CHAPTER II

PRELIMINARIES

In this chapter, we collect definitions, notations, and some useful results that will be used in the later chapters. The first section deals with primitive polynomials over finite fields. Details and proofs can be found in Lidl and Niederreiter [18]. The second section deals with digit system of polynomials, first developed by Scheicher and Thuswaldner [20]. Throughout this thesis, the follwing symbols will be standard:

$\mathbb{F}_q$ a finite field with q elements where q is a prime power,

$\mathbb{N}$ the set of all natural numbers.

2.1 Primitive polynomials over $\mathbb{F}_q$

Definition 2.1.1. [18, 1.57] A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $k \geq 1$ is said to be *irreducible* over $\mathbb{F}_q$ if $f(x) = g(x)h(x)$ with $g(x),\ h(x) \in \mathbb{F}_q[x]$ implies that either $g(x)$ or $h(x)$ is a constant polynomial.

Theorem 2.1.2. [18, 2.8] *For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^*$ of non-zero elements of $\mathbb{F}_q$ is cyclic.*

Definition 2.1.3. [18, 2.9] A generator of the cyclic group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

Definition 2.1.4. [18, 3.2] Let $f(x) \in \mathbb{F}_q[x]$ be a non-zero polynomial. If $f(0) \neq 0$, then the least positive interger e for which $f(x)$ divides $x^e - 1$ is called the *order* of $f(x)$, denoted by $\mathrm{ord}(f) := \mathrm{ord}(f(x))$. If $f(0) = 0$, then $f(x) = x^h g(x)$, where $h \in \mathbb{N}$ and $g(x) \in \mathbb{F}_q[x]$ with $g(0) \neq 0$ uniquely determined; in this case $\mathrm{ord}(f)$ is then defined to be $\mathrm{ord}(g)$.

Definition 2.1.5. [18, 3.15] A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $k \geq 1$ is called a *primitive polynomial* over $\mathbb{F}_q$ if it is the minimal polynomial of a primitive element of $\mathbb{F}_{q^k}$.

Theorem 2.1.6. [18, 3.16] *A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $k \geq 1$ is a primitive polynomial over $\mathbb{F}_q$ if and only if $f(x)$ is monic, $f(0) \neq 0$ and $ord(f) = q^k - 1$.*

Definition 2.1.7. [18, p. 395] Let $k \in \mathbb{N}$, and let $a, a_0, \ldots, a_{k-1}$ be given elements of $\mathbb{F}_q$. A sequence $s_0, s_1, \ldots$ of elements of $\mathbb{F}_q$ satisfying the relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n + a \quad (n = 0, 1, \ldots) \tag{2.1.1}$$

is called a *(kth-order) linear recurring sequence* in $\mathbb{F}_q$. The terms $s_0, s_1, \ldots, s_{k-1}$ are referred to as the *initial values* and the vector $\mathbf{v}_0 := (s_0, s_1, \ldots, s_{k-1})$ is referred to as the *initial state vector*. A relation of the form (2.1.1) is called a *(kth-order) linear recurrence relation*. The sequence $s_0, s_1, \ldots$ is called a *homogeneous* linear recurring sequence in $\mathbb{F}_q$ if $a = 0$; otherwise the linear recurring sequence is said to be *inhomogeneous*.

Definition 2.1.8. [18, 8.3] Let S be an arbitrary nonempty set, and let $s_0, s_1, \ldots$ be a sequence of elements of S. If there exist integer $r > 0$ and $n_0 \geq 0$ such that

$$s_{n+r} = s_n \quad (n \geq n_0),$$

then the sequence is called *ultimately periodic* and r is called a *period* of the sequence. The smallest among all the possible periods of an ultimately periodic sequence is called the *least period* of the sequence.

Lemma 2.1.9. [18, 8.4] *Every period of an ultimately periodic sequence is divisible by the least period.*

Definition 2.1.10. [18, 8.5] An ultimately periodic sequence $s_0, s_1, \ldots$ with least period r is called *purely periodic* if $s_{n+r} = s_n$ hold for all $n = 0, 1, \ldots$. In this case, we also say that the sequence $s_0, s_1, \ldots$ is *periodic*.

Lemma 2.1.11. [18, 8.6] *The sequence $s_0, s_1, \ldots$ is periodic if and only if there exists an integer $r > 0$ such that $s_{n+r} = s_n$ for all $n = 0, 1, \ldots$.*

Definition 2.1.12. [18, p. 404] Let $s_0, s_1, \ldots$ be a kth-order homogeneous linear recurring sequence in $\mathbb{F}_q$ satisfying the linear recurrence relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n \quad (n = 0, 1, \ldots), \tag{2.1.2}$$

where $a_j \in \mathbb{F}_q$ $(0 \leq j \leq k-1)$. The polynomial

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_0 \in \mathbb{F}_q[x]$$

is called the *characteristic polynomial* of the linear recurring sequence.

Theorem 2.1.13. [18, 8.28] *Let $s_0, s_1, \ldots$ be a homogeneous linear recurring sequence in $\mathbb{F}_q$ with non-zero initial state vector, and suppose the characteristic polynomial $f(x) \in \mathbb{F}_q[x]$ is irreducible over $\mathbb{F}_q$ and satisfies $f(0) \neq 0$. Then the sequence is periodic with least period equal to ord(f).*

Theorem 2.1.14. [18, 8.29] *Let $f(x) \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$ with* $\deg(f) = k$. *Then ord(f) divides $q^k - 1$.*

Definition 2.1.15. [18, 8.32] A homogeneous linear recurring sequence in $\mathbb{F}_q$ whose characteristic polynomial is a primitive polynomial over $\mathbb{F}_q$ and which has a non-zero initial state vector is called a *maximal period sequence* in $\mathbb{F}_q$.

Definition 2.1.16. [18, p. 423] Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree. We denote the set of all homogeneous linear recurring sequences in $\mathbb{F}_q$ with characteristic polynomial $f(x)$ by $S(f(x))$. In other words, $S(f(x))$ consists of all sequences in $\mathbb{F}_q$ satisfying the homogeneous linear recurrence relation determined by $f(x)$. The set $S(f(x))$ may be considered as a vector space over $\mathbb{F}_q$ if operations for sequences are defined termwise.

Theorem 2.1.17. [18, 8.55] *Let $f_1(x), \ldots, f_h(x)$ be non-constant monic polynomials over $\mathbb{F}_q$. Then*

$$S(f_1(x)) + \cdots + S(f_h(x)) = S(c(x)),$$

where $c(x)$ is the (monic) least common multiple of $f_1(x), \ldots, f_h(x)$.

Definition 2.1.18. [18, p. 449] For $b \in \mathbb{F}_q$ we denote by $Z(b)$ the number of occurrences of b in one least period of the linear recurring sequence. If $s_0, s_1, \ldots$ is a kth-order maximal period sequence, then

$$Z(b) = \begin{cases} q^{k-1} & \text{if } b \neq 0, \\ q^{k-1} - 1 & \text{if } b = 0. \end{cases}$$

2.2 Digit systems over $\mathbb{F}_q[x]$

In 2003, Scheicher and Thuswaldner [20] devised a new kind of digit systems analogous to the well-known *canonical number systems* (cf. [1]).

Let

$$p(x, y) = y^n + b_{n-1}y^{n-1} + \cdots + b_1 y - b_0 \in \mathbb{F}_q[x, y],$$

where $b_i \in \mathbb{F}_q[x]$, $\deg b_0 > 0$. Let

$$\mathcal{R} := \mathbb{F}_q[x, y]/(p(x, y)), \quad \mathcal{N} := \{g \in \mathbb{F}_q[x] : \deg g < \deg b_0\}.$$

Clearly, each $r \in \mathcal{R} \setminus \{0\}$ is uniquely represented as

$$r = r_0 + r_1 y + \cdots + r_{n-1}y^{n-1}, \quad r_j \in \mathbb{F}_q[x].$$

We say that $r \in \mathcal{R} \setminus \{0\}$ has a finite *y-adic representation* if it admits a finite representation of the form

$$r = d_0 + d_1 y + \cdots + d_h y^h,$$

with all the $d_i \in \mathcal{N}$ and $h \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$. The polynomials d_i are called the *digits* of r and the vector $(d_0, d_1, \ldots, d_h)_y$ is called the *digit representation* of r. The pair $(p(x,y), \mathcal{N})$ is called a *digit system* in $\mathcal{R} \setminus \{0\}$ with y being the *base* and $\mathcal{N}$ being the *digit set*. If each $r \in \mathcal{R} \setminus \{0\}$ has a unique finite y-adic representation, then $p(x,y)$ is referred to as a *DS-polynomial*.

In order to determine those $p(x,y)$ which are DS-polynomials, Scheicher and Thuswaldner make use of the following algorithm. Given

$$r := r^{(0)} = r_0^{(0)} + r_1^{(0)} y + \cdots + r_{n-1}^{(0)} y^{n-1} \in \mathcal{R} \setminus \{0\},$$

there exist unique $d_0 \in \mathcal{N}$ and $\tilde{r}_0 \in \mathbb{F}_q[x]$ such that $r_0^{(0)} = \tilde{r}_0 b_0 + d_0$, $\deg \tilde{r}_0 < \deg r_0^{(0)}$. In order to mimic the case of integers, we adopt the square bracket notation by writing

$$\tilde{r}_0 := \left[r_0^{(0)} / b_0 \right].$$

Using

$$\frac{b_0}{y} = b_1 + b_2 y + \cdots + b_n y^{n-1}, \tag{2.2.1}$$

we define

$$\begin{aligned} r^{(1)} := r_0^{(1)} + r_1^{(1)} y + \cdots + r_{n-1}^{(1)} y^{n-1} &= \frac{r^{(0)} - d_0}{y} \\ &= \left(r_1^{(0)} + \tilde{r}_0 b_1 \right) + \left(r_2^{(0)} + \tilde{r}_0 b_2 \right) y + \cdots + \left(r_n^{(0)} + \tilde{r}_0 b_n \right) y^{n-1} \end{aligned} \tag{2.2.2}$$

so that

$$r_i^{(1)} = r_{i+1}^{(0)} + \tilde{r}_0 b_{i+1} \quad (0 \le i \le n-1) \quad \text{and} \quad \tilde{r}_1 = \left[\left(\tilde{r}_0 b_1 + r_1^{(0)} \right) / b_0 \right].$$

Continuing in the same manner, for $k \ge 1$, define

$$r^{(k)} := r_0^{(k)} + r_1^{(k)} y + \cdots + r_{n-1}^{(k)} y^{n-1} = \frac{r^{(k-1)} - d_{k-1}}{y} \tag{2.2.3}$$

so that, for $i = 0, 1, \ldots, n-1$, we have

$$r_i^{(k)} = r_{i+1}^{(k-1)} + \tilde{r}_{k-1} b_{i+1} \tag{2.2.4}$$

$$= \tilde{r}_{k-1} b_{i+1} + \tilde{r}_{k-2} b_{i+2} + \cdots + \tilde{r}_0 b_{i+k} + r_{i+k}^{(0)}$$

$$\tilde{r}_k = \left[\left(\tilde{r}_{k-1} b_1 + \tilde{r}_{k-2} b_2 + \cdots + \tilde{r}_0 b_k + r_k^{(0)} \right) / b_0 \right], \tag{2.2.5}$$

and we get the y-adic representation

$$r = r^{(0)} = d_0 + d_1 y + \cdots + d_{k-1} y^{k-1} + y^k r^{(k)}. \tag{2.2.6}$$

If there exists $k \in \mathbb{N}$ such that $r^{(k)} = 0$, then (2.2.6) yields a finite y-adic representation for r of length k. If $r \equiv 0$, define its length to be 0. If there are indices $j < k$ such that $r^{(j)} = r^{(k)}$, then (2.2.6) yields an ultimately *periodic* representation for r with period length $k - j$.

The main results of Scheicher and Thuswaldner state that:

Lemma 2.2.1. [20, 2.1] *Let $p(x, y) = y^n + b_{n-1} y^{n-1} + \cdots + b_1 y - b_0 \in \mathbb{F}_q[x, y]$, where $b_i \in \mathbb{F}_q[x]$, $\deg b_0 > 0$. Each $r \in \mathcal{R} = \mathbb{F}_q[x, y] / (p(x, y))$ has a unique representation*

$$r = r_0 + r_1 y + \cdots + r_{n-1} y^{n-1} := (r_0, r_1, \ldots, r_{n-1})_s$$

such that

$$r_j = \sum_{i=1}^{n} \varepsilon_i b_{i+j} \quad (j = 0, 1, \ldots, n-1)$$

with $r_j, \varepsilon_i \in \mathbb{F}_q[x]$. For such sums, $r := (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)_\varepsilon$ is called the ε-representation of r. The map $(r_0, r_1, \ldots, r_{n-1})_s \longrightarrow (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)_\varepsilon$ is a bijection.

Theorem 2.2.2. [20, 2.5] *Let $p(x, y) = y^n + b_{n-1} y^{n-1} + \cdots + b_1 y - b_0 \in \mathbb{F}_q[x, y]$, where $b_i \in \mathbb{F}_q[x]$, $\deg b_0 > 0$. Then $p(x, y)$ is a DS-polynomial if and only if*

$$\max_{i=1,\ldots,n-1} \deg b_i < \deg b_0.$$

Theorem 2.2.3. [20, 3.1] *Let* $p(x,y) = y^n + b_{n-1}y^{n-1} + \cdots + b_1 y - b_0 \in \mathbb{F}_q[x,y]$, *where* $b_i \in \mathbb{F}_q[x]$, $\deg b_0 > 0$. *Then the sequence* $\mathcal{U}_r := \left(r^{(0)}, r^{(1)}, r^{(2)}, \ldots\right)$, *with* $r := r^{(0)}$, *is ultimately periodic for all* $r \in \mathcal{R} \setminus \{0\}$ *if and only if*

$$\max_{i=1,\ldots,n-1} \deg b_i \leq \deg b_0.$$

Note that the ultimately periodic case properly contains the finite case.