statistical existential viewpoint of Shannon. Most of coding theory papers of early 1950 laid the basis for various codes i.e. Linear codes, Group codes, Polynomial codes and Cyclic codes.

When using a code, it is important to know the probability of correct decoding. To be able to compute this in a practical situation, it is necessary to know the minimum distance and weight distribution of the code.

The minimum distance is an important parameter for a code as error detection and correction depends on it. Bassalygo [5], Brouwer and Verhoeff [24], Campopiano [32], Cavior [33], Chen [34], Cohen [36], Ecker [42], Hartmann [54], Johnson [58],
Joshi [59], Kasami [61, 64] and MacDonald [77] obtained minimum distances and bounds on distances of some codes.

The weight distribution is an important aspect of a code. Thus there has been a great deal of efforts to determine the weight distributions of specified codes, which is every difficult task for any but modest sized codes. The authors Baumert et.al [9], Berlekamp et.al [13, 14], Bhargva and Ngugen [17] and Calabi [27] discussed the weight distribution of various codes. Worth mentioning here are Muller [81] and Reed [91] who not only constructed important classes of codes but invented the decoding procedure also. They very firmly indicated also that how finite mathematical structures are the basic need of the coding problems. Elias [43, 44] introduced a remarkable construction of block codes. The construction of error correcting codes was the advent of Reed Solomon (RS) codes [60] and the Bose-Chaudhuri-Hocquenghem (BCH) codes [22, 23]. Prengie [85, 86] seems to have first to study cyclic codes. It is well known that code discovered by Golay [47] is most useful nowadays and, are studied as binary BCH codes. The growth of coding theory has been global during the preceding two and half decades and an account of the development can be had from the various articles. The survey articles by Berlekamp [10] and Sloane [103] are worth mentioning. The papers by Berlekamp [11, 12], Blake [18], Cowell [38], Delsarte [40], Lee and Cheng [68], MacWilliams [78], Racsmany [88], Roos [94], Shannon [97, 98] and Ward [108, 109] deal with some more practical aspects in coding theory.

The books by Apostol [1], Blake and Mullin [20], Burton [26], Curtis [39], Griffin [46], Hall [49], Hardy [52], Huffman [56], Lidl [71], van Lint [73], MacWilliams and Sloane [79], Mann [80], Peterson [82], Pless [83], Storer [105] and Vermani [107] are good references.

Objective of the thesis is to study “Minimal Cyclic Codes” since they admit a fast decoding algorithm. The cyclic codes are important class of codes which contains many families of codes including Golay codes, the binary Hamming codes and codes equivalent to Reed-Muller codes that are either cyclic or extended cyclic codes. The study of cyclic codes began with Prengie [85, 86] and the book by Peterson [82] that
Chapter 1

Introduction and Review of Literature

compiled extensive results about cyclic codes. It then laid the framework for much of
the present day theory.

Here, we discuss the cyclic codes of length $n$ over the finite fields and rings.
Let $F_l$ be the finite field of order $l$ and $C$ be the cyclic code of length $n$. Then there is
one-one and onto correspondence between a codeword $c = c_0 c_1 \ldots c_{n-1} \in C$ over $F_l$
and the polynomials $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ in $F_l[x]$ of at most degree
$n - 1$. This fact allows us that the $c$ and $c(x)$ are interchangeable. Notice that if $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ then $xc(x) = c_{n-1} x^n + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1}$ represents the codeword $c$ cyclically shifted one to the right if $x^n$ was set
equal to 1. Equivalently, the cyclic code $C$ is invariant under a cyclic shift
modulo $x^n - 1$. This fact allows us for studying cyclic codes in the residue class ring
$R_n = \frac{F_l[x]}{<x^n-1>}$. It is well known that a minimal cyclic code of a given length $n$ over $F_l$ is
an minimal ideal in semisimple ring $R_n$ [83] and every ideal (cyclic code) in $R_n$ is the
direct sum of its minimal ideals. Therefore, the study of minimal cyclic code over the
finite field $F_l$ is equivalent to the study of the minimal ideals in $R_n$.

It is observed that the study of minimal ideals in $R_n$ completely depends on
irreducible factors of $x^n - 1$ over $F_l$. But factorization of polynomials is not an easy
task. To overcome the problem of factorization, a minimal ideal can also be obtained
by a polynomial known as \textbf{primitive idempotent}. Therefore, to describe the complete
set of ideals (codes over $F_l$) in $R_n$, it is sufficient to find its complete set of primitive
idempotents.

Throughout this thesis we are under the assumption that the characteristic of the
field $F_l$ does not divide the length of the cyclic codes. This assumption also implies that
$R_n$ is semisimple and thus the Wedderburn structure theorem is applicable. Apart from
minimal cyclic codes over finite field $F_l$, we have also discussed Quadratic Residue
Codes (QR-Codes) of prime power length over ring of integers modulo 4. As minimal
cyclic codes can be viewed as an ideal in the group algebra of a cyclic group over a
finite field, therefore, a natural case of more general arises. An Abelian code over a
finite field is an ideal of the group algebra $F_lG$, $G$ is an abelian group. In view of above
discussion abelian codes are the generalized cyclic codes. Camion [31] has shown that

\textbf{Minimal Cyclic and Abelian Codes}
there exist some abelian codes that are not obtainable as direct product of cyclic codes. In case \(\gcd(l, k) = 1\), then the group algebra \(F_lG\) is semisimple and hence can be written as direct sum of minimal ideals.

**Some results and definitions**

**1.1 The Group Algebra**

**Definition 1.1.1.** Let \(G\) be a multiplicative group and \(F\) be a field. Let \(FG\) denotes the set of all formal sums

\[
\alpha = \sum_{g \in G, \alpha(g) \in F} \alpha(g)g,
\]

where \(\{g \in G| \alpha(g) \neq 0\}\) is a finite set.

Then \(FG\) is a ring (associative) with respect to addition and multiplication defined as follows:

\[
\sum_{g \in G} \alpha(g)g + \sum_{g \in G} \beta(g)g = \sum_{g \in G} (\alpha(g) + \beta(g))g
\]

and

\[
\left(\sum_{g \in G} \alpha(g)g\right)\left(\sum_{h \in G} \beta(h)h\right) = \sum_{g, h \in G} \alpha(g)\beta(h)gh
\]

\[
= \sum_{z \in G} \gamma(z)z,
\]

where

\[
\gamma(z) = \sum_{gh = z} \alpha(g)\beta(h)
\]

and the sum is taken over all pairs \((g, h) \in G \times G\) such that \(gh = z\). This ring is called the group ring of the group \(G\) over the field \(F\).

With the scalar multiplication defined as:

\[
\delta \left(\sum_{g \in G} \alpha(g)g\right) = \sum_{g \in G} (\delta \alpha(g))g
\]
\[
\sum_{g \in G} \alpha(g)(\delta g) \text{ for all } \delta \in F,
\]

\(FG\) becomes \(F\) – algebra with basis \(\{g \mid g \in G\}\).

Note that the field \(F\) may be finite or infinite. In this thesis we have used finite field.

**Definition 1.1.2.** The ring epimorphism \(w : FG \to F\) defined by

\[
w \left( \sum_{g \in G} \alpha(g)g \right) = \sum_{g \in G} \alpha(g)
\]

is called augmentation mapping.

**Remark 1.1.3.** Let \(G = \langle g \rangle = C_n\) be a cyclic group of finite order \(n\) and \(F\) be a field. Let \(F[x]\) be the ring of polynomials in indeterminate \(x\). Then the natural homomorphism

\[
F[x] \to FG
\]

defined by \(x \to g\) is an epimorphism with kernel \(<x^n - 1>\) the ideal generated by \(x^n - 1\) in \(F[x]\). Hence \(FC_n \cong \frac{F[x]}{<x^n - 1>}\).

1.2 **Semisimple Group Algebra**

**Definition 1.2.1.** The Jacobson Radical of a ring \(R\) is defined to be the intersection of all maximal ideals of \(R\). We denote it by \(J(R)\).

**Definition 1.2.2.** A ring \(R\) is called semisimple if \(J(R) = 0\).

**Maschke Theorem 1.2.3.** [20] If \(F\) is a field, then \(FG\) is a semisimple ring if and only if \(G\) is finite and the characteristic of \(F\) does not divides the order of the group \(G\).

**Definition 1.2.4.** An element \(e\) of \(R\) is called an idempotent if \(e^2 = e\).

**Definition 1.2.5.** An element \(e\) of \(R\) is called a primitive idempotent if it cannot be written as sum of two orthogonal (nonzero) idempotents.
Chapter 1

Introduction and Review of Literature

Definition 1.2.6. A ring $R$ is called Artinian if every decreasing sequence of left ideals of $R$ is finite.

Theorem 1.2.7. [92] If $R$ is semisimple Artinian ring and $M \neq 0$ is an ideal of $R$, then $M = eR$ for some idempotent $e$ of $R$ (the idempotent $e$ is called generating idempotent of $M$).

Wedderburn Theorem 1.2.8. [20] A semisimple Artinian ring is direct sum of finite number of simple Artinian rings.

1.3 Some results of Number Theory

Definition 1.3.1. (Euler’s $\varphi$ function). For each positive integer $m$, the number of integers in the set $\{1, 2, \ldots, m\}$ which are relatively prime to $m$, denoted by $\varphi(m)$, is called Euler’s $\varphi$ function. $\varphi(m)$ is always even integer for all $m > 2$.

If $p$ is a prime number then for every integer $r \geq 1$,

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p - 1).$$

It is clear that $\varphi$ value for an odd prime is always even. In fact $\varphi(m)$ is always even integer for all $m > 2$.

If $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, $p_i$ are distinct primes and $\alpha_i \geq 0$, then

$$\varphi(m) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r})$$

$$= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_r^{\alpha_r})$$

$$= p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\ldots p_r^{\alpha_r-1}(p_r-1).$$

Theorem 1.3.2. (Euler’s). If $a$ and $m$ are positive integers with $\gcd(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$ 

Definition 1.3.3. If $\gcd(a, m) = 1$, the least positive integer $r$ such that $a^r \equiv 1 \pmod{m}$, is called the order of $a$ modulo $m$.

By Theorem 1.3.2, $1 \leq r \leq \varphi(m)$. If $r = \varphi(m)$, then $a$ is called Primitive Root modulo $m$. Further, if $a$ is a primitive root mod $p^n$, then
\[
\alpha^{\varphi(p^n)/2} \equiv -1 \pmod{p^n}.
\]

**Definition 1.3.4.** A set of integers \(\{a_1, a_2, a_3, \ldots, a_{\varphi(m)}\}\) such that for \(i \neq j\), \(a_i \not\equiv a_j \pmod{m}\) and \(\gcd(a_i, m) = 1\), is called reduce residue system modulo \(m\).

If \(a\) is primitive root modulo \(m\), then the set

\[
\{1, a, a^2, \ldots, a^{\varphi(m)-1}\}
\]

is a reduced residue system modulo \(m\).

**Definition 1.3.5.** Let \(p\) be an odd prime. The numbers \(1^2, 2^2, \ldots, (p-1)^2\) reduced modulo \(p\) are called **Quadratic Residues** mod \(p\). In general, if \(m > 1\) is an integer and \(a\) is any integer with \(\gcd(a, m) = 1\), then \(a\) is called quadratic residue modulo \(m\) if the congruence \(x^2 \equiv a \pmod{m}\) has a solution. Otherwise \(a\) is called quadratic non residues mod \(m\).

**Theorem 1.3.6.** [76] An integer \(m > 1\) have a primitive root if and only if \(m\) is one of the \(2, 4, p^t, 2p^t\), where \(p\) is an odd prime and \(t \geq 1\) is an arbitrary positive integer.

**Theorem 1.3.7.** [83]

(a) Let \(p\) be an odd prime. Then \(-1\) is quadratic residue modulo \(p\) iff \(p \equiv 1 \pmod{4}\).

(b) Product of two quadratic residues or quadratic non residues is a quadratic residue but the product of a quadratic residue and a quadratic non residue is a quadratic non residue.

### 1.4 Codes over Finite Fields

**Definition 1.4.1.** A polynomial \(m(x)\) is said to be a minimal polynomial of an element \(\alpha\) in \(F_{p^r}\), if \(m(x)\) is monic polynomial of smallest degree with coefficients in \(F_p\) that has \(\alpha\) as a root. It is unique always.

**Theorem 1.4.2.** [83] Let \(m(x)\) be the minimal polynomial of an element \(\alpha\) in \(F_{p^r}\). Then
Chapter 1: Introduction and Review of Literature

(i) \( m(x) \) is irreducible.

(ii) If \( \alpha \) is a root of a polynomial \( f(x) \) with coefficients in \( F_p \), then \( m(x) \) divides \( f(x) \).

(iii) \( m(x) \) divides \( x^{p^r} - x \).

(iv) if \( m(x) \) is primitive, then its degree is \( r \). In any case the degree of \( m(x) \) is less than or equal to \( r \).

Definition 1.4.3. Consider the set \( \{0, 1, 2, \ldots, n-1\} \). Let \( l \) be the number such that \( \gcd(l, n) = 1 \). The cyclotomic coset containing the integer \( s \) is \( \{s, sl, sl^2, \ldots, sl^{t-1}\} \), where \( t \) is the smallest integer such that \( sl^t \equiv s \pmod{n} \). We denote it by \( C_s \).

Theorem 1.4.4. [83] \( GF(p^s) = F_{p^s} \subseteq F_{p^r} = GF(p^r) \) if and only if \( s \) divides \( r \) and an element \( \alpha \) in \( F_{p^r} \) is in \( F_{p^s} \) if and only if \( \alpha^{p^s} = \alpha \).

Assume that \( n \) is an integer and \( \gcd(n, p) = 1 \). Let \( m \) be the smallest integer such that \( p^m \equiv 1 \pmod{n} \), then \( F_{p^m} \) is the smallest field containing all the \( n^{th} \) root of unity. We now have following results:

Theorem 1.4.5. [83] Let \( \alpha \) be a root of \( x^n = 1 \) in the smallest field \( F_{p^m} \) of characteristic \( p \) containing all the \( n^{th} \) root of unity and let \( m(x) \) be its minimal polynomial. Let \( \beta \) be a primitive \( n^{th} \) root of unity in \( F \) and let \( \alpha = \beta^s \). If \( C_s \) is the cyclotomic coset mod \( n \) containing \( s \), then

\[
    m(x) = \prod_{i \in C_s} (x - \beta^i).
\]

Inversion Formula 1.4.6. [79] Let \( \alpha \) be a primitive \( n^{th} \) root of unity in the smallest field of characteristic \( p \). Then the vector \( c = (c_0, c_1, \ldots, c_{n-1}) \) can be derived from

\[
    c(x) = (c_0 + c_1x + \cdots + c_{n-1}x^{n-1})
\]

by
Chapter 1

Introduction and Review of Literature

We now assume \( q \) is a prime or some prime power. Let \( V(n,q) \) denotes the vector space of all \( n \)-tuples \((\alpha_1, \alpha_2, \ldots, \alpha_n)\) over \( F_q \).

**Definition 1.4.7.** An \((m,n)\) block code \((m < n)\) over \( F_q \) consists of an encoding function \( E : V(m,q) \to V(n,q) \) and a decoding function \( D : V(n,q) \to V(m,q) \).

**Definition 1.4.8.** If \( \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \) is in \( V(n,q) \), then the weight of \( \alpha \) denoted by \( wt(\alpha) \), is the number of positions \( i \) with \( \alpha_i \neq 0 \).

**Definition 1.4.9.** If \( \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \) and \( \beta = (\beta_1, \beta_2, \ldots, \beta_n) \) are two codewords then the distance between \( \alpha \) and \( \beta \) written as \( d(\alpha, \beta) \) is equal to the number of positions \( i \) such that \( \alpha_i \neq \beta_i \).

**Definition 1.4.10.** Any subspace \( C \) of \( V(n,q) \) is called a linear code over \( F_q \) of length \( n \). Thus if \( C \) is a linear code and \( \alpha, \beta \in C \), then 
\[
d(\alpha, \beta) = wt(\alpha - \beta).
\]

**Definition 1.4.11.** The minimum distance of a linear code \( C \) denoted by \( d(C) \) is defined as \( d(C) = \min \{d(\alpha, \beta) | \alpha, \beta \in C, \alpha \neq \beta\} \).

In view of Definition 1.4.10, \( d(C) = \min \{wt(\alpha) | \alpha \in C, \alpha \neq 0\} \).

**Definition 1.4.12.** A linear code of length \( n \), dimension \( k \) and minimum distance \( d \) is called an \([n,k,d]\) code.

The parameter \( k \); in the description of an \([n,k,d]\) code is important, because \( k/n \), the rate of the code depends on it. The parameter \( d \) is also important because the error correcting and detecting capabilities of a code depends on it.

**Theorem 1.4.13.** A code with minimum distance \( d \) can correct \( [(d - 1) / 2] \) errors (where \([x]\) denotes the greatest integer less than or equal to \( x \)). If \( d \) is even, then the code can detect \( d/2 \) errors and can correct \( [(d - 1) / 2] \) errors.

**Definition 1.4.14.** A code \( C \) of length \( n \) is called a Cyclic Code if
(i) If \(C\) is a linear code

(ii) Whenever \((\alpha_0, \alpha_1, \ldots, \alpha_{n-1})\) is in \(C\), then \((\alpha_{n-1}, \alpha_0, \alpha_1, \ldots, \alpha_{n-2})\) is also in \(C\).

**Theorem 1.4.15.** [20] The unique monic polynomial \(g(x)\) of minimal degree in any ideal \(A\) of \(\frac{F_q[x]}{<x^n-1>}\) is a generator of \(A\) and divides \(x^n - 1\). The dimension of \(A\) is \(n - \text{degree } g(x)\). Conversely, a divisor of \(x^n - 1\) is a generator of an ideal in \(\frac{F_q[x]}{<x^n-1>}\).

Such a polynomial defined in Theorem 1.4.15 is called the generating polynomial of the cyclic code \(C\).

**Theorem 1.4.16.** [83]

If \(e(x)\) is the idempotent generator of cyclic code \(C\), then the generating polynomial \(g(x)\) of \(C\) equals \(\text{gcd}(e(x), (x^n - 1))\).

**Theorem 1.4.17.** [83] If \(x^n - 1 = (x - 1)f_1(x)f_2(x) \cdots f_k(x)\) is a factorization of \(x^n - 1\) into irreducible factors and \(\overline{f_i(x)}\) denotes the product of all factors except \(f_i(x)\) then there are \(k + 1\) minimal ideals \(C_1, C_2, \ldots, C_{k+1}\) with generating polynomial \(\overline{f_1(x)}, \overline{f_2(x)}, \ldots, \overline{f_k(x)}\) and \(\overline{(x - 1)}\). Let \(e_1, e_2, \ldots, e_{k+1}\) be the generating idempotents of \(C_1, C_2, \ldots, C_{k+1}\) then \(e_i(x)\) satisfies the following conditions.

(i) \(e_i(x) e_j(x) = 0\) if \(i \neq j\)

(ii) \(1 = \sum_{i=1}^{k+1} e_i(x)\).

Furthermore, a cyclic code \(C\) is a sum of minimal ideals \(C_i\). Then \(e(x)\), the generating idempotent of \(C\) is the sum of the primitive idempotents \(e_i(x)\), where \(e_i(x)\) is the generating idempotent of \(C_i\).

**Remark 1.4.18.** In view of Theorem 1.4.5 and 1.4.20, it is obvious that the number of primitive idempotents in \(R_n\) is equal to the number of cyclotomic cosets modulo \(n\).
Chapter 1

Introduction and Review of Literature

**Theorem 1.4.19.** [79] A polynomial \( E(x) \in R_n \) is an idempotent if and only if \( E(\alpha^i) = 0 \) or 1 for \( i = 0, 1, \ldots, n - 1 \), where \( \alpha \) is primitive \( n \)th root of unity in some extension field of \( F_q \).

**Definition 1.4.20.** [4] For an integer \( s \), \( \theta_s(x) \) the primitive idempotent in \( R_n = \frac{F_q[x]}{<x^n-1>} \) corresponding to the cyclotomic coset \( C_s \) containing \( s \) modulo \( n \), is \( \theta_s(x) = \sum_{i=0}^{n-1} \varepsilon_i x^i \) where \( \varepsilon_i = \frac{1}{n} \sum_{j \in C_s} \alpha^{-ij} \), where \( \alpha \) is primitive \( n \)th root of unity.

**Definition 1.4.21.** The permutation \( \mu_g \) of the coordinate positions \( \{0, 1, \ldots, m - 1\} \) defined by \( \mu_g(i) \equiv ig(mod m) \) with \( \gcd(g, m) = 1 \) is called a multiplier. Since cyclic codes of length \( m \) are ideals in \( R_m \), for \( g > 0 \), we regard \( \mu_g \) acting on \( R_m \) by

\[
\mu_g(f(x)) \equiv f(x^g)(mod(x^m - 1)).
\]

**Theorem 1.4.22.** [83] Let \( C \) be a code of length \( m \) over \( F_1 \), with the generating idempotent \( e(x) \). Let \( g \) be an integer with \( \gcd(g, m) = 1 \). Then, \( \mu_g(e(x)) \) is the generating idempotent of the cyclic code \( \mu_g(C) \).

**Theorem 1.4.23.** Let \( C_1 \) and \( C_2 \) be a cyclic codes of length \( m \) over \( F_1 \). Then \( C_1 \) and \( C_2 \) are permutation equivalent if there exists a multiplier that maps \( C_1 \) to \( C_2 \) i.e. if there exists a multiplier that maps the generating idempotent of \( C_1 \) to the generating idempotent of \( C_2 \).

**Notation 1.4.24.** Throughout this thesis

(i) The length \( n \) of the code \( C \) is co prime to the char. \( F_1 \) i.e. \( \gcd(n, \text{char. } F_1) = 1 \).

(ii) \( R_n = \frac{F_q[x]}{<x^n-1>} \), the ring of congruence classes of polynomials in \( F_q[x] \) modulo \( (x^n - 1) \) and we think these classes as polynomials of degree less than \( n \).

1.5 Plan of Thesis

The Thesis consists of six chapters. The chapter-wise brief description of the Thesis is as follows:
Chapter 1, is an introduction to the concepts, contains various definitions and well known results on Coding theory, Number theory, Linear algebra and Group algebra which are used frequently in the thesis.

In Chapter 2, we describe minimal cyclic codes of length $2p^n$, where $l$ is $d^{th}$ residues modulo $2p^n$. We obtain explicit expressions for all the $2(nd + 1)$ primitive idempotents in $R_k$, when $k = 2p^n$, where $p, l$ are distinct odd primes, $o(l)_{2p^n} = \frac{\varphi(2p^n)}{d}, d$ is a positive integer. The minimum distance, generating polynomial and dimension of the minimal cyclic codes generated by these primitive idempotents are also discussed. In Section 2.2, we obtain the cyclotomic cosets modulo $2p^n$ (Theorem 2.2.3). The explicit expressions of primitive idempotents are obtained in Section 2.3 (Theorem 2.3.1 – 2.3.2). In Section 2.4 (Theorem 2.4.1 – 2.4.4), we discuss the dimension, generating polynomial and minimum distance of minimal cyclic codes of length $2p^n$. In Section 2.5, the various parameters of minimal cyclic codes of length 22 and 26 are discussed.

In Chapter 3, the explicit expressions for all the $2n(d + 1) + 4$ primitive idempotents in $R_k$ are obtained, when $k = 2p^nq$, where $p, q, l$ are distinct odd primes, $o(l)_{2p^n} = \varphi(2p^n) = \varphi(p^n), o(l)_q = \varphi(q), \gcd(\varphi(2p^n), \varphi(q)) = d, p$ does not divide $q - 1$. In Section 3.2 (Lemmas 3.2.1 – 3.2.17 and Theorem 3.2.5), we obtain the cyclotomic cosets modulo $2p^nq$ and some basic results for describing the primitive idempotents in $R_k$. In this case the explicit expressions for all the $2n(d + 1) + 4$ primitive idempotents in $R_k$ are given by the Theorem 3.3.2 and the minimum distance, generating polynomials and dimension $n$ of the minimal cyclic codes generated by these primitive idempotents are obtained in Section 3.4. In section 3.5, we obtained the various parameters of minimal cyclic codes of length 70.

In Chapter 4, the weight distribution of minimal cyclic codes of length $2p^n$ is discussed. In Section 4.3 (Theorem 4.3.4-4.3.5) the weight distribution of $M_p^{(2p^n_m)}$, for $1 \leq j \leq m$ are investigated. In Section 4.4 (Theorem 4.4.12) the weight distribution
of $\mathbb{M}_1^{(2p^r)} (1 \leq r \leq m)$ is discussed. In Section 4.5, the weight distribution of minimal cyclic code of length 50 is obtained.

In Chapter 5, Quadratic residue codes of prime power length over $\mathbb{Z}_4$ (ring of integers modulo 4) are discussed. In Section 5.3 (Theorems 5.3.2-5.3.5) some properties of QR-codes of prime power length are obtained. In Section 5.4, the properties of quadratic residue codes of length 49 are investigated.

In Chapter 6, we obtain explicit expression of primitive idempotents of some minimal abelian codes of the group algebra $F_lG$, where $F_l$ a finite field with $l$ elements, $G = H_1 \times H_2$, $H_1$ and $H_2$ are abelian groups of order 2 and exponent $p^n$ respectively.