PERIODS OF LINEARLY RECURRING SEQUENCES

A Thesis
Submitted to the Faculty
of
Washington and Lee University

By

Danjoseph Quijada

In Partial Fulfillment of the Requirements
for the Degree of
BACHELOR OF SCIENCE
WITH HONORS

Major Department: Mathematics

Thesis Advisor: Dr. Michael Bush

Second Reader: Dr. Carrie Finch

May 2015

ABSTRACT

In this thesis, we investigate sequences defined by linear recurrence relations. These are sequences whose subsequent terms are generated using some linear combination of the previous terms. We call the equation that determines the next terms of the sequence the "linear recurrence relation" satisfied by the sequence.

As it turns out, if the ring over which the sequence is defined is finite, then the sequence is guaranteed to eventually repeat. It is then natural to consider the following questions: (1) What factors determine the periods of these sequences once they begin to repeat? And (2) which periods arise from sequences that satisfy a particular linear recurrence relation, or from linear recurrences over a particular ring? Here we address these kinds of questions. Predicting the periodic behavior of any particular linearly recurring sequence, however, is actually exceedingly difficult, and so we instead attempt to determine the sets of periods that will arise from sequences defined by linear recurrences of a fixed degree and over some well-behaved ring.

In Chapter 2, we discuss various properties of sequences defined over a finite (commutative) ring with unity. In particular, we generalize a result of Ward [2] to show that the set of sequences has a natural ring structure and decomposes into a direct sum of periodic and null sequences (see Proposition 2.30). In Chapter 3, we give an exposition of the theory of sequences defined over finite fields. In particular, we show that the (least) period of a sequence is the order of a certain polynomial (see Theorem 3.17). We use this to describe the sets of possible periods of all linear recurrences of given degree k for small k. Finally, in Chapter 4, we apply some of the earlier theory to understand the periods of sequences defined over finite quotients of principal ideal domains.

ACKNOWLEDGMENTS

Special thanks to my thesis advisor Professor Michael Bush, who has helped me learn virtually everything I know about our research. I thank the Washington & Lee Mathematics Department's faculty for providing a great environment for cultivating my passion for learning, and to my peers for sharing in my joys and struggles as a math major and enthusiast. Finally, I thank God for putting me on the path of pursuing a profession in mathematics, and my parents and family for being extremely supportive of everything I do.

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION

Let $\mathbf{s} := (s_i)_{i \geq 0}$ be a sequence of elements in a ring R. Then $\mathbf{s}$ is said to satisfy a *linear recurrence relation of degree* $k \in \mathbb{Z}^+$ if each term from s_k onward in the sequence can be expressed as a linear function of the k previous terms, i.e. there exist elements $a_0, a_1, \ldots, a_{k-1} \in R$ such that for every integer $i \geq 0$, we have:

$$a_0 s_i + a_1 s_{i+1} + \ldots + a_{k-1} s_{i+k-1} = s_{i+k} \tag{1}$$

A sequence defined by a linear recurrence of degree k is completely determined by its first k terms. Later, we will refer to these terms collectively as the initial state vector (see Definition 2.1). For example, the sequence of Fibonacci numbers over $\mathbb{Z}$ is given by $\mathbf{s} := (0, 1, 1, 2, 3, 5,)$ and satisfies the linear recurrence relation of degree 2:

$$1 \cdot s_i + 1 \cdot s_{i+1} = s_{i+2} \qquad \forall i \geq 0$$

with initial state vector $(0, 1)$.

If there exists $n \in \mathbb{Z}^+$ such that for some integer $m \geq 0$, $s_i = s_{i+n}$ for all integers $i \geq m$, then we say that $\mathbf{s}$ is *ultimately periodic*, and call n a *period* of $\mathbf{s}$. If $m = 0$, then we say that $\mathbf{s}$ is *purely periodic*, or simply *periodic*. The *least period* $\rho(\mathbf{s})$ of $\mathbf{s}$ is defined to be a period satisfing $\rho(\mathbf{s}) \leq n$ for all periods n of $\mathbf{s}$, and the *preperiod* $\eta(\mathbf{s})$ of $\mathbf{s}$ is the least nonnegative integer such that the subsequence $(s_i)_{i \geq \eta(\mathbf{s})}$ is periodic. Finally, if $s_i = 0$ for all integers $i \geq n$ for some n, then we say $\mathbf{s}$ is a *null sequence*.

The terms in the Fibonacci sequence over $\mathbb{Z}$ increase exponentially, so that the sequence is not ultimately periodic. However, if we consider the Fibonacci sequence $\mathbf{s}$ over $\mathbb{Z}_2$, such that $\mathbf{s}$ satisfies the same linear recurrence relation and initial state vector as the sequence of Fibonacci numbers over $\mathbb{Z}$, we get:

$$\mathbf{s} := (0, 1, 1, 0, 1, 1, 0, 1, 1, \ldots)$$

For every integer $i \geq 0$, we obtain the same tuple of length 3: $(s_{3i}, s_{3i+1}, s_{3i+2}) = (0, 1, 1)$. Thus, $\mathbf{s}$ is periodic, with $\eta(\mathbf{s}) = 0$ and $\rho(\mathbf{s}) = 3$. Indeed, all the periods of $\mathbf{s}$ are of the form $3n$, where $n \in \mathbb{Z}^+$, as we shall see in Lemma 1.1.

Note that since any tuple of length k in a sequence satisfying a linear recurrence relations of degree k completely determines all subsequent terms in the sequence, a sufficient condition for $\mathbf{s}$ to begin to repeat (and be ultimately periodic) is for the same tuple of length k to appear twice in the sequence. Thus, for the Fibonacci sequence $\mathbf{s}$ over $\mathbb{Z}_2$, we see that $\mathbf{s}$ repeats immediately since the initial state vector $(0, 1)$ reappears after a shift of 3 terms.

Consider now the Fibonacci sequence $\mathbf{s}$ over $\mathbb{Z}_4$:

$$\mathbf{s} := (0, 1, 1, 2, 3, 1, 0, 1 \ldots)$$

Since we have returned to our initial state vector $(0, 1)$ after a shift of 6, we know that $\mathbf{s}$ repeats immediately, with $\eta(\mathbf{s}) = 0$ and $\rho(\mathbf{s}) = 6$.

In Lemma 2.4, we shall see that since $\mathbb{Z}_2$ and $\mathbb{Z}_4$ are finite rings (with unity), any linearly recurring sequence $\mathbf{s}$ is ultimately periodic. Furthermore, if $\mathbf{s}$ satisfies a linear recurrence such that, with respect to the notation in Equation 1, a_0 is a unit, then $\mathbf{s}$ is purely periodic. If a_0 in the linear recurrence is not a unit, then the latter does not necessarily hold. Consider the following sequence $\mathbf{t}$ over $\mathbb{Z}_4$ satisfying the linear recurrence relation $2t_i + t_{i+1} = t_{i+2}$ for every integer $i \geq 0$ and having the initial state vector $(0, 1)$:

$$\mathbf{t} := (0, 1, 1, 3, 1, 3, \ldots)$$

In this case, we never return to our initial state vector. Rather, $\mathbf{t}$ begins to repeat at $t_2 = 1$, with the tuple $(1, 3)$ of length 2 reappearing after a shift of 2. Thus, $\eta(\mathbf{t}) = 2$ and $\rho(\mathbf{t}) = 2$, and so $\mathbf{t}$ is ultimately periodic, but not periodic. Notice that $\mathbf{t}$ is defined in almost exactly the same way as the Fibonacci sequence $\mathbf{s}$ over $\mathbb{Z}_4$. The only difference is that, with respect to the notation in Equation 1, here we have $a_0 = 2$ not a unit in $\mathbb{Z}_4$.

The objective of this thesis is to study the sets of least periods that arise from linear recurrences of a specified degree k over finite fields and over related finite quotients of principal ideal domains. In Chapter 2, we will look into the general characteristics of sequences over finite rings with unity, laying the foundations for later chapters. In Chapter 3, we will focus on sequences over finite fields, and completely determine their least periods using the uniquely determined minimal polynomials associated to those sequences. Finally, in Chapter 4, we will study the broader class of linearly recurring sequences over principal ideal domains in order to draw conclusions about sequences over various types of quotients of polynomial rings over finite fields. We will then apply these results, in particular, to sequences defined over cyclic group algebras.

1.1. General Properties of Ultimately Periodic Sequences

Since all linearly recurring sequences over a finite ring with unity inevitably repeat, we shall first analyze general properties of ultimately periodic sequences so as to lay the groundwork for future inquiry.

Lemma 1.1. *Let $\mathbf{s}$ be an ultimately periodic sequence. Then $n \in \mathbb{Z}^+$ is a period of $\mathbf{s}$ if and only if $\rho(s)|n$.*

Proof. Since $\mathbf{s}$ is ultimately periodic with (least) period $\rho(\mathbf{s})$, it follows that for all sufficiently large integers i, $s_i = s_{i+\rho(\mathbf{s})}$. By induction, we then have $s_i = s_{i+j\cdot\rho(\mathbf{s})}$ for each integer $j \geq 0$, so that every integer $n := j \cdot \rho(\mathbf{s})$ is a period of $\mathbf{s}$

Conversely, let n be a period of $\mathbf{s}$. Then $n \geq \rho(\mathbf{s})$ by definition. By the division algorithm, $n = q \cdot \rho(\mathbf{s}) + r$ for some unique nonnegative integers q and r, where $0 \leq r < \rho(\mathbf{s})$. Since $\mathbf{s}$ is ultimately periodic with periods n and $\rho(\mathbf{s})$, it follows that for all sufficiently large integers i, $s_i = s_{i+\rho(\mathbf{s})}$ and $s_i = s_{i+n}$. We know from above that $s_i = s_{i+j\cdot\rho(\mathbf{s})}$ for each integer $j \geq 0$. Thus,

$$s_i = s_{i+n} = s_{i+q\cdot\rho(\mathbf{s})+r} = s_{i+r+q\cdot\rho(\mathbf{s})} = s_{i+r},$$

for sufficiently large i, so either $r < \rho(\mathbf{s})$ is also a period of $\mathbf{s}$ or $r = 0$. We rule out the former by the definition of $\rho(\mathbf{s})$. Hence, $n = q \cdot \rho(\mathbf{s})$, i.e. $\rho(\mathbf{s})|n$. □

Definition 1.2. Let $\mathbf{s} := (s_i)_{i\geq 0}$ be a sequence and let j be a nonnegative integer. Then $\mathbf{s}^{(j)} := (s_{j+i})_{i\geq 0}$ denotes the j-shifted subsequence of $\mathbf{s}$.

It is obvious that any period of an ultimately periodic sequence is bound to arise in a shift of the sequence. Hence, using the above notation, for every integer $j \geq 0$, $\rho(\mathbf{s}^{(j)}) = \rho(\mathbf{s})$.

Lemma 1.3. *Let S_1 and S_2 be sets, and let $\mathbf{s} := (u_i, v_i)_{i\geq 0}$ be a sequence in the cartesian product $S_1 \times S_2$, with component sequences $\mathbf{u} := (u_i)_{i\geq 0}$ in S_1 and $\mathbf{v} := (v_i)_{i\geq 0}$ over S_2. Then $\mathbf{s}$ is ultimately periodic if and only if $\mathbf{u}$ and $\mathbf{v}$ are ultimately periodic, and in this case $\rho(\mathbf{s}) = \operatorname{lcm}(\rho(\mathbf{u}), \rho(\mathbf{v}))$.*

Proof. $\mathbf{s}$ is ultimately periodic if and only if for sufficiently large integer $i \geq 0$ and some $n \in \mathbb{Z}^+$, $s_i = (u_i, v_i) = s_{i+n} = (u_{i+n}, v_{i+n})$ if and only if $\mathbf{u}$ and $\mathbf{v}$ are each ultimately periodic. Now suppose $\mathbf{s}$ is ultimately periodic. Let $c := \operatorname{lcm}(\rho(\mathbf{u}), \rho(\mathbf{v}))$. Note that $\rho(\mathbf{s})$ is a period of $\mathbf{s}$, and is subsequently a period of its components. Hence, $\rho(\mathbf{u})|\rho(\mathbf{s})$ and $\rho(\mathbf{v})|\rho(\mathbf{s})$, so that $c|\rho(\mathbf{s})$. On the other hand, by Lemma 1.1, c is a period of $\mathbf{u}$ and $\mathbf{v}$, so that for all sufficiently large integer $i \geq 0$, $s_i = (u_i, v_i) =$

$(u_{i+c}, v_{i+c}) = s_{i+c}$. Hence, c is also a period of $\mathbf{s}$, which implies that $\rho(\mathbf{s})|c$. Therefore, $\rho(\mathbf{s}) = c$. □

We can inductively apply Lemma 1.3 to obtain the following generalized statement:

Corollary 1.4. For any $n \in \mathbb{Z}^+$, the least period of a linearly recurring sequence over the (external) direct sum of n rings with unity is equal to the least common multiple of the corresponding least periods of the component sequences.

1.2. Review Material on Algebra

In this section, we remind the reader of certain facts in Abstract Algebra, mostly pertaining to finite fields and principal ideal domains, that will come into play later on in the thesis. It may be helpful to skip it for now and refer back to it as needed when reading through later chapters. Much of the results and definitions in this section can be found in [3].

1.2.1. External and Internal Direct Sums

Definition 1.5. Let A_1 and A_2 be abelian groups. We define the (external) direct sum of A_1 and A_2 (commonly denoted by $A_1 \oplus A_2$) to be the group of elements in the set $\{(x, y) \mid x \in R_1, y \in R_2\}$ — i.e. the cartesian product of A_1 and A_2 — with commutative addition $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$.

Theorem 1.6. *Let N, P be subgroups of an abelian group A. If $N \cap P = \{0\}$ and $N + P = A$, then the map $\phi : N \oplus P \to A$ defined by $\phi((n, p)) = n + p$ is a group isomorphism.*

Definition 1.7. When the conditions in Theorem 1.6 hold, we say that A is an *internal direct sum* of N and P.

Definition 1.8. Let R_1 and R_2 be rings. We define the (external) direct sum of R_1 and R_2 (commonly denoted by $R_1 \oplus R_2$) to be the ring of elements in the set $\{(x, y) \mid x \in R_1, y \in R_2\}$ with addition and multiplication defined component-wise, so that $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ and $(x_1, y_1)(x_2, y_2) = (x_1x_2, y_1y_2)$.

Theorem 1.9. *Let I, J be ideals in a commutative ring R. If $I \cap J = \{0\}$ and $I + J = R$, then the map $\phi : I \oplus J \to R$ defined by $\phi((x, y)) = x + y$ is a ring isomorphism.*

Definition 1.10. When the conditions in Theorem 1.9 hold, we say that R is an *internal direct sum* of I and J.

1.2.2. Matrices

Definition 1.11. Let R be a ring. Then $M_k(R)$ denotes the space of all $k \times k$ matrices with entries in R. $GL_k(R)$ denotes the group (under matrix multiplication) of all invertible $k \times k$ matrices in $M_k(R)$, where invertibility means that a two-sided inverse exists. If R is commutative and has unity, the determinant can be defined, and a matrix M is invertible if and only if $\det(M)$ is a unit in R.

Finally, if R is a finite commutative ring with unity, then $GL_k(R)$ is a finite group under matrix multiplication. For any $A \in GL_k(R)$, let $\text{ord}(A)$ denote the multiplicative order of A in $GL_k(R)$. In general, if G is a finite group, we will use $\text{ord}(g)$ to denote the order of the element $g \in G$.

1.2.3. Finite Fields, Polynomials, and Extensions

Lemma 1.12. *Let $\mathbb{F}$ be a field, I a nonzero ideal in $\mathbb{F}[x]$, and $g(x) \in \mathbb{F}[x]$. Then $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.*

Proof. See [3] Theorem 16.4. □

Lemma 1.13. *Let R be a commutative ring with prime characteristic p, and let $n \in \mathbb{Z}^+$. Then for any $x, y \in R$, $(x+y)^{p^n} = x^{p^n} + y^{p^n}$*

Proof. See [3] Chapter 13, Exercise # 45.

□

Lemma 1.14. *Let $\mathbb{F}$ be a field. Then any polynomial $f(x) \in \mathbb{F}[x]$ has a multiple zero (in some extension of $\mathbb{F}$) if and only if $f(x)$ and its derivative $f'(x)$ share a common factor of positive degree in $\mathbb{F}[x]$.*

Proof. See [3] Theorem 20.5. □

Lemma 1.15. *Let $\mathbb{F}_q$ be a finite field with q elements, and let $f(x) \in \mathbb{F}_q[x]$ have degree $k \in \mathbb{Z}^+$. Then the quotient ring $\mathbb{F}_q[x] \big/ \langle f(x) \rangle$ has q^k distinct residue classes.*

Proof. Since $\mathbb{F}_q$ is a UFD, so is $\mathbb{F}_q[x]$. Thus, for any $g(x) \in \mathbb{F}_q[x]$, there exist unique polynomials $q(x), r(x) \in \mathbb{F}_q[x]$ with $\deg(r(x)) < k$ for which $g(x) = f(x)q(x) + r(x)$, so that $g(x) \equiv r(x) \bmod f(x)$. Hence, every residue class of $\mathbb{F}_q[x] \big/ \langle f(x) \rangle$ contains some $r(x)$ with $\deg(r(x)) < k$. Now, suppose that there exist $r_1(x), r_2(x) \in \mathbb{F}_q[x]$

with $r_1(x) \equiv r_2(x) \bmod f(x)$ and $\deg(r_1(x)), \deg(r_2(x)) < k$. Then $r_1(x) - r_2(x) \equiv 0 \bmod f(x)$, and $\deg(r_1(x) - r_2(x)) < k$. This is only true if $r_1(x) = r_2(x)$. Thus, every polynomial $r(x) \in \mathbb{F}_q[x]$ uniquely represents a residue class of $\mathbb{F}_q[x] \big/ \langle f(x) \rangle$. There exist q^k such polynomials, from the q possible coefficients of each power of x between 0 and $k-1$. Hence, $\mathbb{F}_q[x] \big/ \langle f(x) \rangle$ has q^k distinct residue classes.

□

If we replace the finite field F_q in Lemma 1.15 with an arbitrary commutative ring R of order q, then the statement there still holds under the additional assumption that $f(x)$ has a unit leading coefficient, as in the following lemma.

Lemma 1.16. *Let R be a commutative ring with q elements, and let $f(x) \in R[x]$ have degree $k \in \mathbb{Z}^+$ and a unit leading coefficient. Then the quotient ring $R[x] \big/ \langle f(x) \rangle$ has q^k distinct residue classes.*

Proof. Since $f(x)$ has a unit leading coefficient, every $g(x) \in R[x]$ has $r(x) \in R[x]$ with $\deg(r(x)) < k$ such that $g(x) \equiv r(x) \bmod f(x)$ via long division. Hence, there are at most q^k residue classes. For us to prove that each residue class has a unique representative with degree less than k, we note that if $f(x) | r(x)$ and $\deg(r(x)) < k$, then we must have $r(x) = 0$, since the leading coefficient of $f(x)$ is a unit (and hence not a zero divisor). Thus, using the same reasoning as in Lemma 1.15, it follows that each polynomial $r(x)$ of degree less than k uniquely represents a residue class of the quotient $R[x] \big/ \langle f(x) \rangle$.

□

Corollary 1.17. *Let $\mathbb{F}_q$ be a finite field, and let $p(y) \in \mathbb{F}_q[y]$ be an irreducible polynomial of degree d. Then*

$$\mathbb{F}_q[y] \big/ \langle p(y) \rangle \cong \mathbb{F}_{q^d}$$

Proof. See [3] Theorems 17.5 (Corollary 1), 20.3, and 22.3. We then apply Lemma 1.15 and the fact that finite fields are unique up to isomorphism. □

1.2.4. Principal Ideal Domains

Definition 1.18. If R is a commutative ring with unity, we say that ideals $I, J \subseteq R$ are relatively prime if $I + J = R$. We then say that elements $x, y \in R$ re relatively prime if the principal ideals $\langle x \rangle$ and $\langle y \rangle$ are relatively prime.

Lemma 1.19. Chinese Remainder Theorem

Let R be a principal ideal domain, let $m \in R$, and let $m := q_1 q_2 \cdots q_r$ be a decomposition of m in R such that $\{q_i \mid i = 1, 2, \ldots r\}$ is a pairwise relatively prime set. Then $R/\langle m\rangle \cong R/\langle q_1\rangle \oplus R/\langle q_2\rangle \oplus \cdots \oplus R/\langle q_r\rangle$.

Proof. We will prove this by induction. For integers $1 \leq s \leq r$, define $Q_s := \prod_{i=1}^{s} q_i$. Consider the homomorphism $\phi_1 : R \to R/\langle Q_1\rangle \oplus R/\langle q_2\rangle$ that maps $x \mapsto (x + \langle Q_1\rangle, x + \langle q_2\rangle)$. Since Q_1 and q_2 are relatively prime, there exist $a_1, a_2 \in R$ such that $a_1 Q_1 + a_2 q_2 = 1$. Let $(x_1 + \langle Q_1\rangle, x_2 + \langle q_2\rangle) \in R/\langle Q_1\rangle \oplus R/\langle q_2\rangle$. We then consider $x = x_2 a_1 Q_1 + x_1 a_2 q_2 \in R$. Since $a_1 Q_1 \equiv 1 \bmod q_2$ and $a_2 q_2 \equiv 1 \bmod Q_1$, we thus have $\phi(x) = (x + \langle Q_1\rangle, x + \langle q_2\rangle) = (x_1(a_2 q_2) + \langle Q_1\rangle, x_2(a_1 Q_1) + \langle q_2\rangle) = (x_1 + \langle Q_1\rangle, x_2 + \langle q_2\rangle)$. Therefore, ϕ_1 is surjective. Now, $\ker(\phi) := \{x \in R \mid \phi(x) = (0 + \langle Q_1\rangle, 0 + \langle q_2\rangle)\} = \langle \mathrm{lcm}(Q_1, q_2)\rangle = \langle Q_1 q_2\rangle$, since Q_1 and q_2 are relatively prime. Therefore, by the First Isomorphism Theorem,

$$R/\langle Q_2\rangle = R/\langle Q_1 q_2\rangle \cong R/\langle Q_1\rangle \oplus R/\langle q_2\rangle = R/\langle q_1\rangle \oplus R/\langle q_2\rangle$$

Now consider the homomorphism $\phi_2 : R \to R/\langle Q_2\rangle \oplus R/\langle q_3\rangle$ that maps $x \mapsto (x + \langle Q_2\rangle, x + \langle q_3\rangle)$. We note that since $\{q_i \mid i = 1, 2, \ldots r\}$ is a set of pairwise relatively prime elements, for any i, q_i is relatively prime to $\prod_{j \in S} q_j$, where $S \subset \{1, 2, \ldots r\}$ such that $i \notin S$. Thus, by similar arguments as above, since Q_2 and q_3 are relatively prime, we have

$$R/\langle Q_3\rangle = R/\langle Q_2 q_3\rangle \cong R/\langle Q_2\rangle \oplus R/\langle q_3\rangle \cong R/\langle q_1\rangle \oplus R/\langle q_2\rangle \oplus R/\langle q_3\rangle$$

More generally, an inductive argument shows that:

$$R/\langle m\rangle = R/\langle Q_r\rangle \cong R/\langle q_1\rangle \oplus R/\langle q_2\rangle \oplus \ldots \oplus R/\langle q_r\rangle$$

□

Corollary 1.20. *Let R be a principal ideal domain, let $m \in R$, and let $m := p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be the prime factorization of m in R. Then $R/\langle m\rangle \cong R/\langle p_1^{e_1}\rangle \oplus R/\langle p_2^{e_2}\rangle \oplus \cdots \oplus R/\langle p_r^{e_r}\rangle$.*

Proof. For integers $1 \leq s \leq r$, define $q_s := p_s^{e_s}$. The statement then follows from Lemma 1.19. □

Lemma 1.21. *Let R be a principal ideal domain. If $p \in R$ is prime, then for every $e \in \mathbb{Z}^+$, $\langle p^e\rangle/\langle p^{e+1}\rangle \cong R/\langle p\rangle$.*

Proof. Consider the surjective homomorphism $\phi : R \to \langle p^e\rangle/\langle p^{e+1}\rangle$ that maps $x \mapsto xp^e + \langle p^{e+1}\rangle$. Then $\ker(\phi) = \langle p\rangle$ so that by the First Isomorphism Theorem, $R/\langle p\rangle \cong \langle p^e\rangle/\langle p^{e+1}\rangle$. □

Lemma 1.22. *Let R be a principal ideal domain. Then $R/\langle m\rangle$ is finite for every nonzero $m \in R$ if and only if $R/\langle p\rangle$ is a finite field for every prime $p \in R$.*

Proof. In a principal ideal domain, primes are irreducible, and so the ideals they generate are maximal. Quotients of commutative rings with unity by maximal ideals are in turn fields. Thus, for any prime $p \in R$, $R/\langle p\rangle$ is a field. If for every nonzero $m \in R$, $R/\langle m\rangle$ is finite, then $R/\langle p\rangle$ is a finite field, since $p \neq 0$.

Conversely, we now suppose that for every prime $p \in R$, $R/\langle p\rangle$ is a finite field. By Lemma 1.21, we know that for any arbitrary prime p and any $e \in \mathbb{Z}^+$, $R/\langle p\rangle \cong \langle p^e\rangle/\langle p^{e+1}\rangle$. Specifically, $R/\langle p\rangle \cong \langle p\rangle/\langle p^2\rangle$. Let $n := |R/\langle p\rangle| = |\langle p\rangle/\langle p^2\rangle|$. By the Third Isomorphism Theorem, $R/\langle p^2\rangle \Big/ \langle p\rangle/\langle p^2\rangle \cong R/\langle p\rangle$, so that $|R/\langle p^2\rangle \Big/ \langle p\rangle/\langle p^2\rangle| = |R/\langle p\rangle| = n$. Thus, there exist n residue classes in $R/\langle p^2\rangle \Big/ \langle p\rangle/\langle p^2\rangle$, with each residue class having $|\langle p\rangle/\langle p^2\rangle| = n$ elements. Thus, $|R/\langle p^2\rangle| = n^2$. We may then use similar arguments to show that $|R/\langle p^3\rangle| = n^3$, and that, by induction, $|R/\langle p^e\rangle| = n^e$ for every $e \in \mathbb{Z}^+$.

Now let $m \in R$ be an arbitrary nonzero element. Then m has a unique prime factorization $m = \prod_{i=1}^r p_r^{e_r}$. By the Chinese Remainder Theorem (Lemma 1.19), we then have $R/\langle m\rangle \cong R/\langle p_1^{e_1}\rangle \oplus R/\langle p_2^{e_2}\rangle \oplus \cdots \oplus R/\langle p_r^{e_r}\rangle$. Thus, $|R/\langle m\rangle| = \prod_{i=1}^r |R/\langle p_i^{e_i}\rangle|$. Letting $n_i := |R/p_i|$, we then have, by our previous result, that $|R/\langle m\rangle| = \prod_{i=1}^r n_i^{e_i}$. So $R/\langle m\rangle$ is finite.

□

1.3. Power Series and Reciprocal Polynomials

In Chapter 2, we will introduce the concept of characteristic polynomials, which allow for the analysis of linear recurrence relations by viewing them as elements of a polynomial ring. In Chapter 3, we analogously view sequences as ‘polynomials’ of infinite degree, i.e. as power series. This allows for us to view both the linear recurrence and the linearly recurring sequence as elements of the same algebraic space (the ring of power series).

This section sets up the machinery that we need to analyze the interaction between characteristic polynomials of linear recurrence relations and power series expressions of linearly recurring sequences. It may be beneficial to skip this section for now and refer to it while reading through Section 3.3.

Definition 1.23. Let R be a ring. Then $R[[x]]$ denotes the ring of power series such that for every element $S(x) \in R[[x]]]$, we express $S(x) := \sum_{i=0}^{\infty} s_i x^i$, where $s_i \in R$ for all i.

If $S(x) = s_0 + s_1 x + s_2 x^2 + \ldots \in R[[x]]$ and $T(x) = t_0 + t_1 x + t_2 x^2 + \ldots \in R[[x]]$, then we define:

- $S(x) + T(x) = (s_0 + t_0) + (s_1 + t_1)x + (s_2 + t_2)x^2 + \ldots$
- $S(x)T(x) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} s_j t_{i-j} \right) x^i$

Lemma 1.24. *Let R be a commutative ring with unity. $B(x) := \sum_{n=0}^{\infty} b_n x^n \in R[[x]]$ has a multiplicative inverse if and only if $B(0) = b_0$ is a unit.*

Proof. ($\implies$) Suppose there exists an inverse $C(x) := \sum_{n=0}^{\infty} c_n x^n \in R[[x]]$ such that $B(x)C(x) = 1$. Then we have $B(x)C(x) = \sum_{j=0}^{\infty} \left(\sum_{i=0}^{j} b_i c_{j-i} \right) x^j = 1$, so that the following infinite set of equalities hold:

$$\begin{array}{cl}
b_0 c_0 & = 1 \\
b_0 c_1 + b_1 c_0 & = 0 \\
b_0 c_2 + b_1 c_1 + b_2 c_0 & = 0 \\
\vdots & \vdots \\
b_0 c_n + b_1 c_{n-1} + \cdots + b_n c_0 & = 0 \\
\vdots & \vdots
\end{array}$$

From the first equation, $b_0 c_0 = 1$, we determine that b_0 must be a unit.

($\Longleftarrow$) Now suppose b_0 is a unit. Then we may construct a power series $C(x) := \sum_{n=0}^{\infty} c_n x^n$ whose coefficients satisfy the infinite array of equations above in the following manner: We first uniquely determine $c_0 = b_0^{-1}$. We subsequently determine $c_1 = -b_0^{-1} b_1 c_0$ from the second equation, c_2 from the third, etc., so that by strong induction, for any nonnegative integer n, we can recursively obtain c_n via the formula $c_n = -b_0^{-1} \sum_{i=1}^{n} b_i c_{n-i}$. Thus, we have uniquely determined $C(x) \in R[[x]]$ satisfying $B(x)C(x) = 1$.

Hence, $B(x)$ has a multiplicative inverse if and only if b_0 is a unit. □

Note If $B(x) \in R[[x]]$ is a unit, then $\frac{1}{B(x)} \in R[[x]]$ denotes the multiplicative inverse of $B(x)$.

Definition 1.25. Let $f(x) \in R[x]$ be an arbitrary polynomial of degree k. Then the reciprocal polynomial $f^*(x) \in R[x]$ of $f(x)$ is given by:

$$f^*(x) := x^k f(1/x) \tag{2}$$

Note that by this definition:

$$f(x) = x^k f^* \left(\frac{1}{x} \right) \tag{3}$$

where $k := \deg(f(x))$.

Note that $\deg(f^*(x))$ need not equal k, hence, it is not necessarily the case that $(f^*)^*(x) = f(x)$. For example, if $f(x) := x^2 + x$, then $f^*(x) = x + 1$ and $(f^*)^*(x) = x + 1 \neq f(x)$.

Lemma 1.26. *Let R be a ring, and let $a(x), b(x), c(x) \in R[x]$ be polynomials such that $a(x) = b(x)c(x)$. Then $a^*(x) = b^*(x)c^*(x)$.*

Proof. Let $n := \deg(b(x))$ and $m := \deg(c(x))$. Treating $b(x)$ and $c(x)$ as power series, we may then express $b(x) = \sum_{i=0}^{\infty} b_i x^i$ and $c(x) = \sum_{i=0}^{\infty} c_i x^i$, where for all integers $i > n$, $b_i = 0$, and for all integers $i > m$, $c_i = 0$. Then $a(x) = b(x)c(x) =$

$\sum_{j=0}^{\infty}\left(\sum_{i=0}^{j} b_i c_{j-i}\right) x^j$. Taking their reciprocal polynomials, we have:

$$\begin{aligned}
b^*(x) = x^n b(1/x) = x^n \left(\sum_{i=0}^{\infty} b_i \left(\frac{1}{x}\right)^i\right) = \sum_{i=0}^{\infty} b_i x^{n-i} \\
c^*(x) = x^m c(1/x) = x^m \left(\sum_{i=0}^{\infty} c_i \left(\frac{1}{x}\right)^i\right) = \sum_{i=0}^{\infty} c_i x^{m-i}
\end{aligned}$$

where $b^*(x)$ and $c^*(x)$ are indeed polynomials, since the coefficients of all negative exponents vanish by definition.

$$\begin{aligned}
b^*(x)c^*(x) &= \sum_{j=0}^{\infty}\left(\sum_{i=0}^{j} b_i c_{j-i}\right) x^{n+m-j} = x^{n+m}\left(\sum_{j=0}^{\infty}\left(\sum_{i=0}^{j} b_i c_{j-i}\right)\left(\frac{1}{x}\right)^j\right) \\
&= x^{n+m} a(1/x) = a^*(x)
\end{aligned}$$

Note that for any integer $j > n+m$, either $i > n$ or $j - i \geq j - n > m$, and so the coefficient of $\left(\frac{1}{x}\right)^j$ vanishes for all $j > n+m$. Thus, $a^*(x)$ is indeed a polynomial. □

CHAPTER 2. SEQUENCES OVER FINITE RINGS WITH UNITY

We will now describe properties of linearly recurring sequences over arbitrary finite rings with unity, with the goal of describing properties about their corresponding least periods which will become useful in the following two chapters. Particularly, in Section 2.2 we will show that the ring of linearly recurring sequences decomposes nicely into an internal direct sum of the ideals of purely periodic and null sequences. In Section 2.3, we will introduce the associated companion matrix of a linear recurrence relation, and use it to determine properties of the least periods of sequences that satisfy the recurrence.

Since the rings with which we are concerned (finite fields and quotients of polynomial rings over finite fields) always have unity, the term 'ring' will always mean ring with unity from this point onward in the thesis. Later, we will also assume the ring is commutative but not initially.

2.1. Properties of Linearly Recurring Sequences

Recall that a linearly recurring sequence may be completely defined by the linear recurrence relation that it satisfies and its initial state vector. More generally, any substring of k terms completely determines the rest of the sequence via the linear recurrence (of at most k terms). Hence, it is useful to identify these substrings in a precise way, as follows:

Definition 2.1. Let $k \in \mathbb{Z}^+$ be fixed. Then the jth state vector $\mathbf{s}_j$ of a sequence $\mathbf{s} := (s_i)_{i \geq 0}$ is the substring of length k given by $\mathbf{s}_j := (s_j, s_{j+1}, \ldots, s_{j+k-1})$. We will refer to $\mathbf{s}_0$ in particular as the initial state vector of $\mathbf{s}$.

Applying state-vector notation to the ideas discussed in the introductory chapter, we observe that any state vector of a linearly recurring sequence $\mathbf{s}$ completely determines all subsequent terms via the linear recurrence. Thus, a sufficient condition for $\mathbf{s}$ to be ultimately periodic is for two state vectors to be identical. $\mathbf{s}$ begins to repeat at s_j for the least integer $j \geq 0$ such that $\mathbf{s}_j = \mathbf{s}_{j+n}$ for some $n \in \mathbb{Z}^+$. In this case, $j = \eta(\mathbf{s})$ and $\rho(\mathbf{s})$ is the least such n for which the equality $\mathbf{s}_j = \mathbf{s}_{j+n}$ holds.

The next two lemmas follow immediately from the definitions. Their proofs are straightforward and are omitted here:

Lemma 2.2. *The following statements about a linearly recurring sequence* $\mathbf{s}$ *are equivalent for any given integers* $m \geq 0$ *and* $n > 0$*:*

- *$s_i = s_{i+n}$ for all integers $i \geq m$*
- *$\mathbf{s}_i = \mathbf{s}_{i+n}$ for some integer $i \geq m$*
- *$\mathbf{s}$ is ultimately periodic with period n and preperiod $\eta(\mathbf{s}) \leq m$.*

In particular, we conclude the following for the special cases of null and periodic sequences.

Lemma 2.3. *A linearly recurring sequence $\mathbf{s}$ is*

1. *periodic with period n if and only if $\mathbf{s}_0 = \mathbf{s}_n$*
2. *a null sequence with $\eta(\mathbf{s}) \leq n$ if and only if $\mathbf{s}_n = \mathbf{0}$, where $\mathbf{0}$ is the the zero vector.*

We are now ready to address the periodicity of linearly recurring sequences.

Lemma 2.4. *Let R be a finite ring, and let $\mathbf{s} = (s_i)_{i \geq 0}$ be a linearly recurring sequence over R. Then $\mathbf{s}$ is ultimately periodic. If $\mathbf{s}$ satisfies a linear recurrence relation of the form of Equation 1, such that a_0 is a unit in R, then $\mathbf{s}$ is (purely) periodic.*

Proof. Let $\mathbf{s}$ satisfy a linear recurrence relation of degree k given by Equation 1. Since R is finite, there are only a finite number of possible tuples of elements in R of length k. On the other hand, $\mathbf{s}$ is an infinite sequence, with a subsequently infinite number of state vectors. Thus, by the pigeonhole principle, there must exist distinct integers i and j with $i < j$ such that $\mathbf{s}_i = \mathbf{s}_j$. Since a tuple of k elements and a linear recurrence relation of degree k completely determine the subsequent elements in a sequence, all corresponding elements after $\mathbf{s}_i$ and $\mathbf{s}_j$ must be the same. Hence, by Lemma 2.2, the sequence is ultimately periodic.

Referring to Equation 1, suppose a_0 is a unit. We can then reorganize the terms in the linear recurrence relation so as to solve for the previous element in the sequence from the k subsequent elements, as follows:

$$s_i = (-a_0^{-1}a_1)s_{i+1} + \ldots + (-a_0^{-1}a_{k-1})s_{i+k-1} + a_0^{-1}s_{i+k}$$

Thus, we can conclude that all the corresponding elements before every instance of the repeated length-k substring must match as well, and so $\mathbf{s}$ is periodic. □

Recall that a tuple of length k in a sequence generated by a linear recurrence relation of degree k completely determines the rest of the sequence. It follows that for any two sequences $\mathbf{s}$ and $\mathbf{t}$ satisfying the same linear recurrence relation of degree k, $\mathbf{s}_j = \mathbf{t}_{j'}$ for some nonnegative integers j and j' implies that $\mathbf{s}^{(j)} = \mathbf{t}^{(j')}$, and so we arrive at the following statement about $\mathbf{s}$ and $\mathbf{t}$:

Lemma 2.5. *If* $\mathbf{s}$ *and* $\mathbf{t}$ *are sequences that satisfy the same linear recurrence relation and if* $\mathbf{t} = \mathbf{s}^{(j)}$ *for some integer* $j \geq 0$*, then* $\rho(\mathbf{s}) = \rho(\mathbf{t})$*. More generally,* $\rho(\mathbf{s}) = \rho(\mathbf{t})$ *if* $\mathbf{s}$ *and* $\mathbf{t}$ *share a common state vector.*

Although in this thesis we are interested in the least periods of particular linearly recurring sequences, our ultimate goal lies in describing in a meaningful way the sets of least periods that arise from sequences satisfying a general class of linear recurrences of a given degree over a certain ring. We construct the following notation to better address these sets.

Definition 2.6. Let $k \in \mathbb{Z}^+$ and let R be a finite ring. We let $\mathrm{P}(k, R)$ denote the set of least periods that arise from sequences defined by a linear recurrence relation of degree k over R.

Furthermore, in our notation for a general linear recurrence relation as given by Equation 1, we do not restrict any of the coefficients to being nonzero. Hence, by way of example, the linear recurrence that the Fibonacci sequence must satisfy can be vaguely described as being one of degree k, where $k \geq 2$ is an integer, by merely setting $a_i = 0$ for every i between 0 and a_{k-3}. We shall then uniquely label the least possible degree of the linear recurrence as its 'nontrivial' degree, defined below.

Definition 2.7. We say that a linear recurrence relation has the nontrivial degree k if the linear recurrence is given by Equation 1 with $a_0 \neq 0$.

Proposition 2.8. *Let* $k \in \mathbb{Z}^+$ *and let* R *be a finite ring. Then for every integer* $l \geq k$*, if a sequence* $\mathbf{s}$ *satisfies a linear recurrence relation of nontrivial degree* k*, then* $\mathbf{s}$ *also satisfies a linear recurrence relation of nontrivial degree* l*. In particular,* $\mathrm{P}(k, R) \subseteq \mathrm{P}(l, R)$*.*

Proof. Let $\mathbf{s}$ be a sequence over R satisfying a linear recurrence relation of degree k given by Equation 1:

$$a_0 s_i + a_1 s_{i+1} + \ldots + a_{k-1} s_{i+k-1} = s_{i+k}$$

For any integer $i \geq 0$, we may express s_{i+k+1} in terms of the previous k terms and then partially substitute the expansion of s_{i+k}, so as to express s_{i+k+1} with respect to the previous $k+1$ terms, as follows:

$$\begin{aligned} s_{i+k+1} &= a_0 s_{i+1} + a_1 s_{i+2} + \ldots + a_{k-2} s_{i+k-1} + a_{k-1} s_{i+k} \\ &= \left(\sum_{j=0}^{k-2} a_j s_{i+j+1} \right) + a_{k-1} s_{i+k}. \end{aligned}$$

Writing $a_{k-1}s_{i+k} = s_{i+k} + (a_{k-1} - 1)s_{i+k}$ and substituting for s_{i+k}, we then obtain:

$$\begin{aligned} s_{i+k+1} &= \sum_{j=0}^{k-2} a_j s_{i+j+1} + \sum_{j=0}^{k-1} a_j s_{i+j} + (a_{k-1} - 1)s_{i+k} \\ &= \sum_{j=0}^{k-2} a_j s_{i+j+1} + \left(a_0 s_i + \sum_{j=1}^{k-1} a_j s_{i+j} \right) + (a_{k-1} - 1)s_{i+k} \\ &= a_0 s_i + \left(\sum_{j=0}^{k-2} a_j s_{i+j+1} + \sum_{j=0}^{k-2} a_{j+1} s_{i+j+1} \right) + (a_{k-1} - 1)s_{i+k} \\ &= a_0 s_i + \sum_{j=0}^{k-2} (a_j + a_{j+1}) s_{i+j+1} + (a_{k-1} - 1)s_{i+k}. \end{aligned}$$

Hence, **s** also satisfies a linear recurrence relation of degree $k+1$, and by induction **s** satisfies a linear recurrence of degree l, for any integer $l \geq k$. The partial substitution that we used above guarantees that the degree of the new expression of the linear recurrence relation is nontrivial if the old expression is nontrivial, since we still have $a_0 \neq 0$ as the coefficient of s_i. □

It is often useful to associate polynomials to linear recurrences. The structure in the associated polynomial ring gives further insight on the behavior of the sequences that satisfy the recurrences. We define these 'characteristic polynomials' in the following manner.

Definition 2.9. We define the characteristic polynomial of degree k associated with the linear recurrence relation given by Equation 1 to be the polynomial

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_0 \in R[x] \tag{4}$$

where R is the ring over which the sequence is defined.

In the extreme case, the empty recurrence relation given by $s_i = 0$ $(i \geq 0)$ of degree $k = 0$ and solely satisfied by the zero sequence will have the associated characteristic polynomial $f(x) = 1$.

By its definition, the degree of an associated characteristic polynomial is determined by the degree of the recurrence. Note, however, that since a linear recurrence can be vaguely described as being of any arbitrary degree by making the coefficients of a sufficient number of terms zero, it will in turn have an infinite number of possible associated characteristic polynomials, all differing by a factor of x^h, where h is a nonzero integer. In this thesis, we will always implicitly have a particular degree k in mind when referring to a linear recurrence relation, and subsequently have the associated characteristic polynomial be of the same degree k, with Equation 1 directly linked to the Equation 4 through the natural bijection.

Note that the characteristic polynomial of the form $f(x) := x^h g(x)$, where h is a nonnegative integer and $g(0) \neq 0$, corresponds to a linear recurrence relation that ignores the first h terms of the initial state vector when constructing a sequence. These ignored first terms will be of no consequence to the periodicity of the sequence. Hence, as will be the case in Chapter 3, we sometimes limit the scope of our analyses to characteristic polynomials of the form $g(x)$, where again $g(0) \neq 0$. Lemma 2.10 below will help us when we shift gears from studying sequences defined by $f(x)$ to studying sequences defined by $g(x)$, which we note corresponds to limiting the scope of our analysis to linear recurrences of nontrivial degree only.

Lemma 2.10. *Let $\mathbf{s} := (s_i)_{i \geq 0}$ be a sequence that satisfies a linear recurrence relation over the ring R with associated characteristic polynomial $f(x) := x^h g(x) \in R[x]$, where $h \geq 0$ is an integer and $g(x) \in R[x]$ such that $g(0) \neq 0$. Then the subsequence $(s_i)_{i \geq h}$ satisfies a linear recurrence relation with associated characteristic polynomial $g(x)$.*

Proof. If $g(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_0$, then

$$\begin{aligned} f(x) = x^h g(x) &= x^h(x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \ldots - a_0) \\ &= x^{h+k} - a_{k-1}x^{h+k-1} - a_{k-2}x^{h+k-2} - \ldots - a_0 x^h \end{aligned}$$

Thus, $\mathbf{s}$ satisfies the linear recurrence relation given by

$$s_{i+h}a_0 + s_{i+h+1}a_1 + \ldots + s_{i+h+k-1}a_{k-1} = s_{i+h+k} \quad \forall i \geq 0.$$

And so for every integer $i \geq h$, $\mathbf{s}$ satisfies Equation 1. That is:

$$s_j a_0 + s_{j+1} a_1 + \ldots + s_{j+k-1} a_{k-1} = s_{j+k}$$

where $j := i+h \geq h$. Therefore, the subsequence $(s)_{i \geq h}$ satisfies the linear recurrence relation given by Equation 1, with an associated characteristic polynomial $g(x)$. □

The characteristic polynomial offers a convenient way of referring to the linear recurrence relation to which it is associated. Accordingly, we use the following notation to refer to sequences that satisfy a particular linear recurrence:

Definition 2.11. Let R be a ring. We let $\mathcal{A}(f(x))$ denote the set of all sequences over R that satisfy the linear recurrence relation with characteristic polynomial $f(x) \in R[x]$. If R is finite, then we let $\mathcal{P}(f(x))$ and $\mathcal{N}(f(x))$ denote the subsets of periodic and null sequences, respectively, that satisfy the given linear recurrence.

Remark 2.12. *Let $\mathbf{s} \in \mathcal{A}(f(x))$. Then for every integer $j \geq 0$, the shifted subsequence $\mathbf{s}^{(j)} \in \mathcal{A}(f(x))$.*

Using the ring axioms, we can verify that a sequence generated from the term-by-term sum or difference of two sequences satisfying the same linear recurrence relation must satisfy the linear recurrence as well. By way of example, suppose two sequences $\mathbf{s} := (s_i)_{i \geq 0}$ and $\mathbf{t} := (t_i)_{i \geq 0}$ satisfy the recurrence $u_i + 2u_{i+1} = u_{i+2}$ for every integer $i \geq 0$. Then the sequence $\mathbf{s} + \mathbf{t} = (s_i + t_i)_{i \geq 0}$ satisfies $(s_i + t_i) + 2(s_{i+1} + t_{i+1}) = s_i + t_i + 2s_{i+1} + 2t_{i+1} = (s_i + 2s_{i+1}) + (t_i + 2t_{i+1}) = s_{i+2} + t_{i+2}$ for every integer $i \geq 0$. Therefore, $\mathcal{A}(f(x))$ is closed under addition. One can check that the associative property is satisfied as well, that the zero sequence serves as the identity, and that for every sequence in $\mathcal{A}(f(x))$, we can construct an additive inverse by taking the inverse of every term. Hence, $\mathcal{A}(f(x))$ is an abelian group.

It is also clear that the sum of two periodic sequences will be periodic and that the sum of two null sequences will be null. Hence, $\mathcal{P}(f(x))$ and $\mathcal{N}(f(x))$ are subgroups of $\mathcal{A}(f(x))$.

Since any linearly recurring sequence is ultimately periodic by Lemma 2.4, one may break it down into the sum of a null and a purely periodic sequence, leading to the following proposition:

Proposition 2.13. *Let R be a finite ring, and let $f(x) \in R[x]$ be the characteristic polynomial of a linear recurrence relation over R. Then the abelian group $\mathcal{A}(f(x))$ (of component-wise addition) has the internal direct sum decomposition $\mathcal{A}(f(x)) = \mathcal{P}(f(x)) \oplus \mathcal{N}(f(x))$.*

Proof. Note that since component-wise addition of sequences is commutative (from R being a ring), it is straightforward to verify that $\mathcal{P}(f(x))$ and $\mathcal{N}(f(x))$ are subgroups of $\mathcal{A}(f(x))$.

We also see that by the definition of purely periodic and null sequences, $\mathcal{P}(f(x)) \cap \mathcal{N}(f(x)) = \{\mathbf{0}\}$, where here $\mathbf{0}$ denotes the infinite zero sequence.

Now set $S := \{\mathbf{u} + \mathbf{v} \mid \mathbf{u} \in \mathcal{P}(f(x)), \mathbf{v} \in \mathcal{N}(f(x))\} \subseteq \mathcal{A}(f(x))$. We show that $S = \mathcal{A}(f(x))$ by verifying the reverse containment. Let $\mathbf{s} = (s_i)_{i \geq 0} \in \mathcal{A}(f(x))$. We want to construct a purely periodic sequence $\mathbf{u} \in \mathcal{A}(f(x))$ that matches term-by-term with $\mathbf{s}$ from some point onwards, so that the terms cancel when we subtract $\mathbf{s} - \mathbf{u}$ and we are left with a null sequence.

Since $\mathbf{s}$ is ultimately periodic by Lemma 2.4, for every integer $i \geq 0$, $s_{i+\eta(\mathbf{s})} = s_{i+\eta(\mathbf{s})+\rho(\mathbf{s})}$. Let $n \in \mathbb{Z}^+$ be such that $n \geq \eta(\mathbf{s})$ and $\rho(\mathbf{s})|n$. By Lemma 1.1, n is a period of $\mathbf{s}$. Define $\mathbf{u} := (u_i)_{i \geq 0} = \mathbf{s}^{(n)}$. Then for every integer $i \geq 0$, $u_i = s_{i+n} = s_{i+n+\rho(\mathbf{s})} = s_{i+\rho(\mathbf{s})+n} = u_{i+\rho(\mathbf{s})}$. Consequently, by Remark 2.12, $\mathbf{u} \in \mathcal{P}(f(x))$ with $\rho(\mathbf{u}) = \rho(\mathbf{s})$, by Lemma 2.5. Note that n is a period of $\mathbf{s}$ by Lemma 1.1, so that for every integer $i \geq n \geq \eta(\mathbf{s})$, $s_i = s_{i+n}$. Now define $\mathbf{v} := (v_i)_{i \geq 0} = \mathbf{s} - \mathbf{u}$. Then for every integer $i \geq 0$, we have:

$$v_{n+i} = s_{n+i} - u_{n+i} = s_{n+i} - s_{(n+i)+n} = s_{n+i} - s_{n+i} = 0$$

Hence, $v_i = 0$ for sufficiently large i. It follows that $\mathbf{v} = \mathbf{s} - \mathbf{u} \in \mathcal{N}(f(x))$, and therefore, $\mathbf{s} = \mathbf{u} + \mathbf{v} \in S$. Thus, $S = \mathcal{A}(f(x))$.

We have thus established the conditions necessary to show that the abelian group $\mathcal{A}(f(x))$ is the internal direct sum of its subgroups of periodic and null sequences. □

Example 2.14. Let us revisit the sequence $\mathbf{t} \in \mathcal{A}(x^2 - x - 2)$ defined over $\mathbb{Z}_4$ from Chapter 1, which satisfies the linear recurrence relation $2t_i + t_{i+1} = t_{i+2}$ for all integers $i \geq 0$ and with initial state vector $(0, 1)$. We know that $\mathbf{t} := (0, 1, 1, 3, 1, 3, \ldots)$, and that $\rho(\mathbf{t}) = 2$ and $\eta(\mathbf{t}) = 2$. Proposition 2.13 implies that $\mathbf{t}$ can be uniquely expressed as the sum of a purely periodic and null sequence in $\mathcal{A}(x^2 - x - 2)$. We can easily construct such sequences here by extending the periodic part of $\mathbf{t}$ and subtracting it from $\mathbf{t}$, killing off all of the repeating terms. We replace the first $\eta(\mathbf{t})$ terms of

$\mathbf{t}$ to construct a purely periodic sequence $\mathbf{u} := (1, 3, 1, 3, 1, 3, \ldots)$, and subsequently derive the null sequence $\mathbf{v} := \mathbf{t} - \mathbf{u} = (3, 2, 0, 0, 0, 0, \ldots)$, so that $\mathbf{t} = \mathbf{u} + \mathbf{v}$. One can check that indeed $\mathbf{u}, \mathbf{v} \in \mathcal{A}(x^2 - x - 2)$.

We now consider the set of all linearly recurring sequences over a particular ring, and make similar conclusions about this larger set of sequences.

Definition 2.15. Let R be a ring. We let $\mathcal{A}(R)$ denote the set of all linearly recurring sequences over R. Similarly, $\mathcal{P}(R)$ and $\mathcal{N}(R)$ denote the subsets of all linearly recurring periodic and null sequences, respectively, over R.

It is important to note that it is not necessary for any two sequences in $\mathcal{A}(R)$ to satisfy the same linear recurrence. Nevertheless, the following lemma shows that the set is still closed under component-wise addition, i.e. the sum of any two linearly recurring sequences is also a linearly recurring sequence.

Lemma 2.16. *Let R be a finite ring. Then $\mathcal{A}(R)$ is an abelian group, with $\mathcal{P}(R)$ and $\mathcal{N}(R)$ subgroups of $\mathcal{A}(R)$.*

Proof. Let $\mathbf{s}$ and $\mathbf{t}$ be linearly recurring sequences over R. Since every linearly recurring sequence is ultimately periodic by Lemma 2.4, $\mathbf{s}$ and $\mathbf{t}$ must satisfy linear recurrence relations of the form $s_{i+h} = s_{i+h+n_1}$ and $t_{i+h} = t_{i+h+n_2}$ for all integers $i \geq 0$, where $h \geq \max(\eta(\mathbf{s}), \eta(\mathbf{t}))$ is an integer, and where n_1 and n_2 are periods of $\mathbf{s}$ and $\mathbf{t}$, respectively. Thus, by Lemma 1.1, $\mathbf{s}$ and $\mathbf{t}$ both satisfy the linear recurrence relation $u_{i+h} = u_{i+h+n}$ for all integers $i \geq 0$, where $n := \operatorname{lcm}(\rho(\mathbf{s}), \rho(\mathbf{t}))$. Let $f(x) = x^{h+n} - x^h$ be the associated characteristic polynomial of said linear recurrence. Then $\mathbf{s}, \mathbf{t} \in \mathcal{A}(f(x))$, where $\mathcal{A}(f(x))$ is an abelian group. Thus, $\mathbf{s} + \mathbf{t}, -\mathbf{s} \in \mathcal{A}(f(x)) \subseteq \mathcal{A}(R)$, showing that $\mathcal{A}(R)$ is an abelian group. It is subsequently straightforward to verify that $\mathcal{P}(R)$ and $\mathcal{N}(R)$ are subgroups of $\mathcal{A}(R)$. □

Note that in the proof above, we account for the preperiods of $\mathbf{s}$ and $\mathbf{t}$ by inserting the extra h term in the linear recurrence relation and, subsequently, the characteristic polynomial. It is not necessarily the case that for a given characteristic polynomial $f(x)$, there will exist an integer $n > 0$ such that $f(x) | x^n - 1$.

Example 2.17. Consider the characteristic polynomial $x \in \mathbb{Z}_2[x]$ associated with the linear recurrence relation $0 \cdot (s_i) = s_{i+1}$ $(i \geq 0)$. Clearly x does not divide $x - 1$ over $\mathbb{Z}_2$.

Example 2.18. Consider $f(x) = x^2 - x - 2 \in \mathbb{Z}_4[x]$ associated with the linear recurrence relation $2t_i + t_{i+1} = t_{i+2}$. Note that 2 is a root of $f(x)$, and so if $f(x)|x^e - 1$ for some $e \in \mathbb{Z}^+$, then 2 is also a root of $x^e - 1$, i.e. $2^e = 1$, which is impossible in $\mathbb{Z}_4$. Therefore, no such e exists for which $f(x)|x^e - 1$.

The argument made in the proof of Proposition 2.13 may be extended to the abelian group of all linearly recurring sequences over a finite ring, so that:

Lemma 2.19. *For any finite ring R, the abelian group $\mathcal{A}(R)$ has a direct sum decomposition $\mathcal{A}(R) = \mathcal{P}(R) \oplus \mathcal{N}(R)$.*

An immediate implication of Proposition 2.13 is that the set of least periods that arise from sequences in $\mathcal{A}(f(x))$ is equal to the set of least periods that arise from sequences in $\mathcal{P}(f(x))$, i.e. the purely periodic sequences. In general, since $\mathcal{P}(R)$ and $\mathcal{N}(R)$ are also normal subgroups of $\mathcal{A}(R)$ through Lemma 2.16, we have the following Remark.

Remark 2.20. *For any $k \in \mathbb{Z}^+$, we may study $\mathrm{P}(k, R)$ by restricting to sequences in $\mathcal{P}(R)$ of degree k.*

2.2. Criteria for Null and Periodic Sequences

In this section we explore the notion of the set of all linearly recurring sequences being expressed as the *ring* internal direct sum of the sets of all null and periodic sequences. In particular, we will show that for any given characteristic polynomial $f(x) \in R[x]$, $\mathcal{A}(f(x)) = \mathcal{P}(f(x)) + \mathcal{N}(f(x))$, where $\mathcal{P}(f(x))$ and $\mathcal{N}(f(x))$ are ideals in $\mathcal{A}(f(x))$, for an appropriately chosen multiplicative operation.

The results in this section can be found in [2], although the notation we use here differs significantly from that used by M. Ward, in favor of the notation used in [1].

Definition 2.21. Let $\mathbf{s}$ be a sequence over a ring R. Then the associated generating function $S(x) \in R[[x]]$ of $\mathbf{s}$ is given by:

$$S(x) := s_0 + s_1x + s_2x^2 + \ldots + s_ix^i + \ldots = \sum_{i=0}^{\infty} s_ix^i \tag{5}$$

Additionally, for $r \in \mathbb{Z}^+$, we associate to $\mathbf{s}$ the truncated generating function $S_r(x) \in R[x]$ of $\mathbf{s}$ given by:

$$S_r(x) := s_0 + s_1x + s_2x^2 + \ldots + s_{r-1}x^{r-1} \tag{6}$$

Note that it is possible for $s_{r-1} = 0$, and so $\deg(S_r(x)) \leq r-1$. Set $c := r - 1 - \deg(S_r(x))$. Applying our definition of the reciprocal polynomial from Section 1.3, we thus have the following derivation for the reciprocal of $S_r(x)$:

$$x^c S_r^*(x) := x^{n-1} S_r\left(\frac{1}{x}\right) = s_0 x^{n-1} + s_1 x^{n-2} + \ldots s_{n-2}x + s_{n-1}. \tag{7}$$

Definition 2.22. Let $S(x) := \sum_{i=0}^{\infty} s_i x^i$ be the generating function of a sequence satisfying a linear recurrence relation of degree k with characteristic polynomial $f(x)$ given by Equation 4. We define $S_f^{(n)}(x) := -\sum_{j=0}^{k-1}\left(\sum_{i=j+1}^{k} a_i s_{n-(j+1)+i}\right) x^j$, for integers $n \geq 0$.

When operating on generating functions and characteristic polynomials, as with the proof of the Lemma 3.11, it is oftentimes useful to express the linear recurrence relation of Equation 1 in the following manner:

Lemma 2.23. *Let* $\mathbf{s} := (s_i)_{i\geq 0}$ *be a sequence.* $\mathbf{s}$ *satisfies Equation 1 if and only if for all integers* $i \geq 0$, $\sum_{j=0}^{k} a_j s_{i+j} = 0$, *where we set* $a_k := -1$.

We are now finally ready to prove the following lemma:

Lemma 2.24. *Let* $\mathbf{s}$ *be a sequence that satisfies a linear recurrence relation of degree* k *with characteristic polynomial* $f(x)$ *over a commutative ring* R, *and let* $S(x) \in R[[x]]$ *be the generating function of* $\mathbf{s}$. *Then for every integer* $n \geq k$,

$$f(x)x^c S_n^*(x) = x^n S_f^{(0)}(x) - S_f^{(n)}(x). \tag{8}$$

where $c := n - 1 - \deg(S_n(x))$.

Proof. Let $f(x)$ be given by Equation 4. Let $n > k$ be an integer. By the definitions of $f(x)$ and $S_n^*(x)$, and setting the coefficient $a_k := -1$, we then have:

$$f(x)x^c S_n^*(x) = -\left(\sum_{i=0}^{k} a_i x^i\right)\left(\sum_{t=0}^{n-1} s_{n-1-t}x^t\right) = -\left[\sum_{j=0}^{n+k-1}\left(\sum_{i+t=j} a_i s_{n-1-t}\right)x^j\right].$$

For all integers $j \geq 0$, we have

$$\sum_{i+t=j} a_i s_{n-1-t} = \sum_{i=0}^{j} a_i s_{n-1-(j-i)} = \sum_{i=0}^{j} a_i s_{n-1-j+i}$$

where $a_i = 0$ for all $i > k$ and $s_l = 0$ for all $l < 0$. In particular, the coefficient of x^j is 0 once $j > n+k-1$. For $0 \leq j \leq n+k-1$, we consider several cases as follows:

- If $0 \leq j \leq k-1$, then

$$\sum_{i+t=j} a_i s_{n-1-t} = \sum_{i=0}^{j} a_i s_{n-1-j+i}.$$

  Now by Lemma 2.23, we have $\sum_{i=0}^{k} a_i s_{n-1-j+i} = 0$, so that

$$\begin{aligned}\sum_{i+t=j} a_i s_{n-1-t} &= \sum_{i=0}^{j} a_i s_{n-1-j+i} - 0 = \sum_{i=0}^{j} a_i s_{n-1-j+i} - \sum_{i=0}^{k} a_i s_{n-1-j+i} \\ &= -\sum_{i=j+1}^{k} a_i s_{n-1-j+i} = -\sum_{i=j+1}^{k} a_i s_{n-(j+1)+i}.\end{aligned}$$

- If $k \leq j \leq n-1$, then

$$\sum_{i+t=j} a_i s_{n-1-t} = \sum_{i=0}^{j} a_i s_{n-1-j+i} = \sum_{i=0}^{k} a_i s_{n-1-j+i} = 0$$

  by Lemma 2.23. This case only arises if $n > k$.

- If $n \leq j \leq n+k-1$, then

$$\sum_{i+t=j} a_i s_{n-1-t} = \sum_{i=0}^{j} a_i s_{n-1-j+i} = \sum_{i=j-n+1}^{k} a_i s_{n-1-j+i}.$$

  We want to switch indices so that the summation terms match with the first case. To do this, we substitute $j = l + n$, where $0 \leq l \leq k-1$, and observe that

$$\begin{aligned}\sum_{i+t=j} a_i s_{n-1-t} &= \sum_{i=(l+n)-n+1}^{k} a_i s_{n-1-(l+n)+i} = \sum_{i=l+1}^{k} a_i s_{-1-l+i} \\ &= \sum_{i=l+1}^{k} a_i s_{0-(l+1)+i}\end{aligned}$$

Putting together the terms for all three cases, we thus have:

$$\begin{aligned}
&f(x)x^c S_n^*(x) \\
&= -\left[\sum_{j=0}^{k-1}\left(-\sum_{i=j+1}^{k} a_i s_{n-(j+1)+i}\right)x^j + \sum_{j=k}^{n-1} 0\cdot x^j + \sum_{j=n}^{n+k-1}\left(\sum_{i=j-n+1}^{k} a_i s_{n-1-j+1}\right)x^j\right] \\
&= -\left[\sum_{j=0}^{k-1}\left(-\sum_{i=j+1}^{k} a_i s_{n-(j+1)+i}\right)x^j + 0 + \sum_{l=0}^{k-1}\left(\sum_{i=l+1}^{k} a_i s_{0-(l+1)+i}\right)x^{l+n}\right] \\
&= -\left[-\sum_{j=0}^{k-1}\left(\sum_{i=j+1}^{k} a_i s_{n-(j+1)+i}\right)x^j\right] + x^n\cdot\left[-\sum_{l=0}^{k-1}\left(\sum_{i=l+1}^{k} a_i s_{0-(l+1)+i}\right)x^l\right] \\
&= -S_f^{(n)}(x) + x^n S_f^{(0)}(x) = x^n S_f^{(0)}(x) - S_f^{(n)}(x).
\end{aligned}$$

□

Comparing Equation 8 above to Equation 13 in Chapter 3, we shall see that Lemma 2.24 for commutative rings generalizes Lemma 3.12 for finite fields. The following proposition will further show that the statement in Lemma 3.12 can likewise be more broadly applied to integral domains, and is biconditional for suitably large periods of the given sequence.

Proposition 2.25. *Let $S(x)$ be the generating function of a sequence $\mathbf{s}$ satisfying a linear recurrence relation of degree k with characteristic polynomial $f(x)$ over a commutative ring R. Then for any integer $n > k$, the following hold:*

1. *$f(x)|(x^n - 1)S_f^{(0)}(x)$ if and only if $\mathbf{s}$ is (purely) periodic with n as a period.*
2. *$f(x)|x^n S_f^{(0)}(x)$ if and only if $\mathbf{s}$ is a null sequence with $\eta(\mathbf{s}) \le n$.*

Proof. If $\mathbf{s}$ is periodic with period $n > k$, then $s_i = s_{i+n}$ for all integers $i \ge 0$. It follows that $S_f^{(n)}(x) := -\sum_{j=0}^{k-1}\left(\sum_{i=j+1}^{k} a_i s_{n-(j+1)+i}\right)x^j = -\sum_{j=0}^{k-1}\left(\sum_{i=j+1}^{k} a_i s_{0-(j+1)+i}\right)x^j = S_f^{(0)}(x)$, and so by Lemma 2.24, we have

$$\begin{aligned}
f(x)x^c S_n^*(x) &= x^n S_f^{(0)}(x) - S_f^{(n)}(x) = x^n S_f^{(0)}(x) - S_f^{(0)}(x) \\
&= (x^n - 1)S_f^{(0)}(x)
\end{aligned}$$

so that $f(x)|(x^n - 1)S_f^{(0)}(x)$.

Conversely, if $f(x)|(x^n-1)S_f^{(0)}(x)$, then $f(x)|x^nS_f^{(0)}(x)-S_f^{(0)}(x)$. Rearranging Equation 8, we have $x^nS_f^{(0)}(x)=f(x)x^cS_n^*(x)+S_f^{(n)}(x)$, so that $f(x)|f(x)x^cS_n^*(x)+S_f^{(n)}(x)-S_f^{(0)}(x)$. Hence, $f(x)|S_f^{(n)}(x)-S_f^{(0)}(x)$. Since $S_f^{(n)}(x)$ and $S_f^{(0)}(x)$ both have degree less than $k=\deg(f(x))$ by definition, and since $f(x)$ is monic (i.e. its leading coefficient is unity), it follows that $S_f^{(n)}(x)=S_f^{(0)}(x)$. By comparing the terms of both sides of the equality from the highest power of x down, we see that since $a_k=-1$ is a unit by definition, for all integers $0\le i\le k-1$, we have $s_i=s_{i+n}$. Thus, by Lemma 2.3, $\mathbf{s}$ is periodic with period n.

If $\mathbf{s}$ is a null sequence with $\eta(\mathbf{s})\le n$, then it immediately follows that $S_f^{(n)}(x)=0$, and so Equation 8 reduces to $f(x)x^cS_n^*(x)=x^nS_f^{(0)}(x)$, with $f(x)|x^nS_f^{(0)}(x)$, as desired. Conversely, if $f(x)|x^nS_f^{(0)}(x)$, then since $x^nS_f^{(0)}(x)=f(x)x^cS_n^*(x)+S_f^{(n)}(x)$, it follows that $f(x)|S_f^{(n)}(x)$. Since $\deg(S_f^{(n)}(x))<k=\deg(f(x))$ and that again $f(x)$ is monic, we see that $S_f^{(n)}(x)=0$. Thus, the coefficient of every term of $S_f^{(n)}(x)$ must vanish. Since $a_k=-1$ is a unit, we have that $s_{n+i}=0$ for all integers $0\le i\le k-1$. Thus, by Lemma 2.3, $\mathbf{s}$ is a null sequence with $\eta(\mathbf{s})\le n$. □

We see from Proposition 2.25 that for any sequence $\mathbf{s}$ satisfying a linear recurrence relation of degree k over a commutative ring, if $\rho(\mathbf{s})\ge k$, then $\rho(\mathbf{s})$ is the least $n\in\mathbb{Z}^+$ such that item 1 of Proposition 2.25 holds. Such n will always exist for when $f(0)$ is a unit, as will be shown in Lemma 2.26 below.

Lemma 2.26. *Let $f(x)\in R[x]$, where R is a finite commutative ring. Suppose that $\deg(f(x))\ge 1$ and that both $f(0)$ and $f^*(0)$ are units. Then there exists $e\in\mathbb{Z}^+$ such that $f(x)|(x^e-1)$.*

Proof. Let $k:=\deg(f(x))$ and let $q:=|R|$. Since the leading coefficient of $f(x)$ is a unit, the quotient ring $R[x]\big/\langle f(x)\rangle$ has at most q^k distinct residue classes, by Lemma 1.16. Consider then the residue classes $x^j+\langle f(x)\rangle$, for $j=0,1,\ldots,q^k$. Therefore, by the pigeonhole principle, there exist integers r and s with $0\le r<s\le q^k$ such that $x^s+\langle f(x)\rangle=x^r+\langle f(x)\rangle$. This implies $x^s-x^r=x^r(x^e-1)\in\langle f(x)\rangle$, where $e:=s-r$. Since $f(0)$ is a unit, $x+\langle f(x)\rangle$ is a unit in $R[x]\big/\langle f(x)\rangle$. It follows that $x^e-1\in\langle f(x)\rangle$. Hence, $f(x)|x^e-1$. □

We shall see in the following section that the condition of $\rho(\mathbf{s})\ge k$ always holds for the impulse response sequence when $f(0)$ is a unit, and that the least period of the impulse response is an upper bound for all least periods of sequences satisfying a given recurrence relation. Hence, we will always at the very least be able to determine the upper bound of least periods for $f(x)$ when $f(0)$ is a unit, which we will later call the "principal period" of $f(x)$.

Definition 2.27. Let R be a commutative ring, and let $f(x) \in R[x]$ be monic. We define $\psi_f : \mathcal{A}(f(x)) \to R[x] \big/ \langle f(x) \rangle$ by $\psi_f(\mathbf{s}) = S_f^{(0)}(x) + \langle f(x) \rangle$, where $S_f^{(0)}(x)$ is as defined in Definition 2.22.

Proposition 2.28. *Let R be a finite commutative ring, and let $f(x) \in R[x]$ be monic. Then the map $\psi_f : \mathcal{A}(f(x)) \to R[x] \big/ \langle f(x) \rangle$ is a bijection. Furthermore, it preserves the additive group structure and so is a group isomorphism.*

Proof. For any $\mathbf{s} \in \mathcal{A}(f(x))$, $\mathbf{s}$ is completely determined by its initial state vector, with k terms. Sequences in $\mathcal{A}(f(x))$ having distinct initial state vectors are also clearly distinct. Therefore, for $q := |R|$, there exist q^k possible distinct initial state vectors, so that $|\mathcal{A}(f(x))| = q^k$. On the other hand, since $f(x)$ is monic (so that its leading coefficient is 1), we have by Lemma 1.16 that $R[x] \big/ \langle f(x) \rangle$ has exactly q^k elements. Thus, we can prove that ψ_f is bijective by showing that every element in the codomain has a unique preimage.

Let $L(x) := \sum_{i=0}^{k-1} l_i x^i \in R[x] \big/ \langle f(x) \rangle$. We claim that we can construct a unique sequence $\mathbf{s}$ for which $\psi_f(\mathbf{s}) = S_f^{(0)}(x) = L(x)$. Such a sequence would have to satisfy the following array of equations, using the definition of $S_f^{(0)}(x)$.

$$\begin{aligned}
-a_k s_0 &= l_{k-1} \\
-(a_{k-1} s_0 + a_k s_1) &= l_{k-2} \\
\vdots &= \vdots \\
-\sum_{i=j+1}^{k} a_i s_{i-(j+1)} &= l_j \\
\vdots &= \vdots \\
-\sum_{i=1}^{k} a_i s_{i-1} &= l_0
\end{aligned}$$

Since $a_k = -1$ is a unit, we uniquely determine $s_0 = l_{k-1}$ from the first line. Subsequently, we also uniquely determine $s_1 = l_{k-2} + a_{k-1} s_0 = l_{k-2} - a_{k-1} l_{k-1}$. We then obtain the following s_i's in a similar fashion, so that there exists a uniquely determined sequence $\mathbf{s}$ generated by the initial state vector $\mathbf{s}_0$ and the linear recurrence with characteristic polynomial $f(x)$ such that $\psi_f(\mathbf{s}) = L(x)$. Thus, ψ_f is bijective.

Finally, since R is a commutative ring, it is straightforward to check the group homomorphism property: for any $\mathbf{s}, \mathbf{t} \in \mathcal{A}(f(x))$, $\psi_f(\mathbf{s}) + \psi_f(\mathbf{t}) = \psi_f(\mathbf{s} + \mathbf{t})$. Therefore, ψ_f is a group isomorphism under addition.

□

Remark 2.29. *We may then define multiplication in $\mathcal{A}(f(x))$ such that for $\mathbf{s}, \mathbf{t} \in \mathcal{A}(f(x))$, we have $\mathbf{s} \cdot \mathbf{t} = \psi_f^{-1}(\psi_f(\mathbf{s}) \cdot \psi_f(\mathbf{t}))$. In this way, ψ_f can be viewed as a ring isomorphism.*

We are now in a position to extend the result of Proposition 2.13 and show that $\mathcal{A}(f(x))$ decomposes into the internal direct sum of its ideals of purely periodic and null sequences.

Proposition 2.30. *Let R be a finite commutative ring, and let $f(x) \in R[x]$ be the characteristic polynomial of a linear recurrence relation over R. Then for an appropriate definition of multiplication (as in Remark 2.29), the ring $\mathcal{A}(f(x))$ has the internal direct sum decomposition $\mathcal{A}(f(x)) = \mathcal{P}(f(x)) \oplus \mathcal{N}(f(x))$, where $\mathcal{P}(f(x))$ and $\mathcal{N}(f(x))$ are ideals in $\mathcal{A}(f(x))$.*

Proof. We already know from Proposition 2.13 that $\mathcal{A}(f(x))$ has the group internal direct sum decomposition $\mathcal{A}(f(x)) = \mathcal{P}(f(x)) \oplus \mathcal{N}(f(x))$. We have left to check that $\mathcal{P}(f(x))$ and $\mathcal{N}(f(x))$ are indeed ideals in $\mathcal{A}(f(x))$, with multiplication defined as in Remark 2.29. We do this by applying the ideal test on the their images over the ring isomorphism map ψ_f.

Let $\mathbf{s}, \mathbf{t} \in \mathcal{P}(f(x))$ and let $\mathbf{u} \in \mathcal{A}(f(x))$. Note that since $\mathcal{P}(f(x))$ is a subgroup of $\mathcal{A}(f(x))$, we immediately have $\mathbf{s} - \mathbf{t} \in \mathcal{P}(f(x))$. Now choose $n \in \mathbb{Z}^+$ such that $n > k$ and n is a multiple of $\rho(\mathbf{s})$. Then n is a period of $\mathbf{s}$, and is sufficiently large so that, by Proposition 2.25, we have that $f(x) | (x^n - 1)\psi_f(\mathbf{s})$. Thus, $f(x)$ divides $(x^n - 1)\psi_f(\mathbf{s})\psi_f(\mathbf{u}) = (x^n - 1)\psi_f(\mathbf{s} \cdot \mathbf{u})$, and so $\mathbf{s} \cdot \mathbf{u} \in \mathcal{P}(f(x))$. Therefore, $\mathcal{P}(f(x))$ is an ideal in $\mathcal{A}(f(x))$.

Similarly, let $\mathbf{s}, \mathbf{t} \in \mathcal{N}(f(x))$ and let $\mathbf{u} \in \mathcal{A}(f(x))$. Note that since $\mathcal{N}(f(x))$ is a subgroup of $\mathcal{A}(f(x))$, we immediately have $\mathbf{s} - \mathbf{t} \in \mathcal{N}(f(x))$. Now choose $n \in \mathbb{Z}^+$ such that $n > \max(k, \eta(\mathbf{s}))$. Then by Proposition 2.25, we have that $f(x) | x^n \psi_f(\mathbf{s})$. Thus, $f(x)$ divides $x^n \psi_f(\mathbf{s})\psi_f(\mathbf{u}) = x^n \psi_f(\mathbf{s} \cdot \mathbf{u})$, and so $\mathbf{s} \cdot \mathbf{u} \in \mathcal{N}(f(x))$. Therefore, $\mathcal{N}(f(x))$ is an ideal in $\mathcal{A}(f(x))$.

Thus, $\mathcal{A}(f(x))$ has the ring internal direct sum decomposition

$$\mathcal{A}(f(x)) = \mathcal{P}(f(x)) \oplus \mathcal{N}(f(x)).$$

□

2.3. The Companion Matrix

In this section, we will introduce what is called a "companion matrix" of a given linear recurrence relation. We saw in the beginning of the chapter (Lemma 2.2) that state vectors play an important role describing the periodicity of a linearly recurring sequence. Just as the linear recurrence determines the next element of a sequence, the companion matrix determines the next state vector (see Lemma 2.32). It is through the companion matrix that we will formulate methods for determining the least period of a given sequence.

The results in this section can be found in [1], although here we again use slightly different notation. We also usually write proofs for these statements in ways that differ from the source material, so as to keep the thesis as self contained as possible.

Definition 2.31. Consider a linear recurrence relation over a ring R with a characteristic polynomial $f(x)$ as in Equation 4. We define the *companion matrix* A of $f(x)$ as

$$A := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{k-1} \end{pmatrix} \in M_k(R) \tag{9}$$

Going forward, we will use both row and column notations for state vectors (Definition 2.1) in different contexts depending on which is most convenient.

Lemma 2.32. *Let* $\mathbf{s}$ *be a linearly recurring sequence satisfying a recurrence relation of degree* k *over a ring* R *with companion matrix* A*. Then for every integer* $i \geq 0$*,* $\mathbf{s}_i = A^i\mathbf{s}_0$*.*

Proof. Let the linear recurrence relation and its companion matrix A be given by Equations 1 and 9 respectively. One can then check that for each $i \geq 0$, $\mathbf{s}_{i+1} = A\mathbf{s}_i$.

Hence, by induction, we have that for each $i \geq 0$, $s_i = A^i s_0$.

□

Proposition 2.33. *Let A be the companion matrix of a linear recurrence relation of degree k over a finite commutative ring R. If A is given by Equation 9 with a_0 a unit, then $A \in GL_k(R)$. Furthermore, for every sequence $\mathbf{s}$ satisfying the linear recurrence, we have that $\mathbf{s}$ is periodic with $\rho(\mathbf{s})|ord(A)$.*

Proof. Since a_0 is a unit, we have that $\det(A) = (-1)^{k-1}a_0$ is a unit, which implies that $A \in GL_k(R)$. Now let $n := \text{ord}(A)$, so that $A^n = I$, where $I \in GL_k(R)$ is the identity matrix. Let $\mathbf{s}$ be a sequence in R that satisfies the linear recurrence relation, given by Equation 1. Then from Lemma 2.32, we have that for every integer $i \geq 0$, $\mathbf{s}_i = A^i \mathbf{s}_0$. Thus, for every integer $i \geq 0$:

$$\mathbf{s}_{i+n} = A^{i+n}\mathbf{s}_0 = A^i A^n \mathbf{s}_0 = A^i I \mathbf{s}_0 = A^i \mathbf{s}_0 = \mathbf{s}_i.$$

Hence, $\mathbf{s}$ is periodic with period n. Therefore, by Lemma 1.1, $\rho(\mathbf{s})|\text{ord}(A)$.

□

Definition 2.34. For a fixed $k \in \mathbb{Z}^+$, let $\mathbf{0}$ denote the zero vector of length k, and let $[0]$ denote the $k \times k$ zero matrix. For $1 \leq i \leq k$, let $\mathbf{e}_i := (e_1, e_2, \ldots, e_k)$ be the ith standard basis vector, with $e_j = 1$ for $j = i$ and $e_j = 0$ for every $j \neq i$.

Note that the space R^k of all tuples of k elements in a ring R is naturally equipped with operations of component-wise addition and scalar multiplication. If R is a field, then R^k is a vector space over R. More generally, R^k is an example of an *R-module*. An R-module is a closed set of objects, sometimes called vectors, with operations of addition and scalar multiplication over R. Modules are more complicated to deal with than vector spaces since, for example, they do not necessarily have a well-defined dimensionality, i.e. they may have vectors that form a spanning set, but do not necessarily possess a basis. If an R-module *does* possess a basis, then we call it *free*. Such is the case for the direct sum R^k, having the natural basis $\{\mathbf{e}_i \mid i = 1, 2, \ldots, k\}$. We will use this fact in the following lemma to prove that substituting the companion matrix of a linear recurrence relation into its associated characteristic polynomial (in the form of scalar and matrix multiplication) always yields the zero matrix.

Lemma 2.35. *Let $f(x)$ and A be the associated characteristic polynomial and companion matrix, respectively, of a linear recurrence relation of degree k over an integral domain R. Then $f(A) = [0]$.*

This is a consequence of the Cayley-Hamilton Theorem, which states that the equation holds for square matrices over a general commutative ring, but we will give a self-contained proof here.

Proof. Let $f(x)$ and A be given by Equations 4 and 9 respectively. Let $\mathbf{s}$ be a sequence that satisfies Equation 1 over R with an arbitrary initial state vector $\mathbf{s}_0 = (s_0, s_1, \ldots, s_{k-1})$. Then for every integer $i \geq 0$, we have:

$$a_0 s_i + a_1 s_{i+1} + \ldots + a_{k-1} s_{i+k-1} = s_{i+k}$$

Thus, it follows that:

$$a_0 \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{k-1} \end{pmatrix} + a_1 \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_k \end{pmatrix} + \ldots + a_{k-1} \begin{pmatrix} s_{k-1} \\ s_k \\ \vdots \\ s_{2k-2} \end{pmatrix} = \begin{pmatrix} s_k \\ s_{k+1} \\ \vdots \\ s_{2k-1} \end{pmatrix}$$

$$a_0 \mathbf{s}_0 + a_1 \mathbf{s}_1 + \ldots + a_{k-1} \mathbf{s}_{k-1} = \mathbf{s}_k$$

Then by Lemma 2.32, we have that:

$$a_0 A^0 \mathbf{s}_0 + a_1 A^1 \mathbf{s}_0 + \ldots + a_{k-1} A^{k-1} \mathbf{s}_0 = A^k \mathbf{s}_0$$

Reorganizing the terms, we then have:

$$\begin{aligned} \mathbf{0} &= A^k \mathbf{s}_0 - a_{k-1} A^{k-1} \mathbf{s}_0 - a_{k-2} A^{k-2} \mathbf{s}_0 - \ldots - a_0 I \mathbf{s}_0 \\ &= [A^k - a_{k-1} A^{k-1} - a_{k-2} A^{k-2} - \ldots - a_0 I] \mathbf{s}_0 \\ &= f(A) \mathbf{s}_0 \end{aligned}$$

where $f(A) = A^k - a_{k-1} A^{k-1} - a_{k-2} A^{k-2} - \ldots - a_0 I \in M_k(R)$. Now observe that for every integer $1 \leq j \leq k$, $f(A)\mathbf{e}_j = \mathbf{0}$ denotes the jth column of $f(A)$. Hence, $f(A) = [0]$. □

We now have all the tools necessary to determine the maximum possible least period of all sequences that satisfy a given linear recurrence relation, which we will henceforth refer to as the "principal period" associated to the linear recurrence.

Definition 2.36. Let $f(x) \in R[x]$ be the characteristic polynomial of a linear recurrence relation over a finite ring R. Then we define the *principal period* $\rho(f(x))$ of $f(x)$ by $\rho(f(x)) := \max(\rho(\mathbf{s}) \mid \mathbf{s} \in \mathcal{A}(f(x)))$. We will also extend this notation and let $\rho(k, R)$ denote the maximum of the least periods of all linearly recurring sequences of degree k over R.

We shall see in Proposition 2.40 that over finite commutative rings, the principal period of a linear recurrence is always guaranteed to arise from a special kind of sequence, called the 'impulse response sequence.'

Definition 2.37. A sequence $\mathbf{s}$ satisfying a linear recurrence relation of degree k is called the *impulse response sequence* if $\mathbf{s}_0 = \mathbf{e}_k$.

Lemma 2.38. *Let* $\mathbf{s}$ *be the impulse response sequence satisfying a linear recurrence relation of degree* k *over a finite commutative ring* R *. Then* $\{\mathbf{s}_i \mid i = 0, 1, \ldots, k-1\}$ *forms a basis in* R^k*.*

Proof. We consider the following matrix M:

$$M = (\mathbf{s}_{k-1} \mid \mathbf{s}_{k-2} \mid \cdots \mid \mathbf{s}_0) = \begin{pmatrix} s_{k-1} & s_{k-2} & \cdots & s_0 \\ s_k & s_{k-1} & \cdots & s_1 \\ \vdots & \vdots & & \vdots \\ s_{2k-2} & s_{2k-3} & \cdots & s_{k-1} \end{pmatrix}$$

Note that for $0 \leq i < k-1$, $s_i = 0$, and that $s_{k-1} = 1$. Therefore, we have:

$$M = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ s_k & 1 & \cdots & 0 & 0 \\ s_{k+1} & s_k & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ s_{2k-3} & s_{2k-4} & \cdots & 1 & 0 \\ s_{2k-2} & s_{2k-3} & \cdots & s_k & 1 \end{pmatrix}$$

Observe that the columns of M span and form a linearly independent set in R^k. That is, $\{\mathbf{s}_i \mid i = 0, 1, \ldots, k-1\}$ forms a basis for R^k.

□

Lemma 2.39. *Let* $\mathbf{s}$ *be the impulse response sequence satisfying a linear recurrence relation over a commutative ring* R *with companion matrix* A*. Then for any integers* $i, j \geq 0$, $\mathbf{s}_i = \mathbf{s}_j$ *if and only if* $A^i = A^j$*.*

Proof. It follows immediately from Lemma 2.32 that $A^i = A^j$ implies $\mathbf{s}_i = \mathbf{s}_j$. Conversely, suppose that $\mathbf{s}_i = \mathbf{s}_j$. Then by Lemma 2.5, $\mathbf{s}_{i+t} = \mathbf{s}_{j+t}$ for every integer $t \geq 0$. By Lemma 2.32, we then get $A^i\mathbf{s}_t = A^j\mathbf{s}_t$ for every integer $t \geq 0$. Since $\{\mathbf{s}_i \mid i = 0, 1, \ldots, k-1\}$ forms a basis for R^k (via Lemma 2.38), we deduce that for any vector $\mathbf{v} \in R^k$, $A^i\mathbf{v} = A^j\mathbf{v}$. It follows that, by substituting the standard basis vectors for $\mathbf{v}$, every column in A^i matches with the corresponding column in A^j. Hence, $A^i = A^j$.

□

Proposition 2.40. *Let* $\mathbf{s}$ *and* $\mathbf{t}$ *be sequences satisfying the same linear recurrence relation over a finite commutative ring* R *such that* $\mathbf{s}$ *is the impulse response sequence. Then* $\rho(\mathbf{t})|\rho(\mathbf{s})$*.*

Proof. For every integer $i \geq \eta(\mathbf{s})$, $\mathbf{s}_i = \mathbf{s}_{i+\rho(\mathbf{s})}$. Thus, by Lemma 2.39, $A^i = A^{i+\rho(\mathbf{s})}$ for every integer $i \geq \eta(\mathbf{s})$. By Lemma 2.32, we then have $\mathbf{t}_i = A^i\mathbf{t}_0 = A^{i+\rho(\mathbf{s})}\mathbf{t}_0 = \mathbf{t}_{i+\rho(\mathbf{s})}$. Hence, $\rho(\mathbf{s})$ is a period of $\mathbf{t}$, and by Lemma 1.1, $\rho(\mathbf{t})|\rho(\mathbf{s})$. □

We then immediately obtain the following corollary:

Corollary 2.41. *Let* $f(x) \in R[x]$ *be the characteristic polynomial of a linear recurrence relation over a finite commutative ring* R*. If* $\mathbf{s} \in \mathcal{A}(f(x))$ *is the impulse response sequence, then* $\rho(f(x)) = \rho(\mathbf{s})$*.*

The next result relates the period of the impulse response sequence and the order of the companion matrix A when A is invertible.

Proposition 2.42. *Let* $\mathbf{s}$ *be the impulse response sequence satisfying a linear recurrence relation over a finite commutative ring* R *with characteristic polynomial* $f(x)$ *and companion matrix* A *such that* $f(0) := a_0$ *is a unit. Then* $\rho(\mathbf{s}) = ord(A)$

Proof. First recall that by Proposition 2.33, A is invertible and hence $\mathrm{ord}(A)$ is well defined. Now for every integer $i \geq 0$, $A^i = A^iI = A^iA^{\mathrm{ord}(A)} = A^{i+\mathrm{ord}(A)}$. By Lemma 2.39, it follows that $\mathbf{s}_i = \mathbf{s}_{i+\mathrm{ord}(A)}$. Hence, $\rho(\mathbf{s})|\mathrm{ord}(A)$ by Lemma 1.1. On the other hand, since a_0 is a unit, we see that $\mathbf{s}$ is purely periodic by Lemma 2.4. Hence, $\mathbf{s}_0 = \mathbf{s}_{\rho(\mathbf{s})}$, and so by Lemma 2.39, we deduce that $A^0 = I = A^{\rho(\mathbf{s})}$. Thus, $\mathrm{ord}(A)|\rho(\mathbf{s})$, which implies $\mathrm{ord}(A) = \rho(\mathbf{s})$. □

The following lemma gives us a lower limit on the least period of the impulse response sequence for a given linear recurrence relation. It will become useful in

Chapter 4 when we analyze the principal period of a linear recurrence over a quotient ring of a principal ideal domain.

Lemma 2.43. *Let* $\mathbf{s}$ *be the impulse response sequence satisfying a linear recurrence relation over a finite commutative ring* R *with characteristic polynomial* $f(x)$ *such that* $f(0) := a_0$ *is a unit. Then* $\rho(\mathbf{s}) \geq k$*.*

Proof. Let $f(x)$ and A be the associated characteristic polynomial and companion matrix, respectively, of the linear recurrence. Now suppose, by way of contradiction, that $\rho(\mathbf{s}) < k$, so that there exists $j \in \mathbb{Z}^+$ such that $j < k$ and $\mathbf{s}_i = \mathbf{s}_{i+j}$ for all sufficiently large integers i. Then by Lemma 2.39, $A^i = A^{i+j} = A^i A^j$, so that $I = A^j$, since A is invertible via Proposition 2.33. This implies that $\mathbf{s}_0 = A^j \mathbf{s}_0 = \mathbf{s}_j$. But by Lemma 2.38, we know that $\{A^i \mathbf{s}_0 = \mathbf{s}_i \mid i = 0, 1, \ldots, j, \ldots k-1\}$ forms a pairwise distinct set of vectors, and so $\mathbf{s}_0 \neq \mathbf{s}_j$, a contradiction. Thus, $\rho(\mathbf{s}) \geq k$. □

Recalling our results in the previous section, we therefore arrive at the following proposition:

Proposition 2.44. *Let* $f(x)$ *be the characteristic polynomial of a recurrence relation over a finite commutative ring, with* $f(0)$ *a unit. Then the principal period* $\rho(f(x))$ *is the least* $n \in \mathbb{Z}^+$ *such that* $f(x) | x^n - 1$*.*

Proof. Let $\mathbf{s} \in \mathcal{A}(f(x))$ be the impulse response sequence. Then $\rho(f(x)) = \rho(\mathbf{s})$ by Corollary 2.41. Let $n = \rho(\mathbf{s})$ and $k = \deg(f(x))$. By Lemma 2.43, we have $n \geq k$ and since $\mathbf{s}_0 = \mathbf{e}_k$ we have $S_f^{(0)}(x) = 1$. Then bt Proposition 2.25(1), we have $f(x) | (x^n - 1)(1) = x^n - 1$.

On the other hand, if $f(x) | x^n - 1$ for some $n \in \mathbb{Z}^+$ then $n \geq \deg(f(x)) = k$ since $f(x)$ is monic. By Proposition 2.25(1), we see that such an n is a period of $\mathbf{s}$ and so $n \geq \rho(\mathbf{s})$. Thus, $\rho(\mathbf{s})$ is the smallest n such that $f(x) | x^n - 1$. □

CHAPTER 3. SEQUENCES OVER FINITE FIELDS

In this chapter, we will be working with $R := \mathbb{F}_q$, and attempt to determine the set of all least periods of sequences satisfying linear recurrence relations of a given degree k. As we shall see in Theorem 3.10 (Section 3.2), there exists a close relationship between the least period of a sequence and the order of the characteristic polynomial of a linear recurrence which it satisfies. We will introduce the notion of the order of a polynomial and describe some of its properties in Section 3.1 below.

Now recall from Proposition 2.8 that a linearly recurring sequence in fact satisfies an infinite set of linear recurrences. Thus, the least period of the sequence is related to the orders of the characteristic polynomials associated to all of these recurrences. The order of one such polynomial, which we will later refer to as the minimal polynomial, exactly determines the least period of the sequence. Section 3.3 will be devoted to identifying the minimal polynomial. In Section 3.4, we will then apply the results of the previous section on the order of the minimal polynomial, and finally arrive at our goal of identifying the set of least periods that arise from families of linear recurrences of degree k.

Much of the results in Sections 3.1, 3.2 and 3.3 can be found in [1] Chapters 3 and 8.

3.1. Orders of Polynomials

Before defining the order of a particular polynomial $f(x)$, we need the following lemma.

Lemma 3.1. *Let $f(x) \in \mathbb{F}_q[x]$, and suppose that $\deg(f(x)) \geq 1$ with $f(0) \neq 0$. Then there exists $e \in \mathbb{Z}^+$ such that $f(x)|(x^e - 1)$.*

Proof. This follows from Lemma 2.26.

□

Definition 3.2. Let $f(x) \in \mathbb{F}_q[x]$ with $\deg(f(x)) \geq 1$. If $f(0) \neq 0$, then we define $\operatorname{ord}(f(x)) := \min\{e \mid f(x)|(x^e - 1)\}$. If $f(0) = 0$, then $f(x) = x^h g(x)$, where $h \in \mathbb{Z}^+$ and $g(x) \in \mathbb{F}_q[x]$ such that $g(0) \neq 0$. We subsequently define $\operatorname{ord}(f(x)) := \operatorname{ord}(g(x))$. Finally, if $f(x)$ is a constant function, then we set $\operatorname{ord}(f(x)) = 1$.

Lemma 3.3. *Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree k. If $f(0) \neq 0$, then ord$(f(x))$ = ord(α), where α is a root of $f(x)$ and an element of the multiplicative group $\mathbb{F}_{q^k}^*$. Consequently, for any irreducible polynomial $f(x)$ of degree k,* *ord*$(f(x))|q^k - 1$.

Proof. Set $e := \text{ord}(f(x))$. If $f(x) = x$, then $e = 1$, which divides $q^k - 1$.

Now suppose that $f(0) \neq 0$. Since $f(x)$ is irreducible in $\mathbb{F}_q[x]$, for any root α of $f(x)$, $\mathbb{F}_q(\alpha) \cong \mathbb{F}_q[x] \big/ \langle f(x) \rangle$, with $\mathbb{F}_q(\alpha) \cong \mathbb{F}_{q^k}$. Since $f(\alpha) = 0$ and $f(x) + \langle f(x) \rangle = 0 + \langle f(x) \rangle$, we see that α corresponds to the coset $x + \langle f(x) \rangle$ in the isomorphism $\mathbb{F}_{q^k} \cong \mathbb{F}_q[x] \big/ \langle f(x) \rangle$. We then observe that $f(x)|x^e - 1$ if and only if $(x + \langle f(x) \rangle)^e - (1 + \langle f(x) \rangle) = 0 + \langle f(x) \rangle$, i.e. $(x + \langle f(x) \rangle)^e = 1 + \langle f(x) \rangle$, which is then equivalent to $\alpha^e = 1$ in $\mathbb{F}_{q^k}$. Keeping in mind that e is by definition the smallest positive integer n that satisfies $f(x)|x^n - 1$, we conclude that $e = \text{ord}(\alpha)$. Since $|\mathbb{F}_{q^k}^*| = q^k - 1$, it then immediately follows that $e|q^k - 1$.

□

Lemma 3.4. *Let $g(x) \in \mathbb{F}_q[x]$ and $c \in \mathbb{Z}^+$. If $g(x)|x^c - 1$, then ord$(g(x))|c$*

Proof. Let $e := \text{ord}(g(x))$. From the definition of the order of a polynomial, we know that $e \leq c$. Then by the division algorithm, we may express $c = me + r$, for some unique integers $m > 0$ and $0 \leq r < e$. So $x^c - 1 = x^{me}x^r - 1 + x^r - x^r = (x^{me} - 1)x^r + (x^r - 1)$. Note that $x^e - 1|x^{me} - 1$, so that $g(x)$ divides both $x^c - 1$ and $x^{me} - 1$. Hence $g(x)|x^r - 1$. In order to not contradict the definition of e, since $r < e$, we must have that $r = 0$. Therefore, $e|c$. □

Lemma 3.5. *Let $f(x) := \prod_{i=1}^n g_i(x) \in \mathbb{F}_q[x]$, and for every i, let $e_i :=$ ord$(g_i(x))$. If $\{g_1(x), g_2(x), \ldots, g_n(x)\}$ is a pairwise relatively prime set, then we have ord$(f(x)) =$* $\text{lcm}(e_1, e_2, \ldots, e_n)$.

Proof. Set $e_i := \text{ord}(g_i(x))$ for each $g_i(x)$, and set $e := \text{lcm}(e_1, e_2, \ldots, e_n)$.

First, suppose that $f(0) \neq 0$, so that for each i, $g_i(0) \neq 0$. Then for every i, $g_i(x)|x^{e_i} - 1$, and so $g_i(x)|x^e - 1$. Since $g_1(x), g_2(x), \ldots, g_n(x)$ are pairwise relatively prime, it follows that their product, $f(x)$, divides $x^e - 1$. Hence, $\text{ord}(f(x)) \leq e$. On the other hand, since each factor $g_i(x)$ of $f(x)$ also divides $x^{\text{ord}(f(x))} - 1$, we have that for each i, $e_i|\text{ord}(f(x))$ by Lemma 3.4. Thus, $e|\text{ord}(f(x))$, so that $\text{ord}(f(x)) = e$.

Now suppose that $f(0) = 0$. Then for some j, $g_j(x) = x^h \bar{g}(x)$, where $h \in \mathbb{Z}^+$, $\bar{g}(0) \neq 0$ and for every $i \neq j$, $g_i(0) \neq 0$. Let $g(x) = \bar{g}(x) \cdot \prod_{i \neq j}^n g_i(x)$. Note that by definition, $e_j = \text{ord}(g_j(x)) = \text{ord}(\bar{g}(x))$. Then from the first case, we have $\text{ord}(f(x)) = \text{ord}(g(x)) = e$. □

Using Lemma 3.5, we can now determine the order of a polynomial in terms of its prime power decomposition, since each prime power factor is relatively prime to the other factors. We have thus reduced the problem from determining the order of a general monic polynomial to that of a power of an irreducible. We address the latter in the following lemma.

Lemma 3.6. *Let $f(x) := (g(x))^b \in \mathbb{F}_q[x]$, where b is a nonnegative integer and $g(x)$ is an irreducible polynomial with $g(0) \neq 0$. Let $p \in \mathbb{Z}^+$ be the characteristic of $\mathbb{F}_q$, and let $t := \min(t' \in \mathbb{Z}^+ \cup \{0\} \mid p^{t'} \geq b)$. Then $ord(f(x)) = p^t ord(g(x))$.*

Proof. Set $c := \operatorname{ord}(f(x))$ and $e := \operatorname{ord}(g(x))$. Since $g(x)|f(x)$, we have $g(x)|x^c - 1$. By Lemma 3.4, we deduce that $e|c$. Note that $g(x)|x^e - 1$ by definition, so that $f(x)|(x^e - 1)^b$. Therefore, by Lemma 1.13, $f(x)|(x^e - 1)^{p^t} = x^{ep^t} - 1$, since p is the characteristic of $\mathbb{F}_q$. Thus, by Lemma 1.13, we conclude that $c|ep^t$. Putting $e|c$ and $c|ep^t$ together, we have that $c = ep^u$, where $0 \leq u \leq t$ is an integer.

From Lemma 3.3, we know that since $g(x)$ is irreducible, $e|q^k - 1$ where $k = \deg(g(x))$. Thus, since the characteristic p of $\mathbb{F}_q$ divides q, it follows that $p \nmid e$. From Lemma 1.14, we know that any polynomial $h(x) \in \mathbb{F}_q[x]$ has a multiple zero if and only if $h(x)$ and its derivative $h'(x)$ have a common factor of positive degree in $\mathbb{F}_q[x]$. Now, since the characteristic p does not divide e, we see that the derivative $[x^e - 1]' = ex^{e-1} \neq 0$. Since x and $x^e - 1$ are relatively prime, and since $\mathbb{F}_q[x]$ is a unique factorization domain, it follows that $x^e - 1$ and ex^{e-1} are also relatively prime. Hence, all the roots of $x^e - 1$ must have multiplicity 1. Therefore, all the roots of $x^{ep^u} - 1 = (x^e - 1)^{p^u}$ have multiplicity p^u. Since $(g(x))^b | x^{ep^u} - 1$, the restriction on the multiplicity of the roots necessitates that $b \leq p^u$. Thus, by definition, $t \leq u$, and so $u = t$. Therefore, $c = ep^t$. □

From the above lemmas, we now have all the tools to derive the order of any monic polynomial:

Corollary 3.7. *Let $f(x) := \prod_{i=1}^n (g_i(x))^{b_i}$ be the prime power decomposition of $f(x) \in \mathbb{F}_q[x]$, with $\mathbb{F}_q$ having characteristic p. Let $e_i := ord(g_i(x))$ and $t_i := \min(t \in \mathbb{Z}^+ \cup \{0\} \mid p^t \geq b_i)$ for every i. Then $ord(f(x)) = \operatorname{lcm}(e_1, e_2, \ldots, e_n) \cdot p^t$, where $t := \max(t_1, t_2, \ldots, t_n)$.*

Proof. As noted in the proof of Lemma 3.6, $\gcd(e_i, p) = 1$ if $g_i(x)$ is irreducible and

$g_i(0) \neq 0$. By Lemmas 3.5 and 3.6, we thus have

$$\begin{aligned}
\operatorname{ord}(f(x)) &= \operatorname{lcm}(e_1 p^{t_1}, e_2 p^{t_2}, \dots, e_n p^{t_n}) \\
&= \operatorname{lcm}(e_1, e_2, \dots, e_n) \cdot \operatorname{lcm}(p^{t_1}, p^{t_2}, \dots, p^{t_n}) \\
&= \operatorname{lcm}(e_1, e_2, \dots, e_n) \cdot p^t
\end{aligned}$$

as desired. □

3.2. The Order of the Characteristic Polynomial

In Chapter 2 we were able to relate the least period of a linearly recurring sequence $\mathbf{s}$ to the order of the companion matrix A associated to the linear recurrence. We shall hence observe that, at least over finite fields, we can readily relate the least period of $\mathbf{s}$ to the order of the associated characteristic polynomial $f(x)$ as well, by showing that $\operatorname{ord}(A)$ and $\operatorname{ord}(f(x))$ are in fact equivalent. To prove this equivalence, we will need the following lemma.

Lemma 3.8. *Let $f(x)$ and A be the associated characteristic polynomial and companion matrix, respectively, of a linear recurrence relation of degree k over $\mathbb{F}_q$. Then $\{h(x) \in \mathbb{F}_q[x] \mid h(A) = 0 \in M_k(\mathbb{F}_q)\} = \langle f(x) \rangle$.*

Proof. Let $D := \{h(x) \in \mathbb{F}_q[x] \mid h(A) = 0 \in M_k(\mathbb{F}_q)\}$. It is straightforward to verify that the set D is a nontrivial ideal. Since $f(x) \in D$ by Lemma 2.35, we have $\langle f(x) \rangle \subseteq D$. Since a nonzero ideal in $\mathbb{F}_q[x]$ is generated by an element of least degree in the ideal (via Lemma 1.12), we can verify that $\langle f(x) \rangle = D$ by showing that every nonzero element in D has degree at least k.

Suppose there exists a polynomial $g(x) \in D$ with $g(x) := b_{k-1}x^{k-1} + b_{k-2}x^{k-2} + \dots + b_0$, for some $b_{k-1}, b_{k-2}, \dots, b_0 \in \mathbb{F}_q$. Let $\mathbf{s}_0 \in \mathbb{F}_{q^k}$. Then we have

$$\begin{aligned}
g(A) &= b_{k-1}A^{k-1} + b_{k-2}A^{k-2} + \dots + b_0 I \\
\mathbf{s}_0 g(A) &= \mathbf{s}_0[b_{k-1}A^{k-1} + b_{k-2}A^{k-2} + \dots + b_0 I] \\
\mathbf{s}_0 \cdot 0 &= b_{k-1}(\mathbf{s}_0 A^{k-1}) + b_{k-2}(\mathbf{s}_0 A^{k-2}) + \dots + b_0(\mathbf{s}_0 I) \\
\mathbf{0} &= b_{k-1}(\mathbf{s}_0 A^{k-1}) + b_{k-2}(\mathbf{s}_0 A^{k-2}) + \dots + b_0(\mathbf{s}_0 A^0) \\
\mathbf{0} &= b_{k-1}(\mathbf{s}_{k-1}) + b_{k-2}(\mathbf{s}_{k-2}) + \dots + b_0(\mathbf{s}_0)
\end{aligned}$$

If we choose $\mathbf{s}_0 = \mathbf{e}_k$, then by Lemma 2.38, $\{\mathbf{s}_i \mid i = 0, 1, \dots, k-1\}$ is a linearly independent set. Therefore, $b_{k-1} = b_{k-2} = \dots = b_0 = 0$. Thus, $g(x) = 0$, and so we're done.

□

Proposition 3.9. *Let $f(x)$ and A be the associated characteristic polynomial and companion matrix, respectively, of a linear recurrence relation of degree $k \in \mathbb{Z}^+$ over $\mathbb{F}_q$ given by Equation 1, such that $a_0 \neq 0$. Then $ord(f(x)) = ord(A)$.*

The proposition does not take into account all possible linear recurrences. We will address these exceptions later in the chapter, but as it turns out, determining a relationship between the order of the associated characteristic polynomial and the order of the companion matrix for the given subset of linear recurrences is sufficient to determine the least periods of all linearly recurring sequences.

Proof. Let $f(x)$ and A be given by Equations 4 and 9 respectively. Since $\deg(f(x)) = k \geq 1$ and $f(0) = a_0 \neq 0$, we conclude from Lemma 3.1 that there exists $e' \in \mathbb{Z}^+$ such that $f(x)|(x^{e'} - 1)$. Let $e = \operatorname{ord}(f(x))$, so that $f(x)|x^e - 1$. Now, since A is the companion matrix associated with $f(x)$, it follows from Lemma 2.35 that $f(A) = 0$. Therefore, $A^e - I = 0$, and so $A^e = I$. Thus, $\operatorname{ord}(A)|e$.

Conversely, since $A^{\operatorname{ord}(A)} = I$, so that $A^{\operatorname{ord}(A)} - I = 0$, it follows from Lemma 3.8 that $x^{\operatorname{ord}(A)} - 1 \in \langle f(x) \rangle$. Therefore, $f(x)|(x^{\operatorname{ord}(A)} - 1)$ which then implies that $e \leq \operatorname{ord}(A)$. And so combining this with $\operatorname{ord}(A)|e$, we see that $\operatorname{ord}(f(x)) = e = \operatorname{ord}(A)$. □

It is through the equivalence in Proposition 3.9 that we call $\operatorname{ord}(f(x))$ in the preceding definition the 'order' of the polynomial $f(x)$ in $\mathbb{F}_q[x]$. This terminology also arises naturally when we consider the order of a root of an irreducible polynomial, which, as we shall see in Lemma 3.3, is equivalent to the order of the polynomial itself.

Theorem 3.10. *Let $\mathbf{s}$ satisfy a linear recurrence relation over $\mathbb{F}_q$ with associated characteristic polynomial $f(x)$. Then $\rho(\mathbf{s})|ord(f(x))$.*

Proof. If $f(0) \neq 0$, then the statement follows immediately by combining Propositions 2.33 and 3.9. More generally, suppose $f(x) := x^h g(x)$, where $h \geq 0$ is an integer and $g(x) \in \mathbb{F}_q[x]$ such that $g(0) \neq 0$. Then by Lemma 2.10, we have that $\mathbf{s}^{(h)}$ satisfies a linear recurrence relation with characteristic polynomial $g(x)$. By Lemma 2.5, $\rho(\mathbf{s}^{(h)}) = \rho(\mathbf{s})$. By definition we also have that $\operatorname{ord}(f(x)) := \operatorname{ord}(g(x))$. Therefore, $\rho(\mathbf{s})|\operatorname{ord}(f(x))$ if and only if $\rho(\mathbf{s}^{(h)})|\operatorname{ord}(g(x))$, which again follows from Propositions 2.33 and 3.9.

□

3.3. The Minimal Polynomial

As described in the introduction of this chapter, for every linearly recurring sequence, there exists a unique associated characteristic polynomial, called the minimal polynomial, whose order determines the least period of the sequence. This section discusses the derivation of the minimal polynomial. The key to the minimal polynomial's derivation lies in the construction of a mechanism for characteristic polynomials to interact algebraically with linearly recurring sequences. We accomplish this goal by viewing the space of characteristic polynomials as residing in the larger space of power series, and by expressing linearly recurring sequences as elements of this space via their corresponding generating function (Definition 2.21). In the space of power series, a characteristic polynomial 'acts on' a linearly recurring sequence through the standard multiplication of the sequence's generating function and the *reciprocal* of the characteristic polynomial. The generating function, the ring of power series, and the reciprocal of a polynomial are all discussed in Section 1.3.

Lemma 3.11. *Let a linear recurrence relation of degree k over $\mathbb{F}_q$ be given, with characteristic polynomial $f(x)$. Set $a_k = -1$.*

If $\mathbf{s}$ is a sequence that satisfies a linear recurrence relation, and if $S(x) \in \mathbb{F}_q[[x]]$ is the generating function of $\mathbf{s}$, then

$$S(x) = \frac{g(x)}{f^*(x)} \tag{10}$$

where

$$g(x) := -\sum_{j=0}^{k-1}\left(\sum_{i=0}^{j} a_{i+k-j}s_i\right)x^j \in \mathbb{F}_q[x]. \tag{11}$$

Conversely, let $k \in \mathbb{Z}^+$. For all polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ such that $\deg(g(x)) < \deg(f(x)) = k$ *and $f(x)$ is monic, the formal power series $S(x) \in \mathbb{F}_q[[x]]$ defined by Equation 10 is the generating function of some sequence $\mathbf{s} \in \mathbb{F}_q$ that satisfies a linear recurrence relation with $f(x)$ as the characteristic polynomial.*

Proof. ($\Longrightarrow$) Let $\mathbf{s}$ satisfy a linear recurrence relation over $\mathbb{F}_q$ with reciprocal characteristic polynomial $f^*(x)$, so that

$$f^*(x) := x^k f(1/x) = 1 - a_{k-1}x - a_{k-2}x^2 - \ldots - a_0x^k \in R[x]. \tag{12}$$

Let the generating function $G(x)$ of $\mathbf{s}$ be given by Equation 5. Then setting $a_k = -1$, we have

$$f^*(x)S(x) = -\left(\sum_{n=0}^{k} a_{k-n}x^n\right)\left(\sum_{i=0}^{\infty} s_i x^i\right) = -\left[\sum_{j=0}^{\infty}\left(\sum_{n+i=j} a_{k-n}s_i\right)x^j\right]$$

Now for all integers $j \geq 0$, we have

$$\sum_{n+i=j} a_{k-n}s_i = \sum_{i=0}^{j} a_{k-(j-i)}s_i = \sum_{i=0}^{j} a_{i+k-j}s_i$$

where we define $a_i = 0$ for all integers $i < 0$. If $j < k$, then $\sum_{n+i=j} a_{k-n}s_i = \sum_{i=0}^{j} a_{i+k-j}s_i$ as above. On the other hand, if $j \geq k$, then $\sum_{n+i=j} a_{k-n}s_i = \sum_{i=j-k}^{j} a_{i+k-j}s_i$, since for any $i < j-k$, $i+k-j < j-k+k-j = 0$, and so $a_{i+k-j} = 0$. Therefore,

$$\begin{aligned} f^*(x)S(x) &= \left[-\sum_{j=0}^{k-1}\left(\sum_{i=0}^{j} a_{i+k-j}s_i\right)x^j - \sum_{j=k}^{\infty}\left(\sum_{i=j-k}^{j} a_{i+k-j}s_i\right)x^j\right] \\ &= g(x) - z(x) \end{aligned}$$

where $g(x)$ is given by Equation 11 and $z(x) := \sum_{j=k}^{\infty}\left(\sum_{i=j-k}^{j} a_{i+k-j}s_i\right)x^j = \sum_{j=k}^{\infty}\left(\sum_{i=0}^{k} a_i s_{j-k+i}\right)x^j$. By Lemma 2.23, we then have that for any integer $j \geq k$, $\sum_{i=0}^{k} a_i s_{j-k+i} = 0$. Hence, all coefficients of $z(x)$ vanish. Therefore, $f^*(x)S(x) = g(x)$. Now, since $f^*(x) \in \mathbb{F}_q[[x]]$ and $f^*(0) = 1 \neq 0$ is a unit, by Lemma 1.24 it follows that $f^*(x)$ has a multiplicative inverse. Therefore, $S(x) = \frac{g(x)}{f^*(x)}$.

($\Longleftarrow$) Now let $k \in \mathbb{Z}^+$, and let $f(x), g_0(x) \in \mathbb{F}_q[x]$ such that $\deg(g_0(x)) < \deg(f(x)) = k$ and $f(x)$ is monic. Note then that $f^*(0) = 1 \neq 0$. Thus, by Lemma 1.24, $f^*(x)$ has a multiplicative inverse $\frac{1}{f^*(x)} \in \mathbb{F}_q[[x]]$. Define the power series $S(x) := \frac{g_0(x)}{f^*(x)}$. Then by construction, $g_0(x) = f^*(x)S(x)$. By the calculation in the first part of our proof, we then have $g_0(x) = g(x) - z(x)$, with $g(x)$ and $z(x)$ as defined above. Since the degrees of $g_0(x)$ and $g(x)$ are both less than k, we observe that all coefficients of $z(x)$ must be 0. That is, for all integers $j \geq k$, $\sum_{i=j-k}^{j} a_{i+k-j}s_i = 0$, so that for all integers $j \geq 0$, $\sum_{i=0}^{k} a_i s_{i+j} = 0$. Hence, in light of Lemma 2.23, the sequence $\mathbf{s} := (s_i)_{i\geq 0}$ formed by the coefficients of $S(x) \in \mathbb{F}_q[x]$ satisfies te linear recurrence relation with characteristic polynomial $f(x)$.

□

Lemma 3.12. *Let* $\mathbf{s}$ *be a periodic sequence that satisfies a linear recurrence relation of degree* k *with characteristic polynomial* $f(x) \in \mathbb{F}_q[x]$*. Let* $n \in \mathbb{Z}^+$ *be a period of* $\mathbf{s}$*. Then there exists* $h(x) \in \mathbb{F}_q[x]$ *such that:*

$$f(x)S_n^*(x) = (x^n - 1)h(x) \tag{13}$$

Proof. Let $f(x)$ and its reciprocal $f^*(x)$ be given by Equations 4 and 12. Let $S(x)$ be the generating function of $\mathbf{s} := (s_i)_{i\geq 0}$. Since $\mathbf{s}$ is periodic with period n, $S(x)$ can be written in the following way:

$$S(x) = (s_0 + s_1x + s_2x^2 + \ldots + s_{n-1}x^{n-1})(1 + x^n + x^{2n} + \ldots) = \frac{S_n(x)}{1 - x^n}$$

From Lemma 3.11 we know that $S(x) = \frac{g(x)}{f^*(x)}$, where $g(x)$ is given by Equation 11. Therefore,

$$\frac{S_n(x)}{1 - x^n} = \frac{g(x)}{f^*(x)},$$

and so

$$f^*(x)S_n(x) = g(x)(1 - x^n). \tag{14}$$

Now, utilizing the derivation $x^cS_n^*(x) = x^{n-1}S_n(1/x)$ for $c := n - 1 - \deg(S_n(x))$ by Equation 7 and the fact that $f(x) = x^kf^*(1/x)$ by Equation 11, we have:

$$x^cf(x)S_n^*(x) = x^kf^*(1/x)x^{n-1}S_n(1/x) = x^{k+n-1}(f^*(1/x)S_n(1/x)).$$

Thus, by Equation 14, we get:

$$\begin{aligned} x^cf(x)S_n^*(x) &= x^{k+n-1}g(1/x)\left[1 - \left(\frac{1}{x}\right)^n\right] = x^{k-1}g(1/x)(x^n - 1) \\ &= (x^n - 1)H(x) \end{aligned}$$

where:

$$H(x) := g(1/x)x^{k-1} \tag{15}$$

Recall that $\deg(g(x)) \leq k - 1$, and so we see that $H(x)$ is indeed a polynomial, with $\deg(H(x)) \leq k - 1$. Note that x^c and $x^n - 1$ are relatively prime, so that x^c must divide $H(x)$. Hence, dividing x^c from both sides, we have

$$f(x)S_n^*(x) = (x^n - 1)h(x)$$

where

$$h(x) := \frac{H(x)}{x^c} = g(1/x)x^{k-c-1} \tag{16}$$

Therefore, there exists a polynomial $h(x) \in \mathbb{F}_q[x]$ such that $f(x)S_n^*(x) = (x^n - 1)h(x)$. □

Remark 3.13. *Lemma 3.12 states that* if $\mathbf{s}$ *is periodic, then there will exist a polynomial, namely $h(x)$, that satisfies Equation 13. We will hereafter use Equation 16 to define $h(x)$ even when* $\mathbf{s}$ *is not periodic.*

Note also that the definition of $h(x)$ depends solely on $g(x)$ and the degree k of the recurrence. Hence, in the case that $\mathbf{s}$ is periodic, the same polynomial $h(x)$ will arise in the proof of Lemma 3.12 regardless of the period n used. Thus, for every period $n \in \mathbb{Z}^+$ of a periodic sequence $\mathbf{s}$, Equation 13 is satisfied by $h(x)$ as defined in Equation 16.

Finally, as it turns out, $h(x)$ – whose definition is intimately related to $\mathbf{s}$ and $f(x)$ – holds the key to determining the minimal polynomial of $\mathbf{s}$. Specifically, if $h(x)$ and $f(x)$ are relatively prime, then $f(x)$ is in fact the minimal polynomial of $\mathbf{s}$. More generally, the minimal polynomial $m(x)$ of $\mathbf{s}$ is the greatest factor of $f(x)$ which is relatively prime to $h(x)$, as we shall see in the following theorem.

Theorem 3.14. *Let* $\mathbf{s} \in \mathbb{F}_q$ *be a linearly recurring sequence. Then there exists a uniquely determined monic polynomial $m(x) \in \mathbb{F}_q[x]$ such that for any $f(x) \in \mathbb{F}_q[x]$ with $f(x)$ monic,* $\mathbf{s}$ *satisfies a linear recurrence relation with characteristic polynomial $f(x)$ if and only if $m(x)|f(x)$.*

We shall refer to this uniquely determined monic polynomial $m(x)$ as the *minimal polynomial* of $\mathbf{s}$.

Proof. If $\mathbf{s}$ is the zero sequence, then $\mathbf{s}$ satisfies any linear recurrence relation, and we can take $m(x) = 1$ as the minimal polynomial of $\mathbf{s}$.

Now suppose that $\mathbf{s}$ is not the zero sequence, and that it satisfies the linear recurrence with characteristic polynomial $f_0(x) \in \mathbb{F}_q[x]$ of degree k_0. Let $S(x) \in \mathbb{F}_q[[x]]$ be the generating function of $\mathbf{s}$. Then by Lemma 3.11, there exist $g_0(x) \in \mathbb{F}_q[x]$ such that $S(x) = \frac{g_0(x)}{f_0^*(x)}$. Let $h_0(x) \in \mathbb{F}_q[x]$ be the polynomial determined by $f_0(x)$ and $g_0(x)$, as in Equation 16. Let $d(x) := \gcd(f_0(x), h_0(x))$ such that $d(x)$ is monic. Then $f_0(x) = m(x)d(x)$ and $h_0(x) = b(x)d(x)$, where $m(x), b(x) \in \mathbb{F}_q[x]$ and $\gcd(m(x), b(x)) = 1$. It is this polynomial $m(x)$ that is the desired minimal polynomial of $\mathbf{s}$.

We will first prove that $m(x)$ is monic. Note that since $d(x)$ and $f_0(x)$ are monic by definition, so is $m(x)$.

We now want to show that $m(x)$ indeed does satisfy the biconditional statement. Going in the forward direction, we will verify that $m(x)$ divides any characteristic polynomial which $\mathbf{s}$ satisfies. Suppose $\mathbf{s}$ also satisfies the linear recurrence with characteristic polynomial $f(x) \in \mathbb{F}_q[x]$. Again by Lemma 3.11, there exist $g(x) \in \mathbb{F}_q[x]$ such that $\frac{g(x)}{f^*(x)} = S(x) = \frac{g_0(x)}{f_0^*(x)}$. Thus,

$$g_0(x)f^*(x) = g(x)f_0^*(x)$$

Let $h(x) \in \mathbb{F}_q[x]$ be the polynomial determined by $f(x)$ and $\mathbf{s}$, as in Equation 16. Recall from Remark 3.13 that $h(x)$ exists and is defined by the equation regardless of whether $\mathbf{s}$ is periodic or not.

Then by the definitions of $f_0(x)$, $f(x)$, $h_0(x)$ and $h(x)$ as in Equations 16 and 3, we have the following:

$$\begin{aligned} h(x)f_0(x) &= g\left(\frac{1}{x}\right)x^{k-c-1}x^{k_0}f_0^*\left(\frac{1}{x}\right) = x^{k+k_0-c-1}g\left(\frac{1}{x}\right)f_0^*\left(\frac{1}{x}\right) \\ &= x^{k+k_0-c-1}g_0\left(\frac{1}{x}\right)f^*\left(\frac{1}{x}\right) = g_0\left(\frac{1}{x}\right)x^{k_0-c-1}x^kf^*\left(\frac{1}{x}\right) \\ &= h_0(x)f(x) \end{aligned}$$

We have that $h(x)m(x)d(x) = h(x)f_0(x) = h_0(x)f(x) = b(x)d(x)f(x)$, and canceling $d(x)$ gives:

$$h(x)m(x) = b(x)f(x)$$

.

Since $m(x)$ and $b(x)$ are relatively prime, it must therefore be that $m(x)|f(x)$. Thus, since $f(x)$ is arbitrary, it follows that $m(x)$ necessarily divides any characteristic polynomial of $\mathbf{s}$.

We will now show that every monic polynomial that is a multiple of $m(x)$ is necessarily a characteristic polynomial of $\mathbf{s}$. We know by definition that $h_0(x)m(x) = b(x)d(x)m(x) = b(x)f_0(x)$, and from Equation 16, we have that $h_0(x) = g_0(1/x)x^{k_0-c-1}$, so that $g_0(x) = x^{k_0-c-1}h_0(1/x)$. Therefore, letting $\kappa := \deg(m(x))$, the following holds:

$$\begin{aligned}
g_0(x)m^*(x) &= x^{k_0-c-1}h_0\left(\frac{1}{x}\right)x^{\kappa}m\left(\frac{1}{x}\right) = x^{k_0-c-1}x^{\kappa}h_0\left(\frac{1}{x}\right)m\left(\frac{1}{x}\right) \\
&= x^{\kappa-c-1}x^{k_0}b\left(\frac{1}{x}\right)f_0\left(\frac{1}{x}\right) = x^{\kappa-c-1}b\left(\frac{1}{x}\right)x^{k_0}f_0\left(\frac{1}{x}\right) \\
&= a(x)f_0^*(x)
\end{aligned}$$

where $a(x) := x^{\kappa-c-1}b\left(\frac{1}{x}\right)$. We check that $a(x)$ is indeed a polynomial. Note that by Equation 16, $\deg(h_0(x)) \leq k_0 - c - 1$. Since $h_0(x) = b(x)d(x)$ and $f_0(x) = m(x)d(x)$, it follows that $\deg(b(x)) = \deg(h_0(x)) - t \leq k_0 - c - t - 1$ and $\kappa = \deg(m(x)) = k_0 - t$, where $t := \deg(d(x))$. Therefore, $\deg(a(x)) = \kappa - c - 1 - \deg(b(x)) \geq (k_0 - t) - c - 1 - (k_0 - c - t - 1) = 0$. Hence, $a(x) \in \mathbb{F}_q[x]$. Also note that since $m(x)$ is monic, $m^*(0) = 1 \neq 0$, and so by Lemma 1.24, there exists a multiplicative inverse $\frac{1}{m^*(x)} \in \mathbb{F}_q[[x]]$.

Now let $f_1(x) \in \mathbb{F}_q[x]$ be such that $f_1(x)$ is monic and $m(x)|f_1(x)$. Then $f_1(x) := C(x)m(x)$, for some nonzero $C(x) \in \mathbb{F}_q[x]$. We know by Lemma 1.26 that $f_1^*(x) = C^*(x)m^*(x)$. We thus have:

$$g_0(x)m^*(x) = a(x)f_0^*(x)$$

$$S(x) = \frac{g_0(x)}{f_0^*(x)} = \frac{a(x)}{m^*(x)} = \frac{a(x)C^*(x)}{m^*(x)C^*(x)} = \frac{g_1(x)}{f_1^*(x)}$$

where $g_1(x) := a(x)C^*(x) \in \mathbb{F}_q[x]$. Since $\deg(a(x)) \leq \kappa - c - 1 < \deg(m(x))$ and $\deg(C^*(x)) \leq \deg(C(x))$, we have that $\deg(g_1(x)) = \deg(a(x)C^*(x)) = \deg(a(x)) + \deg(C^*(x)) < \deg(m(x)) + \deg(C(x)) = \deg(m(x)C(x)) = \deg(f_1(x))$.

Therefore, by Lemma 3.11, the sequence $\mathbf{s}$ satisfies a linear recurrence relation over $\mathbb{F}_q[x]$ with $f_1(x)$ as the associated characteristic polynomial. Thus, since $f_1(x)$ is arbitrary, we have that every nonzero monic multiple of $m(x)$ in $\mathbb{F}_q[x]$ is necessarily a characteristic polynomial of $\mathbf{s}$.

Finally, we shall prove that $m(x)$ is uniquely determined by the biconditional statement in the theorem. If $m_1(x)$ and $m_2(x)$ are two polynomials for which the biconditional statement in the theorem holds, then both must be characteristic polynomials for the sequence $\mathbf{s}$ and hence each must divide the other. Since they are monic, this implies that $m_1(x) = m_2(x)$.

□

Remark 3.15. *As mentioned in the proof of Theorem 3.14, the minimal polynomial of a linearly recurring sequence is also the characteristic polynomial of some linear recurrence relation satisfied by the sequence, since the minimal polynomial clearly divides itself.*

Remark 3.16. *Also note that in the proof of Theorem 3.14, the minimal polynomial $m(x)$ of $\mathbf{s}$ must satisfy $m(x) \cdot \gcd(f(x), h(x)) = f(x)$ for any arbitrary characteristic polynomial $f(x)$ of degree $k \in \mathbb{Z}^+$ of $\mathbf{s}$ and corresponding polynomial $h(x)$ as provided in Lemma 3.12.*

Theorem 3.17. *Let $\mathbf{s} \in \mathbb{F}_q$ be a linearly recurring sequence, and let $m(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of $\mathbf{s}$. Then $\rho(\mathbf{s}) = ord(m(x))$.*

Proof. Let $\rho(\mathbf{s})$ and $\eta(\mathbf{s})$ be the least period and preperiod of $\mathbf{s}$, respectively. Then for any integer $i \geq \eta(\mathbf{s})$, $s_i = s_{i+\rho(\mathbf{s})}$, so that for any integer $i \geq 0$, $s_{i+\eta(\mathbf{s})} = s_{i+\eta(\mathbf{s})+\rho(\mathbf{s})}$. Therefore, $\mathbf{s}$ satisfies the linear recurrence relation $s_{i+\eta(\mathbf{s})} = s_{i+\eta(\mathbf{s})+\rho(\mathbf{s})}$, with a corresponding characteristic polynomial $f(x) := x^{\eta(\mathbf{s})+\rho(\mathbf{s})} - x^{\eta(\mathbf{s})} = x^{\eta(\mathbf{s})}(x^{\rho(\mathbf{s})} - 1)$. Now let $m(x) \in \mathbb{F}_q[x]$ be the associated minimal polynomial of $\mathbf{s}$. Then by Theorem 3.14, $m(x)|f(x)$, so that $m(x) = x^h g(x)$, where $h \leq \eta(\mathbf{s})$ and $g(x) \in \mathbb{F}_q[x]$ such that $g(0) \neq 0$ and $g(x)|x^{\rho(\mathbf{s})} - 1$. By definition, we then have that $\text{ord}(m(x)) = \text{ord}(g(x)) \leq \rho(\mathbf{s})$. On the other hand, we know from Theorem 3.14 that $m(x)$ is a characteristic polynomial of $\mathbf{s}$. Then by Theorem 3.10, $\rho(\mathbf{s})|\text{ord}(m(x))$. Hence, $\rho(\mathbf{s}) = \text{ord}(m(x))$. □

3.4. Periods of Families of Linear Recurrences

We will summarize all our findings about the sets of least periods for a given linear recurrence relation, and then for a given class of degree-k linear recurrence relations, in this section.

Proposition 3.18. *For any given $k \in \mathbb{Z}^+$ and $\mathbb{F}_q$, and for every integer $l \geq k$, $\mathrm{P}(k, \mathbb{F}_q) \subseteq \mathrm{P}(l, \mathbb{F}_q)$.*

This is a special case of Proposition 2.8. We give an alternative proof using the minimal polynomial.

Proof. Let $\mathbf{s}$ be a sequence such that $\rho(\mathbf{s}) \in \mathrm{P}(k, \mathbb{F}_q)$. Then $\mathbf{s}$ satisfies a linear recurrence relation with characteristic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree k. Let $m(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of $\mathbf{s}$. By Theorem 3.14, $m(x)|f(x)$, so that $\deg(m(x)) \leq k \leq l$. Let $g(x) \in \mathbb{F}_q[x]$ be such that $f(x)|g(x)$ and $\deg(g(x)) = l$.

Then by Theorem 3.14, $\mathbf{s}$ satisfies the linear recurrence relation with characteristic polynomial $g(x)$. Hence, $\rho(\mathbf{s}) \in \mathrm{P}(l, \mathbb{F}_q)$. □

Lemma 3.19. *Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of degree k. Then there exists a linearly recurring sequence $\mathbf{s} \in \mathbb{F}_q$ such that $f(x)$ is the minimal polynomial of $\mathbf{s}$.*

Proof. If $k = 0$, then $f(x) = 1$, which is the minimal polynomial of the zero sequence.

If $k \in \mathbb{Z}^+$, then consider $g(x) := x^{k-1}$. Then by Lemma 3.11, the formal power series $S(x) := \frac{g(x)}{f^*(x)}$ is the generating function of some sequence $\mathbf{s}$ satisfying the linear recurrence relation with $f(x)$ as the associated characteristic polynomial. From Equation 16, the polynomial determined by $f(x)$ and $\mathbf{s}$ as in Lemma 3.12 is given by $h(x) := g(1/x)x^{k-c-1} = x^{-c}$. Since $h(x)$ is guaranteed to be a polynomial, it follows that $c = 0$ and that $h(x) = 1$. Let $m(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of $\mathbf{s}$. Then from the proof of Theorem 3.14, we have that $f(x) = m(x)\gcd(f(x), h(x)) = m(x) \cdot 1$. Thus, $f(x)$ is the minimal polynomial of $\mathbf{s}$. □

The polynomial $g(x) := x^{k-1}$, $k \in \mathbb{Z}^+$, that we used in the Proof of Lemma 3.19 actually corresponds to the impulse response sequence. From Proposition 2.40, we see that the impulse response sequence always yields the maximum possible least period for any linear recurrence relation, which is given by the order of the characteristic polynomial. However, the impulse response is not necessarily the only sequence that may yield the maximum possible least period. For example, by Theorem 3.14, we see that any nonzero sequence satisfying a linear recurrence with an irreducible characteristic polynomial necessarily has the maximum possible least period. Generally, for any sequence $\mathbf{s}$ satisfying a linear recurrence with characteristic polynomial $f(x)$ such that the associated polynomial $h(x) := g(1/x)x^{k-1}$ is relatively prime to $f(x)$, we have that $\rho(\mathbf{s}) = \mathrm{ord}(f(x))$.

We now have all the tools necessary to determine the sets of least periods that arise from linearly recurring sequences of small degree k over some finite field $\mathbb{F}_q$. To determine these sets of periods, we use the following facts: (1) that the least periods of sequences are equal to the orders of their associated minimal polynomials (Theorem 3.17), (2) that the minimal polynomial of a sequence divides every characteristic polynomial it satisfies (Theorem 3.14), and (3) that for any characteristic polynomial, there exists a linearly recurring sequence for which the polynomial is minimal. Hence, the set of least periods that will arise from linear recurrences of a given degree k over the finite field $\mathbb{F}_q$ is exactly the set of orders of all monic polynomials in $\mathbb{F}_q[x]$ of up to degree k. Additionally, as we shall see from Lemma 3.21, the set of orders of all monic polynomials of degree k completely accounts for the set of orders of all monic polynomials of degree less than k, and by extension accounts for the set of least periods arising from linear recurrences of degree k. We state this conclusion in Proposition 3.22.

Definition 3.20. Let $k \in \mathbb{Z}^+$. We let $\mathrm{M}(k, \mathbb{F}_q)$ denote the set of monic polynomials $f(x) \in \mathbb{F}_q[x]$ with $\deg(f(x)) = k$, and we let $\mathrm{O}(k, \mathbb{F}_q) := \{\mathrm{ord}(f(x)) \mid f(x) \in \mathrm{M}(k, \mathbb{F}_q)\}$.

Lemma 3.21. *Let $k \in \mathbb{Z}^+$ and $\mathbb{F}_q$ be given. For any nonnegative integer $j \leq k$, $\mathrm{O}(j, \mathbb{F}_q) \subseteq \mathrm{O}(k, \mathbb{F}_q)$.*

Proof. Let $n \in \mathrm{O}(j, \mathbb{F}_q)$. Then $n = \mathrm{ord}(g(x))$ for some monic polynomial $g(x) \in \mathbb{F}_q$ of degree j. Let $f(x) := x^h g(x)$, where $h = k - j$ is a nonnegative integer, so that $\deg(f(x)) = h + j = k$. Then by definition, $\mathrm{ord}(f(x)) = \mathrm{ord}(g(x)) = n$, and so $n \in \mathrm{O}(k, \mathbb{F}_q)$.

□

Proposition 3.22. *For any given $k \in \mathbb{Z}^+$ and $\mathbb{F}_q$, $\mathrm{P}(k, \mathbb{F}_q) = \mathrm{O}(k, \mathbb{F}_q)$.*

Proof. First, we check that $\mathrm{P}(k, \mathbb{F}_q) \subseteq \mathrm{O}(k, \mathbb{F}_q)$. Let $n \in \mathrm{P}(k, \mathbb{F}_q)$. Then there exists a linearly recurring sequence $\mathbf{s}$ with $\rho(\mathbf{s}) = n$, and characteristic polynomial $f(x)$ of degree k. By Theorem 3.14, the minimal polynomial $m(x)$ of $\mathbf{s}$ divides $f(x)$, and so $j \leq k$, where $j := \deg(m(x))$. $m(x)$ is also monic by definition, so we have that $m(x) \in \mathrm{M}(j, \mathbb{F}_q)$. Then by Theorem 3.17, $n = \rho(\mathbf{s}) = \mathrm{ord}(m(x)) \in \mathrm{O}(j, \mathbb{F}_q)$. Consequently, since $0 \leq j \leq k$, by Lemma 3.21, $n \in \mathrm{O}(k, \mathbb{F}_q)$.

Now we check the reverse containment. Let $n \in \mathrm{O}(k, \mathbb{F}_q)$. Then $n = \mathrm{ord}(m(x))$, for some $m(x) \in \mathrm{M}(k, \mathbb{F}_q)$, so that $m(x)$ is monic and $\deg(m(x)) = k$. By Lemma 3.19, there exists a linearly recurring sequence $\mathbf{s} \in \mathbb{F}_q$ such that $m(x)$ is the minimal polynomial of $\mathbf{s}$. By Remark 3.15, $m(x)$ is also a characteristic polynomial of degree k of $\mathbf{s}$. Thus, by Theorem 3.17 , $n = \mathrm{ord}(m(x)) = \rho(\mathbf{s}) \in \mathrm{P}(k, \mathbb{F}_q)$. □

Viewing the set of least periods as a set of orders of polynomials allows for us to determine their least upper bound, as in the corollary below.

Corollary 3.23. *For any $k \in \mathbb{Z}^+$ and finite field $\mathbb{F}_q$, $\rho(k, \mathbb{F}_q) = q^k - 1$.*

Proof. If $\mathbf{s}_0 = \mathbf{0}$, then $\mathbf{s}$ is the zero sequence and $\rho(\mathbf{s}) = 1$. Now observe that there exist at most $q^k - 1$ possible distinct nonzero tuples of length k over $\mathbb{F}_q$. Since $\mathbf{s}$ repeats when two state vectors are equal, it follows that $\rho(k, \mathbb{F}_q) = \rho(\mathbf{s}) \leq q^k - 1$.

We will now prove that there exists a polynomial of degree k over $\mathbb{F}_q$ whose order is $q^k - 1$, so that $q^k - 1$ is indeed the largest principal period for all linear recurrences of degree k. Take the generator of the cyclic group $\mathbb{F}_{q^k}^*$ and let $m(x)$ be its associated minimal polynomial. Note that $m(x)$ is irreducible, so we have by Lemma 3.3 that $\operatorname{ord}(m(x)) = q^k - 1$. We also have that $\mathbb{F}_{q^k}$ is obtained by adjoining a root of $m(x)$ to $\mathbb{F}_q$, so that $\deg(m(x)) = k$. Hence, by Proposition 3.22, $q^k - 1 = \operatorname{ord}(m(x)) \in \mathrm{O}(k, \mathbb{F}_q) = \mathrm{P}(k, \mathbb{F}_q)$. Thus, $\rho(k, \mathbb{F}_q) = q^k - 1$.

□

Combining Proposition 3.22 and the lemmas on orders of polynomials in Section 3.2, we now have all the tools to arrive at the following propositions. We can theoretically calculate the set of least periods associated with any given positive integer k and finite field $\mathbb{F}_q$, but here we will only show how to derive sets of least periods for small values of k.

Definition 3.24. Let $n \in \mathbb{Z}^+$ and let Z be an arbitrary set of positive integers. Then we use $\mathrm{D}(n)$ to denote the set of positive divisors of n, and we define $n \cdot Z := \{nz \mid z \in Z\}$. Furthermore, for any two $Z_1, Z_2 \subset \mathbb{Z}^+$, we define $Z_1 \cdot Z_2 := \{z_1 \cdot z_2 \mid z_1 \in Z_1, z_2 \in Z_2\}$.

Proposition 3.25. *For any given $k \in \mathbb{Z}^+$ and $\mathbb{F}_q$, $\bigcup_{i=1}^k \mathrm{D}(q^i - 1) \subset \mathrm{P}(k, \mathbb{F}_q)$.*

Proof. Let $n \in \mathrm{D}(q^i - 1)$ for some integer $1 \leq i \leq k$. Consider the multiplicative group $\mathbb{F}_{q^i}^*$ with order $q^i - 1$. Since $\mathbb{F}_{q^i}^*$ is cyclic, there exists a subgroup generated by some element $\alpha \in \mathbb{F}_{q^i}^*$ of order n. Let $m(x) \in \mathbb{F}_q(x)$ be the unique monic irreducible polynomial with α as a root and let $j = \deg(m(x))$. Then $1 \leq j \leq i \leq k$, since $j = [\mathbb{F}_q(\alpha) : F_q]$ and $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^i}$. By Lemma 3.6, Lemma 3.21 and Proposition 3.22, $n = \operatorname{ord}(\alpha) = \operatorname{ord}(m(x)) \in \mathrm{O}(j, \mathbb{F}_q) \subseteq \mathrm{O}(k, \mathbb{F}_q) = \mathrm{P}(k, F_q)$.

□

Definition 3.26. According to the division algorithm, for any two positive integers a and b, there exist unique $q, r \in \mathbb{Z}$ with $q \geq 0$ and $0 \leq r < b$ such that $a = qb + r$. The *integer quotient* of a by b is often denoted by $a//b = q$.

Proposition 3.27. *Let $k \in \mathbb{Z}^+$ be given, and let $\mathbb{F}_q$ have characteristic p. For any integer $1 \leq i \leq k$, $\{p^j \mid 0 \leq j \leq t_i\} \cdot \mathrm{D}(q^i - 1) \subseteq \mathrm{P}(k, \mathbb{F}_q)$, where $t_i = \min(t \in \mathbb{Z}^+ \cup \{0\} \mid p^t \geq k//i)$.*

This is a stronger statement than Proposition 3.25.

Proof. Let $n \in \left(\bigcup_{j=0}^{t_i}\{p^j\}\right) \cdot \mathrm{D}(q^i-1)$. Then $n = p^j m$ for some integer $0 \leq j \leq t_i$ and $m \in \mathrm{D}(q^i-1)$. From the proof of Proposition 3.25, we can find a monic irreducible polynomial $g(x) \in \mathbb{F}_q[x]$ with $\mathrm{ord}(g(x)) = m$ and $\deg(g(x)) \leq i$. Let $f(x) := (g(x))^b$, where $b := p^{j-1}+1$. Then by Lemma 3.6, $\mathrm{ord}(f(x)) = p^j m = n$. We also have $\deg(f(x)) = b\deg(g(x)) \leq bi \leq (p^{j-1}+1)i$. Hence, $\deg(f(x)) \leq k$, since $j \leq t_i$ and $p^{t_i-1}+1 \leq k//i$. Thus, by Lemma 3.21 and Proposition 3.22, $n = \mathrm{ord}(f(x)) \in \mathrm{O}(k, \mathbb{F}_q) = \mathrm{P}(k, \mathbb{F}_q)$.

□

Proposition 3.28. *For any $\mathbb{F}_q$,*

$$\mathrm{P}(1, \mathbb{F}_q) = \mathrm{D}(q-1).$$

Proof. From Proposition 3.22 and Lemma 3.3, we infer that $\mathrm{P}(1, \mathbb{F}_q) = \mathrm{O}(1, \mathbb{F}_q) = \{\mathrm{ord}(x-a) \mid a \in \mathbb{F}_q\} \subseteq \mathrm{D}(q-1)$. The reverse containment is guaranteed by Proposition 3.25.

□

Proposition 3.29. *For any $\mathbb{F}_q$ with prime characteristic p,*

$$\mathrm{P}(2, \mathbb{F}_q) = \mathrm{D}(q^2-1) \cup p \cdot \mathrm{D}(q-1).$$

Proof. We know from Proposition 3.22 that $\mathrm{P}(2, \mathbb{F}_q) = \mathrm{O}(2, \mathbb{F}_q)$.

We first prove that $\mathrm{O}(2, \mathbb{F}_q) \subseteq RHS$ (the right hand side). We consider the following cases for an arbitrary monic polynomial $f(x)$ of degree 2.

- Case 1: $f(x)$ is irreducible.

  Then from Lemma 3.3, $\mathrm{ord}(f(x)) \in \mathrm{D}(q^2-1)$.

- Case 2: $f(x) = m_1(x)m_2(x)$, where $m_1(x)$ and $m_2(x)$ are distinct monic irreducible polynomials of degree 1.

  Since $m_1(x)$ and $m_2(x)$ are distinct monic irreducibles, they are relatively prime. Then by Lemma 3.5, $\mathrm{ord}(f(x)) = \mathrm{lcm}(\mathrm{ord}(m_1(x)), \mathrm{ord}(m_2(x)))$. Noting that $\deg(m_1(x)) = \deg(m_2(x)) = 1$, we have that $\mathrm{ord}(m_1(x)), \mathrm{ord}(m_2(x)) \in \mathrm{D}(q-1)$. Note that the least common multiple of any two divisors of $q-1$ must also divide $q-1$. Hence, $\mathrm{ord}(f(x)) \in \mathrm{D}(q-1)$.

- Case 3: $f(x) = (m(x))^2$, where $m(x)$ is a monic irreducible polynomial of degree 1.

By Lemma 3.6, $\mathrm{ord}(f(x)) = p^t \mathrm{ord}(m(x))$, where p is the prime characteristic of $\mathbb{F}_q$, and t is the least nonnegative integer such that $p^t \geq 2$. Note that for any prime p, we have $t = 1$. Since $\deg(m(x)) = 1$, it follows that $\mathrm{ord}(m(x)) \in \mathrm{D}(q-1)$. Hence, $\mathrm{ord}(f(x)) = pn$, where $n \in \mathrm{D}(q-1)$.

Gathering all cases, we thus have that $\mathrm{O}(2, \mathbb{F}_q) \subseteq \mathrm{D}(q^2-1) \cup \mathrm{D}(q-1) \cup p \cdot \mathrm{D}(q-1) = \mathrm{D}(q^2-1) \cup p \cdot \mathrm{D}(q-1)$, where p is the characteristic of $\mathbb{F}_q$.

Now for the reverse containment. From Proposition 3.27, we determine that for all p, we have that $t_1 = 1$ and $t_2 = 0$, so that $\mathrm{O}(2, \mathbb{F}_q) = \mathrm{P}(2, \mathbb{F}_q) \supseteq \{1, p\} \cdot \mathrm{D}(q-1) \cup \mathrm{D}(q^2-1) = \mathrm{D}(q^2-1) \cup p \cdot \mathrm{D}(q-1)$.

□

Proposition 3.30. *Let $\mathbb{F}_q$ have prime characteristic p. If $p = 2$, then*

$$\mathrm{P}(3, \mathbb{F}_q) = \bigcup_{i=1}^{3} \mathrm{D}(q^i - 1) \cup \bigcup_{i=1}^{2} p^i \cdot \mathrm{D}(q-1).$$

Otherwise,

$$\mathrm{P}(3, \mathbb{F}_q) = \bigcup_{i=1}^{3} \mathrm{D}(q^i - 1) \cup p \cdot \mathrm{D}(q-1).$$

Proof. We know from Proposition 3.22 that $\mathrm{P}(3, \mathbb{F}_q) = \mathrm{O}(3, \mathbb{F}_q)$.

We consider the following cases for an arbitrary monic polynomial $f(x)$ of degree 3.

- Case 1: $f(x)$ is irreducible.

  Then from Lemma 3.3, $\mathrm{ord}(f(x)) \in \mathrm{D}(q^3 - 1)$.

- Case 2: $f(x) = m_1(x)m_2(x)$, where $m_1(x)$ and $m_2(x)$ are distinct monic irreducible polynomials of degrees 1 and 2, respectively.

  Since $m_1(x)$ and $m_2(x)$ are distinct monic irreducibles, they are relatively prime. Then by Lemma 3.5, $\mathrm{ord}(f(x)) = \mathrm{lcm}(\mathrm{ord}(m_1(x)), \mathrm{ord}(m_2(x)))$. Noting that $\deg(m_1(x)) = 1$ and $\deg(m_2(x)) = 2$, we have that $\mathrm{ord}(m_1(x)) \in \mathrm{D}(q-1) \subseteq \mathrm{D}(q^2-1)$ and $\mathrm{ord}(m_2(x)) \in \mathrm{D}(q^2-1)$. Hence, $\mathrm{ord}(f(x)) \in \mathrm{D}(q^2-1)$.

- Case 3: $f(x) = m_1(x)(m_2(x))^2$, where $m_1(x)$ and $m_2(x)$ are distinct monic irreducible polynomials of degree 1.

Since $m_1(x)$ and $m_2(x)$ are distinct monic irreducibles, they are relatively prime. Then by Lemma 3.5, $\text{ord}(f(x)) = \text{lcm}(\text{ord}(m_1(x)), \text{ord}((m_2(x))^2))$. Noting that $\deg(m_1(x)) = \deg(m_2(x)) = 1$, we have that $\text{ord}(m_1(x)), \text{ord}(m_2(x)) \in \text{D}(q-1)$. Using the same reasoning as in Case 3 of the proof of Proposition 3.29 that $\text{ord}((m_2(x))^2) = pn$, where $n \in \text{D}(q-1)$. Hence, $\text{ord}(f(x)) \in p \cdot \text{D}(q-1)$.

- Case 4: $f(x) = m_1(x)m_2(x)m_3(x)$, where $m_1(x)$, $m_2(x)$, $m_3(x)$ are distinct monic irreducible polynomials of degree 1.

  Since $m_1(x)$, $m_2(x)$, $m_3(x)$ are distinct monic irreducibles, they are pairwise relatively prime. Then by Lemma 3.5, $\text{ord}(f(x)) = \text{lcm}(\text{ord}(m_i(x)) \mid i = 1, 2, 3)$. Noting that $\deg(m_i(x)) = 1 \; \forall i$, we have that $\text{ord}(m_1(x)), \text{ord}(m_2(x)), \text{ord}(m_3(x)) \in \text{D}(q-1)$. Hence, $\text{ord}(f(x)) \in \text{D}(q-1)$.

- Case 5: $f(x) = (m(x))^3$, where $m(x)$ is a monic irreducible polynomial of degree 1.

  By Lemma 3.6, $\text{ord}(f(x)) = p^t \text{ord}(m(x))$, where p is the prime characteristic of $\mathbb{F}_q$, and t is the least nonnegative integer such that $p^t \geq 3$. If $p = 2$, then $t = 2$. Otherwise, $t = 1$. Since $\deg(m(x)) = 1$, it follows that $\text{ord}(m(x)) \in \text{D}(q-1)$. Hence, if $p = 2$, then $\text{ord}(f(x)) = p^2 n$, where $n \in \text{D}(q-1)$. Otherwise, $\text{ord}(f(x)) = pn$ with $n \in \text{D}(q-1)$.

Gathering all cases, we therefore have the following for $\mathbb{F}_q$ with characteristic p:

When $p = 2$, $\text{P}(3, \mathbb{F}_q) \subseteq \text{D}(q^3-1) \cup \text{D}(q^2-1) \cup p \cdot \text{D}(q-1) \cup \text{D}(q-1) \cup p^2\text{D}(q-1) = \bigcup_{i=1}^{3} \text{D}(q^i - 1) \cup \bigcup_{i=1}^{2} p^i \cdot \text{D}(q-1)$.

Otherwise, $\text{P}(3, \mathbb{F}_q) \subseteq \bigcup_{i=1}^{3} \text{D}(q^i - 1) \cup p \cdot \text{D}(q-1)$.

One can check that the reverse-containment for both cases holds by Proposition 3.27.

□

Proposition 3.31. *Let $\mathbb{F}_q$ have prime characteristic p. If $p = 2, 3$, then*

$$\text{P}(4, \mathbb{F}_q) = \bigcup_{i=1}^{4} \text{D}(q^i - 1) \cup \bigcup_{i=1}^{2} p^i \cdot \text{D}(q^{3-i} - 1).$$

Otherwise,

$$\text{P}(4, \mathbb{F}_q) = \bigcup_{i=1}^{4} \text{D}(q^i - 1) \cup p \cdot \text{D}(q^2 - 1).$$

Proof. We know from Proposition 3.22 that $\mathrm{P}(4, \mathbb{F}_q) = \mathrm{O}(4, \mathbb{F}_q)$.

We consider the following cases for an arbitrary monic polynomial $f(x)$ of degree 4.

- Case 1: $f(x)$ is irreducible.

  Then from Lemma 3.3, $\mathrm{ord}(f(x)) \in \mathrm{D}(q^4 - 1)$.

- Case 2: $f(x) = m_1(x)m_2(x)$, where $m_1(x)$ is a degree-1 monic irreducible polynomial $m_2(x)$ is a degree-3 monic polynomial that is relatively prime to $m_1(x)$.

  Then by Lemma 3.5, $\mathrm{ord}(f(x)) = \mathrm{lcm}(\mathrm{ord}(m_1(x)), \mathrm{ord}(m_2(x)))$. Since $\deg(m_1(x)) = 1$, we have that $\mathrm{ord}(m_1(x)) \in \mathrm{D}(q - 1)$. Since $\deg(m_2(x)) = 3$, we infer from Cases 1 through 5 of the proof of Proposition 3.30 that $\mathrm{ord}(m_2(x)) \in \bigcup_{i=1}^{3} \mathrm{D}(q^i - 1) \cup \bigcup_{i=1}^{2} p^i \cdot \mathrm{D}(q - 1)$ if the field characteristic $p = 2$, and that $\mathrm{ord}(m_2(x)) \in \bigcup_{i=1}^{3} \mathrm{D}(q^i - 1) \cup p \cdot \mathrm{D}(q - 1)$ otherwise. Hence, $\mathrm{ord}(f(x)) \in \bigcup_{i=1}^{3} \mathrm{D}(q^i - 1) \cup \bigcup_{i=1}^{2} p^i \cdot \mathrm{D}(q - 1)$ if $p = 2$ and $\mathrm{ord}(f(x)) \in \bigcup_{i=1}^{3} \mathrm{D}(q^i - 1) \cup p \cdot \mathrm{D}(q - 1)$ otherwise.

- Case 3: $f(x) = m_1(x)m_2(x)$, where $m_1(x)$ and $m_2(x)$ are relatively prime degree-2 monic polynomials.

  Since $m_1(x)$ and $m_2(x)$ are relatively prime, by Lemma 3.5, $\mathrm{ord}(f(x)) = \mathrm{lcm}(\mathrm{ord}(m_1(x)), \mathrm{ord}(m_2(x)))$. Since $\deg(m_1(x)) = \deg(m_2(x)) = 2$, we infer from Proposition 3.29 that $\mathrm{ord}(m_1(x)), \mathrm{ord}(m_2(x)) \in \mathrm{D}(q^2 - 1) \cup p \cdot \mathrm{D}(q - 1)$, where p is the characteristic of $\mathbb{F}_q$. Hence, $\mathrm{ord}(f(x)) \in \mathrm{D}(q^2 - 1) \cup p \cdot \mathrm{D}(q - 1)$.

- Case 4: $f(x) = (m(x))^2$, where $m(x)$ is a degree-2 monic irreducible polynomial.

  By Lemma 3.6, $\mathrm{ord}(f(x)) = p^t \mathrm{ord}(m(x))$, where p is the prime characteristic of $\mathbb{F}_q$, and t is the least nonnegative integer such that $p^t \geq 2$. Note that for any prime p, $t = 1$. Since $\deg(m(x)) = 2$, it follows that $\mathrm{ord}(m(x)) \in \mathrm{D}(q^2 - 1)$. Hence, $\mathrm{ord}(f(x)) \in p \cdot \mathrm{D}(q^2 - 1)$.

- Case 5: $f(x) = (m(x))^4$

  By Lemma 3.6, $\mathrm{ord}(f(x)) = p^t \mathrm{ord}(m(x))$, where p is the prime characteristic of $\mathbb{F}_q$, and t is the least nonnegative integer such that $p^t \geq 4$. If $p \leq 3$, then $t = 2$. Otherwise, $t = 1$. Since $\deg(m(x)) = 1$, it follows that $\mathrm{ord}(m(x)) \in \mathrm{D}(q - 1)$. Hence, if $p \leq 3$, then $\mathrm{ord}(f(x)) = p^2 n$, where $n \in \mathrm{D}(q - 1)$. Otherwise, $\mathrm{ord}(f(x)) = pn$.

Gathering all cases, we therefore have the following for $\mathbb{F}_q$ with characteristic p:

When $p \leq 3$, $\mathrm{P}(4, \mathbb{F}_q) \subseteq \bigcup_{i=1}^{4} \mathrm{D}(q^i - 1) \cup \bigcup_{i=1}^{2} p^i \cdot \mathrm{D}(q^{3-i} - 1)$.

Otherwise, $\mathrm{P}(4, \mathbb{F}_q) \subseteq \bigcup_{i=1}^{4} \mathrm{D}(q^i - 1) \cup p \cdot \mathrm{D}(q^2 - 1)$.

One can check that the reverse-containment for both cases holds by Proposition 3.27. □

At this point, the propositions regarding least periods for small values of k seem to suggest that the reverse containment to the relation in Proposition 3.27 also holds for all values of k. This is not true. Consider, for example, the case where $k = 5$ and $q = p = 2$. Let $f(x) = m_1(x)m_2(x)$, where $m_1(x)$ and $m_2(x)$ are monic irreducibles with $\mathrm{ord}(m_1(x)) = 2^2 - 1 = 3$ and $\mathrm{ord}(m_2(x)) = 2^3 - 1 = 7$. Then $\mathrm{ord}(f(x)) = \mathrm{lcm}(3, 7) = 21$. Notice that 21 is odd (not divisible by 2), and that 21 does not divide $2^i - 1$ for all integers $i = 1, 2, 3, 4, 5$. Thus, $\mathrm{ord}(f(x))$ cannot be in the set of periods specified by Proposition 3.27.

CHAPTER 4. SEQUENCES OVER FINITE QUOTIENTS OF PRINCIPAL IDEAL DOMAINS

In this chapter, we will primarily work with sequences defined over finite quotients of principal ideal domains. Our goal in this chapter is to determine the set of all least periods of sequences satisfying linear recurrence relations of a given degree k over R, when R is of the form $\mathbb{F}_q[x] \big/ \langle f(x) \rangle$.

4.1. Periods of Direct Sums

This section is devoted to determining the least periods of sequences when the ring over which the sequences are defined decomposes into a direct sum. To describe such sequences and their projections over the ring decomposition, we first introduce some new notation.

Definition 4.1. Let R and R' be rings, and let $\phi : R \to R'$ be a mapping. Then for any sequence $\mathbf{s} := (s_i)_{i \geq 0}$ over R, we define $\phi(\mathbf{s}) := (\phi(s_i))_{i \geq 0}$.

Definition 4.2. Let R be a commutative ring with an associated ring decomposition $R \cong R_1 \oplus R_2 \oplus \cdots \oplus R_r$, and let $\Phi : R \to R_1 \oplus R_2 \oplus \cdots \oplus R_r$ be the associated isomorphism. Then for every i, we let $\phi_i : R \to R_i$ denote the surjective homomorphism such that the map Φ is given by $x \mapsto (\phi_1(x), \phi_2(x), \ldots, \phi_r(x))$.

Lemma 4.3. *Let* $\mathbf{s}$ *be a linearly recurring sequence over a finite commutative ring* R*, and let* $\Phi : R \to R_1 \oplus R_2 \oplus \cdots \oplus R_r$ *be an isomorphism. Then* $\rho(\mathbf{s}) = \operatorname{lcm}(\rho(\phi_i(\mathbf{s})) \mid i = 1, 2, \ldots, r)$.

Proof. Note that since Φ is a bijection, $\rho(\mathbf{s}) = \rho(\Phi(\mathbf{s}))$. It then follows from Corollary 1.4 that $\rho(\mathbf{s}) = \operatorname{lcm}(\rho(\phi_i(\mathbf{s})) \mid i = 1, 2, \ldots, r)$. □

From this lemma, we immediately see that since the least period of every sequence satisfying a linear recurrence of degree k over R decomposes as a least common multiple of the least periods of sequences satisfying linear recurrences of degree k over the component rings R_i under the isomorphism Φ, it follows that $\mathrm{P}(k, R) \subseteq \{\operatorname{lcm}(n_1, n_2, \ldots, n_r) \mid n_i \in \mathrm{P}(k, R_i)\}$.

As it turns out, the reverse containment also holds. To prove this, we will require the following proposition:

Proposition 4.4. *Let R be a commutative ring which decomposes according to an isomorphism $\Phi : R \to R_1 \oplus R_2 \oplus \cdots \oplus R_r$, and let $f(x) \in R[x]$ be monic. Then $\Theta : \mathcal{A}(f(x)) \to \mathcal{A}(\phi_1(f(x))) \oplus \mathcal{A}(\phi_2(f(x))) \oplus \cdots \oplus \mathcal{A}(\phi_r(f(x)))$ given by $\Theta(\mathbf{s}) = (\phi_1(\mathbf{s}), \phi_2(\mathbf{s}), \ldots, \phi_r(\mathbf{s}))$ is a bijection.*

Proof. First note that if $\mathbf{s} \in \mathcal{A}(f(x))$ then $\phi_i(\mathbf{s}) \in \mathcal{A}(\phi_i(f(x)))$. Hence, $\Theta(\mathbf{s}) = (\phi_1(\mathbf{s}), \phi_2(\mathbf{s}), \ldots, \phi_r(\mathbf{s})) \in \mathcal{A}(\phi_1(f(x))) \oplus \mathcal{A}(\phi_2(f(x))) \oplus \cdots \oplus \mathcal{A}(\phi_r(f(x)))$. Since $\Phi : R \to R_1 \oplus R_2 \oplus \cdots R_r$ is a bijection, it is straightforward to show that Θ is injective. We now show that Θ is surjective.

Let $(\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_r) \in \mathcal{A}(\phi_1(f(x))) \oplus \mathcal{A}(\phi_2(f(x))) \oplus \cdots \oplus \mathcal{A}(\phi_r(f(x)))$, where for each j, $\mathbf{s}_j = (s_{ji})_{i\geq 0}$ (not to be confused with state vector notation). Note that for every i and j, $s_{ji} \in R_j$. Thus, since Φ is a bijection, for every i there exists $s_i \in R$ such that for every j, $\phi_j(s_i) = s_{ji}$. Let $\mathbf{s} := (s_i)_{i\geq 0}$.

Since $\mathbf{s}_j \in \mathcal{A}(\phi_j(f(x)))$ for every j, we then have that $\Phi(\mathbf{s})$ satisfies the following recurrence:

$$\Phi(s_{i+k}) = \Phi(a_0)\Phi(s_i) + \Phi(a_1)\Phi(s_{i+1}) + \ldots + \Phi(a_{k-1})\Phi(s_{i+k-1})$$

By the homomorphic property of Φ, it follows that

$$\Phi(s_{i+k}) = \Phi(a_0 s_i + a_1 s_{i+1} + \ldots + a_{k-1}s_{i+k-1}).$$

Since Φ is a bijection we have $s_{i+k} = a_0 s_i + \ldots a_{k-1}s_{i+k-1}$ for all integers $i \geq 0$. Hence, $\mathbf{s} \in \mathcal{A}(f(x))$. By construction, $\Theta(\mathbf{s}) = (\mathbf{s}_1, \mathbf{s}_2, \ldots \mathbf{s}_r)$. So we have shown that Θ is surjective.

□

Proposition 4.5. *Let $k \in \mathbb{Z}^+$ and let R be a finite commutative ring with an associated ring decomposition $R \cong R_1 \oplus R_2 \oplus \cdots \oplus R_r$. Then $\mathrm{P}(k, R) = \{\mathrm{lcm}(n_1, n_2, \ldots, n_r) \mid n_i \in \mathrm{P}(k, R_i).\}$*

Proof. We already know as a consequence of Lemma 4.3 that $\mathrm{P}(k, R) \subseteq RHS$.

Now for the reverse containment. Let $n \in \mathrm{lcm}(n_1, n_2, \ldots, n_r)$ with $n_i \in \mathrm{P}(k, R_i)$. Then for each j, $n_j = \rho((s_{ji})_{i\geq 0})$ for some $(s_{ji})_{i\geq 0} \in \mathcal{A}(f_j(x))$ where $f_j(x) \in R_j[x]$ is a monic polynomial of degree k. Since Φ induces the isomorphism $R[x] \cong R_1[x] \oplus R_2[x] \oplus \cdots \oplus R_r[x]$, there exists $f(x) \in R[x]$ monic of degree at most k such that $\phi_j(f(x)) = f_j(x)$ for every j. By Proposition 4.4, there exists $\mathbf{s} \in \mathcal{A}(f(x))$ such that $\phi_j(\mathbf{s}) = (s_{ji})_{i\geq 0}$ for every j, and by Lemma 4.3 we have $\rho(\mathbf{s}) = \mathrm{lcm}(\rho((s_{ji})_{i\geq 0}) \mid j = 1, 2, \ldots r) = n$. Thus, $n \in \mathrm{P}(k, R)$.

Therefore, $\mathrm{P}(k, R) = \{\mathrm{lcm}(n_1, n_2, \ldots, n_r) \mid n_i \in \mathrm{P}(k, R_i).\}$ □

We can specifically apply our result in Proposition 4.5 to the finite quotient of a principal ideal domain, as in Corollary 4.7 below.

Definition 4.6. If a ring R has the property in which $R/\langle m\rangle$ is finite for every nonzero $m \in R$, then we will call R a *ring with finite quotients.*

We can utilize Lemma 1.22 as a means of checking whether a given principal ideal domain has finite quotients. Examples of PIDs with finite quotients include $R := \mathbb{Z}$ and $R := \mathbb{F}_q[x]$. For any prime $p \in \mathbb{Z}^+$, $\mathbb{Z}_p \cong \mathbb{F}_p$. Likewise, for any irreducible (and hence prime) polynomial of $p(x) \in \mathbb{F}_q[x]$ of degree d, we have $\mathbb{F}_q[x]/\langle p(x)\rangle \cong \mathbb{F}_{q^d}$.

Corollary 4.7. *Let $k \in \mathbb{Z}^+$ and let R be a principal ideal domain with finite quotients. Let $m := \prod_{i=1}^{r} p_i^{e_i}$ be the prime power factorization of $m \in R$. Then $\mathrm{P}(k, R/\langle m\rangle) = \{\mathrm{lcm}(n_1, n_2, \ldots, n_r) \mid n_i \in \mathrm{P}(k, R/\langle p_i^{e_i}\rangle)\}$.*

Proof. By the Chinese Remainder Theorem (Lemma 1.20), $R/\langle m\rangle$ has the ring decomposition $R/\langle m\rangle \cong R/\langle p_1^{e_1}\rangle \oplus R/\langle p_2^{e_2}\rangle \oplus \cdots \oplus R/\langle p_r^{e_r}\rangle$. The statement then follows from Proposition 4.5. □

In [2], M. Ward analyzes the least periods that will arise over $R := \mathbb{Z}$. In the following section, we will discuss the least periods for the case when $R := \mathbb{F}_q[x]$.

4.2. Periods of Quotients of Polynomial Rings over Finite Fields

Since $\mathbb{F}_q[x]$ is a PID with finite quotients (see Lemma 1.15). We thus have:

Proposition 4.8. *Let $k \in \mathbb{Z}^+$ and let $\mathbb{F}_q$ be a finite field. Let $f(y) := \prod_{i=1}^{r}(p_i(y))^{e_i}$ be the prime power factorization of $f(y) \in \mathbb{F}_q[y]$. Then $\mathrm{P}(k, \mathbb{F}_q[y]/\langle f(y)\rangle) = \{\mathrm{lcm}(n_1, n_2, \ldots, n_r) \mid n_i \in \mathrm{P}(k, \mathbb{F}_q[y]/\langle (p_i(y))^{e_i}\rangle)\}$.*

If $f(y)$ factors into distinct irreducible polynomials of multiplicity 1, then we can use Corollary 1.17 to obtain:

Corollary 4.9. *Let $k \in \mathbb{Z}^+$ and let $\mathbb{F}_q$ be a finite field. Let $f(y) := \prod_{i=1}^{r} p_i(y)$ be the prime power factorization of $f(y) \in \mathbb{F}_q[y]$, where the irreducible factors are all distinct. Define $d_i := \deg(p_i(y))$ for each i. Then $\mathrm{P}(k, \mathbb{F}_q[y]/\langle f(x)\rangle) = \{\mathrm{lcm}(n_1, n_2, \ldots, n_r) \mid n_i \in \mathrm{P}(k, \mathbb{F}_{q^{d_i}})\}$.*

Definition 4.10. The *group algebra K[G]* of a group G over a field K is the set of all possible finite sums of the form $\sum_{i=0}^{n} \alpha_i g_i$, where for every i, $\alpha_i \in K$ and $g_i \in G$. If $K := \mathbb{F}_q$ and $G := C_r$ is a cyclic group of order r, then the *cyclic group algebra* $\mathbb{F}_q[C_r]$ is described by $\mathbb{F}_q[C_r] = \{\sum_{i=0}^{r-1} \alpha_i g^i \mid \alpha_i \in \mathbb{F}_q, \langle g \rangle = G\}$.

Lemma 4.11. *Let $\mathbb{F}_q$ be a finite field, and let C_m be a cyclic group of order m. Then*

$$\mathbb{F}_q[C_m] \cong \mathbb{F}_q[y] \,/ \langle y^m - 1 \rangle$$

Proof. Observe that the map $\mathbb{F}_q[y] \to \mathbb{F}_q[C_m]$ which sends $y \mapsto g$ is a surjective homomorphism. It is then easy to check that the kernel is $\langle y^m - 1 \rangle$. Hence, the statement follows by the First Isomorphism Theorem.

□

Corollary 4.12. *Let $\mathbb{F}_q$ be a finite field, and let C_m be a cyclic group of order m. Let $y^m - 1 = \prod_{i=1}^{r} f_i(y)$ be a decomposition of $y^m - 1 \in \mathbb{F}_q[y]$ such that $\{f_i(y) \mid i = 1, 2, \ldots r\}$ is a set of pairwise relatively prime polynomials. Then*

$$\mathbb{F}_q[C_m] \cong \mathbb{F}_q[y] \,/ \langle f_1(y) \rangle \oplus \mathbb{F}_q[y] \,/ \langle f_2(y) \rangle \oplus \cdots \oplus \mathbb{F}_q[y] \,/ \langle f_r(y) \rangle$$

Proof. This follows immediately from applying the Chinese Remainder Theorem (Lemma 1.19) and Lemma 4.11.

□

Lemma 4.13. *Let $\mathbb{F}_q$ be a finite field with characteristic p, and let $m \in \mathbb{Z}^+$ be such that $\gcd(m, p) = 1$. Then $y^m - 1 \in \mathbb{F}_q[y]$ decomposes into $y^m - 1 = \prod_{i=1}^{r} f_i(y)$, where each $f_i(y)$ is a distinct irreducible polynomial of some degree d_i.*

Proof. Let $f(y) := y^m - 1 \in \mathbb{F}_q[x]$. Then $f'(y) = my^{m-1}$, which does not vanish since m is relatively prime to the characteristic p of $\mathbb{F}_q$. Now $-1(y^m - 1) + ym^{-1}(my^{m-1}) = -y^m + 1 + y^m = 1$. Thus, $f(y)$ and $f'(y)$ are relatively prime, so that $\gcd(f(y), f'(y)) = 1$. It follows that $f(y)$ does not have any multiple roots in its splitting field over $\mathbb{F}_q$, and thus, $f(y)$ factors into distinct irreducible polynomials.

□

Combining Lemmas 4.11 and 4.13, we obtain the following:

Proposition 4.14. *Let $\mathbb{F}_q$ be a finite field with characteristic p, and let C_m be a cyclic group of order m. If $\gcd(m, p) = 1$, then*

$$\mathbb{F}_q[C_m] \cong \mathbb{F}_{q^{d_1}} \oplus \mathbb{F}_{q^{d_2}} \oplus \cdots \oplus \mathbb{F}_{q^{d_m}} \tag{17}$$

where $d_1, d_2, \ldots, d_m$ are defined in Lemma 4.13, and for all $k \in \mathbb{Z}^+$,

$$\mathrm{P}(k, \mathbb{F}_q[C_m]) = \{\mathrm{lcm}(n_1, n_2, \ldots, n_r) \mid n_i \in \mathrm{P}(k, \mathbb{F}_{q^{d_i}}). \tag{18}$$

Proof. According to Lemma 4.13, $y^m - 1$ decomposes into $y^m - 1 = \prod_{i=1}^{r} f_i(y)$, where each $f_i(y)$ is a distinct irreducible polynomial of some degree d_i. By Corollary 4.12, we have that

$$\mathbb{F}_q[C_m] \cong \mathbb{F}_q[y] \,/\langle f_1(y)\rangle \oplus \mathbb{F}_q[y] \,/\langle f_2(y)\rangle \oplus \cdots \oplus \mathbb{F}_q[y] \,/\langle f_r(y)\rangle$$

Also, by Corollary 1.17, for every i,

$$\mathbb{F}_q[y] \,/\langle f_i(y)\rangle \cong \mathbb{F}_{q^{d_i}}$$

Hence, we arrive at Equation 17. Equation 18 follows from Corollary 4.9 and Lemma 4.13. □

To fully grasp the meaning of Proposition 4.14, let us look at the following examples.

Example 4.15. Consider the ring $\mathbb{F}_2[C_3]$. Since 2 and 3 are relatively prime, and since $y^3 - 1$ has the prime factorization $y^3 - 1 = (y-1)(y^2+y+1)$ over $\mathbb{F}_2$, we have $\mathbb{F}_2[C_3] \cong \mathbb{F}_2 \oplus \mathbb{F}_{2^2}$ by Proposition 4.14.

We thus calculate the following sets of periods for linear recurrences of degrees 2 and 3:

- $\mathrm{P}(2, \mathbb{F}_2[C_3]) = \{\mathrm{lcm}(n_1, n_2) \mid n_1 \in \mathrm{P}(2, \mathbb{F}_2), n_2 \in \mathrm{P}(2, \mathbb{F}_4)\}$

  By Proposition 3.29, we have:

  $$\begin{aligned} \mathrm{P}(2, \mathbb{F}_2) &= \mathrm{D}(2^2 - 1) \cup 2 \cdot \mathrm{D}(2-1) = \{1, 2, 3\} \\ \mathrm{P}(2, \mathbb{F}_4) &= \mathrm{D}(4^2 - 1) \cup 2 \cdot \mathrm{D}(4-1) = \{1, 3, 5, 15\} \cup \{2, 6\} = \{1, 2, 3, 5, 6, 15\} \end{aligned}$$

  Hence,

  $$\begin{aligned} \mathrm{P}(2, \mathbb{F}_2[C_3]) &= \{\mathrm{lcm}(n_1, n_2) \mid n_1 \in \{1, 2, 3\}, n_2 \in \{1, 2, 3, 5, 6, 15\}\} \\ &= \{1, 2, 3, 5, 6, 10, 15, 30\} \end{aligned}$$

- $\mathrm{P}(3, \mathbb{F}_2[C_3]) = \{\mathrm{lcm}(n_1, n_2) \mid n_1 \in \mathrm{P}(3, \mathbb{F}_2), n_2 \in \mathrm{P}(3, \mathbb{F}_4)\}$

By Proposition 3.30, we have:

$$\begin{aligned}
\mathrm{P}(3,\mathbb{F}_2) &= \bigcup_{i=1}^{3} \mathrm{D}(2^i-1) \cup \bigcup_{i=1}^{2} 2^i \cdot \mathrm{D}(2-1) = \{1,3,7\} \cup \{2,4\} \\
&= \{1,2,3,4,7\} \\
\mathrm{P}(3,\mathbb{F}_4) &= \bigcup_{i=1}^{3} \mathrm{D}(4^i-1) \cup \bigcup_{i=1}^{2} 2^i \cdot \mathrm{D}(4-1) = \{1,3,5,7,9,15,21,63\} \cup \{2,4,6,12\} \\
&= \{1,2,3,4,5,6,7,9,12,15,21,63\}
\end{aligned}$$

Hence,

$$\begin{aligned}
\mathrm{P}(3,\mathbb{F}_2[C_3]) &= \{\mathrm{lcm}(n_1,n_2) \mid n_1 \in \{1,2,3,4,7\}, n_2 \in \{1,2,3,4,5,6,7,9,12,15,21,63\}\} \\
&= \{1,2,3,4,5,6,7,9,10,12,14,15,18,20,21,28,30,35,36,42,60, \\
&\quad 63,84,105,126,252\}
\end{aligned}$$

We have verified all of the sets of periods above by generating them empirically though a computational algebra program.

Example 4.16. Consider the rings $\mathbb{F}_2[C_5]$ and $\mathbb{F}_5[C_2]$. Since 2 and 5 are relatively prime, we have the following through Proposition 4.14:

- y^5-1 has the prime factorization $y^5-1=(y-1)(y^4+y^3+y^2+y+1)$ over $\mathbb{F}_2$, and so $\mathbb{F}_2[C_5] \cong \mathbb{F}_2 \oplus \mathbb{F}_{2^4}$.
- y^2-1 has the prime factorization $y^2-1=(y-1)(y+1)$ over $\mathbb{F}_5$, and so $\mathbb{F}_5[C_2] \cong \mathbb{F}_5 \oplus \mathbb{F}_5$.

We thus obtain the following sets of periods for linear recurrences of degree 2:

- $\mathrm{P}(2,\mathbb{F}_2[C_5]) = \{\mathrm{lcm}(n_1,n_2) \mid n_1 \in \mathrm{P}(2,\mathbb{F}_2), n_2 \in \mathrm{P}(2,\mathbb{F}_{16})\}$

  By Proposition 3.29, we have:

  $$\begin{aligned}
  \mathrm{P}(2,\mathbb{F}_2) &= \{1,2,3\} \\
  \mathrm{P}(2,\mathbb{F}_{16}) &= \mathrm{D}(16^2-1) \cup 2 \cdot \mathrm{D}(16-1) = \{1,3,5,15,17,51,85,255\} \cup \{2,6,10,30\} \\
  &= \{1,2,3,5,6,10,15,17,30,51,85,255\}
  \end{aligned}$$

  Hence,

  $$\begin{aligned}
  \mathrm{P}(2,\mathbb{F}_2[C_5]) &= \{\mathrm{lcm}(n_1,n_2) \mid n_1 \in \{1,2,3\}, n_2 \in \{1,2,3,5,6,10,15,17,30,51,85,255\}\} \\
  &= \{1,2,3,5,6,10,15,17,30,34,51,85,102,170,255,510\}
  \end{aligned}$$

- $\mathrm{P}(2, \mathbb{F}_5[C_2]) = \{\mathrm{lcm}(n_1, n_2) \mid n_1, n_2 \in \mathrm{P}(2, \mathbb{F}_5)\}$

  By Proposition 3.29, we have:

$$\begin{aligned}\mathrm{P}(2, \mathbb{F}_5) &= \mathrm{D}(5^2 - 1) \cup 5 \cdot \mathrm{D}(5 - 1) = \{1, 2, 3, 4, 6, 8, 12, 24\} \cup \{5, 10, 20\} \\ &= \{1, 2, 3, 4, 5, 6, 8, 10, 12, 20, 24\}\end{aligned}$$

  Hence,

$$\begin{aligned}\mathrm{P}(2, \mathbb{F}_5[C_2]) &= \{\mathrm{lcm}(n_1, n_2) \mid n_1, n_2 \in \{1, 2, 3, 4, 5, 6, 8, 10, 12, 20, 24\}\} \\ &= \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}\end{aligned}$$

We have verified all of the sets of periods above by generating them empirically though a computational algebra program.

Example 4.17. Consider the rings $\mathbb{F}_2[C_6]$. Since 2 and 6 are *not* relatively prime, we cannot apply Proposition 4.14 to calculate its set of least periods. Indeed, $y^6 - 1$ factors into $y^6 - 1 = (y - 1)(y + 1)(y^2 - y + 1)(y^2 + y + 1) = (y + 1)^2(y^2 + y + 1)^2$, and so $y^6 - 1$ does not decompose into distinct irreducible polynomials, which is necessary for the group algebra to decompose into the direct sum of finite fields. Through our computational algebra program, we determine that $\mathrm{P}(2, \mathbb{F}_2[C_6]) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$. A natural open question to explore when following up on this thesis would be whether or not there exists a method of determining the sets of least periods arising from sequences over cyclic group algebras of the form $\mathbb{F}_q[C_m]$ where m is not relatively prime to the characteristic p of $\mathbb{F}_q$, so as to make sense out of the numbers generated through our algebra program.

We now provide bounds on the principal period in the simplest situation where $y^m - 1$ has only two irreducible factors.

Theorem 4.18. *Let $\mathbb{F}_q$ be a finite field, and let m and k be arbitrary positive integers. If $y^m - 1 = (y - 1)(y^{m-1} + y^{m-2} + \ldots + 1)$ cannot be factored any further over $\mathbb{F}_q$, then the principal period $\rho(k, \mathbb{F}_q[C_m])$ is bounded by:*

$$(q^{m-1})^k - 1 \leq \rho(k, \mathbb{F}_q[C_m]) \leq (q^k - 1)((q^{m-1})^k - 1). \tag{19}$$

Moreover, for $k = 2$ and $q = 2$, we have:

$$2[(2^{m-1})^2 - 1] \leq \rho(2, \mathbb{F}_2[C_m]) \leq 3[(2^{m-1})^2 - 1]. \tag{20}$$

Proof. By Proposition 4.14, since $y^m - 1$ only factors into two distinct irreducible polynomials as described in the statement's assumption, we have $\mathrm{P}(k, \mathbb{F}_q[C_m]) = S$, where we define

$$S := \{\mathrm{lcm}(n_1, n_2) \mid n_1 \in \mathrm{P}(k, \mathbb{F}_q), n_2 \in \mathrm{P}(k, \mathbb{F}_{q^{m-1}})\}.$$

Let $n \in \mathrm{P}(k, \mathbb{F}_q[C_m])$. Since $\mathrm{lcm}(n_1, n_2) \leq n_1 n_2$, by Corollary 3.23 we have

$$n \leq \rho(k, \mathbb{F}_q) \cdot \rho(k, \mathbb{F}_{q^{m-1}}) = (q^k - 1)(q^{k(m-1)} - 1)$$

Hence, $\rho(k, \mathbb{F}_q[C_m]) \leq (q^k - 1)(q^{k(m-1)} - 1)$.

Now, since $q^k - 1 | q^{k(m-1)} - 1$, we have $\mathrm{lcm}(q^k - 1, q^{k(m-1)} - 1) = q^{k(m-1)} - 1 \in S = \mathrm{P}(k, \mathbb{F}_q[C_m])$, and so $\rho(k, \mathbb{F}_q[C_m]) \geq q^{k(m-1)} - 1 = (q^{m-1})^k - 1$. We thus arrive at Inequality 19.

If $k = 2$ and $q = 2$, then Inequality 19 simplifies to:

$$(2^{m-1})^2 - 1 \leq \rho(2, \mathbb{F}_2[C_m]) \leq (2^2 - 1)(2^{2(m-1)} - 1) = 3[(2^{m-1})^2 - 1].$$

However, we can place even further restrictions on these bounds. Note that by Proposition 3.29, $\mathrm{P}(2, \mathbb{F}_2) = \{1, 2, 3\}$. Thus, in our special case, $\mathrm{lcm}(2, (2^{m-1})^2 - 1) = 2[(2^{m-1})^2 - 1] \in S = \mathrm{P}(2, \mathbb{F}_2[C_m])$, and so $\rho(2, \mathbb{F}_2[C_m]) \geq 2[(2^{m-1})^2 - 1]$. We then arrive at Inequality 20, and we are done.

□

As an aside, we observe that $\rho(k, \mathbb{F}_q[C_m])$ is strictly less than $(q^m)^k - 1 = \rho(\mathbb{F}_{q^m})$, and so the principal period over a cyclic group algebra is always less the principal period over a finite field of the same size.

We return to our earlier examples to show that the principal period does indeed fall between the bounds prescribed by Theorem 4.18. In practice, the principal period for the general case lies strictly between the bounds of Inequality 19, while the principal period for the special case where $k = q = 2$ seems to consistently fall on the lower bound of Inequality 20.

Example 4.19. From Example 4.15, we know that $y^3 - 1 = (y - 1)(y^2 + y + 1)$ over $\mathbb{F}_2$ so that $\mathbb{F}_2[C_3] \cong \mathbb{F}_2 \oplus \mathbb{F}_4$.

We also have $\rho(2, \mathbb{F}_2[C_3]) = \max(\mathrm{P}(2, \mathbb{F}_2[C_3])) = 30 = 2[(2^2)^2 - 1]$, in agreement with Inequality 20. On the other hand, $\rho(3, \mathbb{F}_2[C_3]) = \max(\mathrm{P}(3, \mathbb{F}_2[C_3])) = 252$. We see that $(2^2)^3 - 1 = 65 < 252$ and $(2^3 - 1)((2^2)^3 - 1) = 441 > 252$, and so $\rho(2, \mathbb{F}_2[C_3]) = 252$ agrees with Inequality 19.

Example 4.20. From Example 4.16, we know that $y^5-1=(y-1)(y^4+y^3+y^2+y+1)$ over $\mathbb{F}_2$ and that $y^2-1=(y-1)(y+1)$ over $\mathbb{F}_5$, so that $\mathbb{F}_2[C_5] \cong \mathbb{F}_2 \oplus \mathbb{F}_{16}$ and $\mathbb{F}_5[C_2] \cong \mathbb{F}_5 \oplus \mathbb{F}_5$.

We also have $\rho(2, \mathbb{F}_2[C_5]) = \max(\mathrm{P}(2, \mathbb{F}_2[C_5])) = 510 = 2[(2^4)^2-1]$, in agreement with Inequality 20. On the other hand, $\rho(2, \mathbb{F}_5[C_2]) = \max(\mathrm{P}(2, \mathbb{F}_5[C_2])) = 120$. We see that $(5^1)^2-1 = 24 < 120$ and $(5^2-1)((5^1)^2-1) = 576 > 120$, and so $\rho(2, \mathbb{F}_5[C_2]) = 120$ agrees with Inequality 19.

REFERENCES

[1] R. Lidl and H. Niederreiter, *Finite Fields*. Encyclopedia of Mathematics and its Applications, Vol. 20, Cambridge University Press, 1997.

[2] M. Ward, *The Arithmetical Theory of Linear Recurring Series*, Trans. Amer. Math. Soc. **35** No. 3 (1933), 600–628.

[3] J. Gallian, *Contemporary Abstract Algebra*. Seventh Edition. Cengage Learning, Belmont, CA, 2010.