GENERATORS OF PERIODIC SEQUENCES
OVER A FINITE FIELD

A Thesis
Presented to
the Faculty of the Department of Mathematics
Kansas State Teachers College of Emporia

In Partial Fulfillment
of the Requirements for the Degree
Master of Science in Mathematics

by
Richard Lee Page
January 1967

GRADUATE COUNCIL APPROVAL

DEPARTMENTAL APPROVAL

Lester E. Laird

ACKNOWLEDGEMENT

The author wishes to express his sincere appreciation to Mr. Lester Laird for his helpful suggestions in preparation of this paper.

To

my wife Carol

$(\text{Happiness})^n - (\text{Love}) \equiv 0 \pmod{\text{Carol}}$

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

When studying infinite sequences, there are many of these sequences whose elements become repetitive. This naturally gives rise to the questions: (1) How can such an infinite sequence be generated?, and (2) If given such a sequence, how can its generator be found? When considering only those sequences of maximum period over a finite field, such questions may be answered.

I. THE PROBLEM

Statement of the problem. The purpose of this study is (1) to show that all sequences of maximum period over a finite field may be generated by a linear recurrence relation; (2) to show an isomorphism of the linear recurrence definition to a set of quotient polynomials; (3) to develope the background for synthesis of the minimum degree generator, given an infinite periodic sequence.

Limitations. Since there have been numerous studies made concerning infinite periodic sequences defined by a recurrence relation, this paper can deal only with those sequences which may be defined by a linear recurrence relation over a modular field of integers. Such sequences are shown to be purely periodic, thus greatly simplifying the task of finding the minimum degree generator.

Importance of the problem. Infinite sequences of maximum period over a modular field have many interesting properites and uses. However, this study was induced by the occurrence of such sequences in natural and physical science phenomenon. One such physical application might be in electrical impulse circuits, where the elements of the sequence are considered as amplitudes of the electrical impulses with respect to time. Generators of such sequences are then of great importance in determining circuit topology.

II. BRIEF HISTORY

In the year 1202 Leonard Pisano, or Fibonacci, used the recurring sequence 1, 2, 3, 5, 8, 13, ... concerning the offspring of a pair of rabbits. Later Girard (1590?-1633?) noted the linear recurrence, $u_{n+2} = u_{n+1} + u_n$, for this sequence (arithemetic series). This sequence, referred to today as the Fibonacci sequence, was probably one of the earliest sequences defined by a linear recurrence relation.

An interesting account of the history of recurring series from the time of Pisano until the early nineteen-hundreds was given by Dickson (1874-1954) in his History of the Theory of Numbers, volume I, Chapter XVII, "Recurring Series".

Lucas (1842-1891) was the first to make any extensive studies on sequences. Lucas in his earlier work stated without proof many theorems on the series of Pisano and also established many properties of second order sequences. Later in 1930 in a paper on extended theory of the Lucas' functions, Lehmer devised a test for the primality of Mersenne numbers 2^p-1 (p, a prime) which has been used for the discovery of a prime with several hundred digits.

In the year 1913 Carmicheal generalized many of the Lucas' theorems and corrected several others. Later in 1920 Carmicheal made the first attempt on sequences in general and established much of the terminology used to dicuss their fundamental property of modular periodicity. In a paper presented to the American Mathematical Society in 1930, Engstrom further developed the concept of modular periodicity by reducing the restrictions on the modulus.

Ward presented a paper to the Society in 1932 which discussed methods to determine the least upper bounds for the characteristic number and the numeric of any solution to a general linear recurrence relation. Also discussed by Ward, and of great importance to the present study, was that there always exist solutions of the defining recurrence relation whose characteristic number modulo m is the principal period of the defining recurrence relation. Ward also presented in the same paper the fundamental theorem on purely periodic sequences and several useful corollaries.

Hall in a paper presented to the American Mathematical Society in 1936 discussed an isomorphism between linear recurring sequences and algebraic rings.

Brenner in a short note presented to the American Mathematical Monthly in 1954 discussed a method to determine the period of a sequence using established theorems about matrices.

Zierler in a paper published in the Journal for the Society of Industrial and Applied Mathematics in 1959, discussed the very small class of linear recurring sequences which are of interest in this study, i.e., sequences of maximum period generated by a linear recurrence over a finite field. Also in the same paper, Zierler gives a proof of the equivalence of the defining linear recurrence and a quotient ring of polynomials. Many of the theorems necessary to find the minimum degree ratio of polynomials which generate a given sequence are presented by Zierler in his paper.

In more recent years linear recurring sequences have also been examined by Albert, Blankinship, and Golomb. However, most of the background for the present study was presented by Zierler, Brenner, Hall, and Ward.

III. OUTLINE OF APPROACH TO THE PROBLEM

An isomorphism is made between infinite periodic sequences over a modular field of integers and infinite degree polynomials whose coefficients are elements of the same modular field. Furthermore, it is shown that these infinite degree polynomials may be expressed as a ratio of finite degree polynomials. These polynomials are defined over the field GF(p), and their root fields are extensions of GF(p). A general synthesis procedure is developed to find the minimum degree ratio of polynomials which will produce any periodic sequence over GF(p). The root of their polynomial representations will be considered so that a synthesis procedure may be developed.

Chapter II shows that the set of all sequences $\{x_i\}_{i=0}^{\infty}$ $x_i \in I_p$ satisfying a defining linear recurrence relation is generated by a (k+1)-tuple of elements of I_p and each $\{x_i\}_{i=0}^{\infty}$ is uniquely determined by the k-tuple which consists of the first k elements of the sequence $\{x_i\}_{i=0}^{\infty}$. It is then shown that this set of k-tuples denoted by A is a linear algebra of order k. The purpose of showing the set A is a linear algebra of order k is to make an isomorphism between the set A and the algebra of k x k matrices. This isomorphism will greatly simplify the task of finding the generator of any particular sequence.

In Chapter III an isomorphism is shown between the defining linear recurrence relation and a set of infinite degree polynomials defined as a ratio of finite degree polynomials.

In Chapter IV the infinite periodic sequence is defined and it is shown that there are always infinite sequences which are solutions of the defining linear recurrence relation whose characteristic number is the principal period of the defining recurrence.

Chapter V gives a brief outline of extension fields and the root fields of polynomials of prime characteristic so that a synthesis procedure might be developed in Chapter VI for finding the minimum degree generator of a given sequence.

CHAPTER II

THE DEFINING LINEAR RECURRING RELATION AND SOME PROPERTIES OF ITS SOLUTIONS

For $k \geq 0$, let $a_0, a_1, \ldots, a_k$ be elements belonging to I_p, the field of integers modulo p, where p is a prime, with $a_0 a_k \neq 0$. Denote the set of all sequences $\{x_i\}_{i=0}^{\infty}$ satisfying the relationship

$$\sum_{j=0}^{k} a_j x_{i-j} = 0 \ (i = k, k+1, \ldots\ ) \qquad (2.1)$$

by $G = G(a_0, a_1, \ldots, a_k)$, where $x_i \in I_p$ and $x_i = 0$ for $i < 0$.

Now the set G contains p^k members, since each of the first k initial terms, x_i $(i = 0, 1, \ldots, k-1)$, of a sequence $\{x_i\}_{i=0}^{\infty}$ may be chosen in the field I_p in p ways and the remaining terms of the sequence $\{x_i\}_{i=0}^{\infty}$ are then determined by the recurrence relation

$$x_i = -a_0^{-1} \sum_{j=1}^{k} a_j x_{i-j} \ (i = k, k+1, \ldots\ ). \qquad (2.2)$$

The elements of G are said to be the (linear recurring) sequences generated by the (k+1)-tuple of a_i's; i.e., $a_0, \ldots, a_k$ generate the set G. (11, p. 31)

Let the first k elements of a solution, $\{x_i\}_{i=0}^{\infty}$, of (2.1); i.e., an element of G, be associated with the k-tuple $(x_0, \ldots, x_{k-1})$ which will be denoted by (x_k). There are p^k such k-tuples with elements belonging to I_p satisfying (2.1), hence all k-tuples with elements belonging to I_p satisfy (2.1). Now each such k-tuple (x_k) is unique, thus letting the first k terms of a sequence $\{x_i\}_{i=0}^{\infty}$ be those of such a k-tuple, uniquely determines a solution $\{x_i\}_{i=0}^{\infty}$ of (2.1). A one-to-one correspondence may be set up between the set of all such k-tuples with elements in I_p and the set G, i.e., all sequences $\{x_i\}_{i=0}^{\infty}$ satisfying (2.1). Denote this set of k-tuples by A.

To illustrate the linear recurring relationship of (2.1) consider as an example the sequence of $\{x_i\}_{i=0}^{\infty}$ generated by the 4-tuple $(a_0,a_1,a_2,a_3) = (1,2,1,1)$ and the 3-tuple of initial values $(x_0,x_1,x_2) = (1,2,2)$, where $a_i,x_i \in I_p$ and $k = 3$. With these specifications the equations (2.1) become

$$\begin{array}{llll}
1x_3 & + 2x_2 & + 1x_1 & + 1x_0 = 0, \\
1x_4 & + 2x_3 & + 1x_2 & + 1x_1 = 0, \\
1x_5 & + 2x_4 & + 1x_3 & + 1x_2 = 0, \\
\multicolumn{4}{l}{\cdots\cdots\cdots\cdots\cdots\cdots,} \\
1x_{n+3} & + 2x_{n+2} & + 1x_{n+1} & + 1x_n = 0, \\
\text{etc.}
\end{array} \tag{2.3}$$

The following system of equations is obtained from (2.3) by solving for the x_i's $(i = 3,4,5,\ldots)$.

$$\begin{array}{llll}
x_3 = -(2x_2 & + 1x_1 & + 2x_0 &), \\
x_4 = -(2x_3 & + 1x_2 & + 2x_1 &), \\
x_5 = -(2x_4 & + 1x_3 & + 2x_2 &), \\
\multicolumn{4}{l}{\cdots\cdots\cdots\cdots\cdots\cdots,} \\
x_n = -(2x_{n-1} & + 1x_{n-2} & + 2x_{n-3} &), \\
\text{etc.}
\end{array} \tag{2.4}$$

The solution, $\{x_i\}_{i=0}^{\infty}$, may be obtained from the system of equations (2.4). Substitution of the assumed values $x_0 = 1$, $x_1 = 2$, and $x_2 = 2$ into the first equation of (2.4) determines the value $x_3 = 2$.

Having obtained x_3 we may solve for x_4 using the second equation of (2.4). If continuing in this manner indefinitely the solution, $\{x_i\}_{i=0}^{\infty}$ would be obtained. It is this property; i.e., the recurrence of the x_i's $(i<n)$ in determining the n^{th} term of the sequence, that leads us to call equation (2.1) a recursive relation. (6, p. 28) After solving for a finite number of terms, it is realized the sequence in this example becomes repetitive. In fact, all sequences which are solutions of (2.1) be come repetitive. Since, all that is necessary for a solution, $\{x_i\}_{i=0}^{\infty}$ with the initial k terms $x_0,x_1,\ldots,x_{k-1}$, to become repetitive is that some k consecutive terms previously used, occur again later in the sequence. Now, some k consecutive terms must always re-occur later in the sequence. Since there only p^k such k-tuples over the field I_p, suppose that the first p^k terms of a sequence $\{x_i\}_{i=0}^{\infty}$ are elements of the field I_p such that no k consecutive terms re-occur up to and including the $(p^k)^{th}$ term; i.e., $\{x_0,x_1,\ldots,x_{pk-1},\ldots\}$ $x_i \in I_p$ where $(x_i,x_{i+1},\ldots,x_{i+k}) \neq (x_{i+t},x_{i+t+1},\ldots,x_{i+t+k})$ for $0 \leq i \leq (p^k-(k+1))$. Now with these conditions we realize that there are at most only $(k-1)$ k-tuples which are not included in the first p^k terms of the sequence. And that if the terms of any k-tuple $(x_{pk},x_{pk+1},x_{pk+2},\ldots,x_{pk+k})$ where to comprise the next k terms of the sequence, then the sequence must at least repeat some k consecutive terms upon reaching the $(p^k+k)^{th}$ term, since all p^k k-tuples have definitely occurred by the $(p^k+(k-1))^{th}$ term. In fact, the number of terms in which a sequence $\{x_i\}_{i=0}^{\infty}$, a solution of (2.1), must become repetitive is at most p^k. A result of this argument is summarized in

Chapter IV, Theorem 4.4, after a periodic sequence is defined. The solution to the example given above is $\{1,2,2,2,1,0,0,1,1,0,1,0,2,1,2,2,\ldots\}$, which begins repeating after the thirteenth term.

Now recalling that the set A is the set of k-tuples whose elements are the first k elements of a solution to the defining recurrence relation (2.1), define operations of sum on A to be

$$(u_k) + (v_k) = (u_k + v_k) \tag{2.5}$$

and scalar product to be

$$c(v_k) = (cv_k), \tag{2.6}$$

where $c \in I_p$ and $(u_k),(v_k) \in A$. The operations are obviously closed since these are the ordinary operations defined for k-tuples over a field. The identity element for the operation of addition is $(0) = (0,0,\ldots,0)$, and the additive inverse of (u_k) is $-(u_k) = (-u_k)$ which is defined to be $(-u_0,-u_1,\ldots,-u_k)$. Furthermore, it is evident that addition is commutative and associative. Therefore A is an Abelian group with respect to addition, and for $c,d \in I_p$, $c(v_k + u_k) = (cv_k) + (cu_k)$, $(c + d)(v_k) = (cv_k) + (dv_k)$. Also $(cd)(v_k) = c(dv_k)$ and $1(v_k) = (v_k)$. (9, p. 137)

Hence, according to the following definition, A is a vector space.

Definition 2.1. A "vector space" V over a field F consists of a nonempty set of elements, called vectors, such that for any two vectors $X,Y \in V$ the sum $X + Y$ is a unique vector of V, and for any scalar $a \in F$, the scalar product $aX \in V$. The set V is then called "a vector space over the field F" if V has the following properties:

(i) V is an Abelian group with respect to addition,

(ii) $a(X + Y) = aX + aY, \quad a \in F; X, Y \in V,$

(iii) $(a + b)X = aX + bX, \quad a, b \in F; X \in V,$

(iv) $a(bX) = (ab)X, \quad a, b \in F; X \in V,$

(v) $1X = X, \quad$ 1 the unity of F.

The following is a definition of a linear algebra.

Definition 2.2. A "linear algebra" is a set of elements K which forms a vector space over a field F and which has defined an associative and bilinear multiplication, that is

(i) $\alpha(\beta\gamma) = (\alpha\beta)\gamma, \quad \alpha, \beta, \gamma \in K,$

(ii) $\alpha(c\beta + d\gamma) = c(\alpha\beta) + d(\alpha\gamma), \quad \alpha, \beta, \gamma \in K; c, d \in F,$

(iii) $(c\alpha + d\beta)\gamma = c(\alpha\gamma) + d(\beta\gamma), \quad \alpha, \beta, \gamma \in K; c, d \in F.$

K has a unity element δ if there exists $\delta \in K$ such that $\delta\alpha = \alpha = \alpha\delta$ for all $\alpha \in K$. The "order" of a linear algebra K is the dimension of K when K is considered as a vector space over the field F.

Now on the set of elements contained in A define multiplication as

$$(v_k) * (u_k) = (v_0, \ldots, v_i, \ldots, v_{k-1}) * (u_0, \ldots, u_i, \ldots, u_{k-1})$$
$$= (v_0\boxed{u_0}, \ldots, \sum_{j=0} v_{i-j}u_j, \ldots, v_{k-1}u_0 + \ldots + v_0u_{k-1}). \quad (2.7)$$

Since the elements u_i and v_i are elements of a field, it follows that the above operation is closed. Now it is easily shown that multiplication * is commutative and associative and satisfies the two postulates of bilinear multiplication in definition 2.2.

Defining the unity $\delta = (1,0,0,\ldots,0)$, it is obvious from the definition of * that

$$\begin{aligned}(1,0,0,\ldots,0) * (u_0,u_1,\ldots,u_{k-1}) &= (u_0,u_1,\ldots,u_{k-1}) * (1,0,0,\ldots,0)\\ &= (u_0,u_1,\ldots,u_{k-1})\end{aligned}$$

Consequently all of the postulates of a linear algebra are satisfied.

Hence we have the following theorem.

Theorem 2.1. The set A of k-tuples defined by the correspondence $(x_0,x_1,\ldots,x_{k-1}) \longleftrightarrow \{x_i\}_{i=0}^{\infty}$, where $\{x_i\}_{i=0}^{\infty}$ is a solution of (2.1), forms a commutative linear algebra with unity for the three operations defined by (2.5),(2.6) and (2.7).

Definition 2.3. An isomorphism between two algebraic systems B and B' is a correspondence between B and B'. That is, if $\alpha,\beta \in B$, $\alpha',\beta' \in B'$, and the correspondence is $\alpha \longleftrightarrow \alpha'$, $\beta \longleftrightarrow \beta'$, with the operation in B denoted by $\textcircled{1}$ and the operation in B' denoted by $\oplus$, then

$$(\alpha \ \textcircled{1}\ \beta)' = \alpha' \oplus \beta'.$$

Theorem 2.2. Every linear algebra of order k, with unity is isomorphic to an algebra of k x k matrices. (4, pp. 216-217)

Theorem 2.3. The correspondence of

$$(u_0,u_1,\ldots,u_{k-1}) \longleftrightarrow U = [u_{ij}] = \begin{bmatrix} u_0 & ,0 & ,0 & ,\ldots,0 \\ u_1 & ,u_0 & ,0 & ,\ldots,0 \\ u_2 & ,u_1 & ,u_0 & ,\ldots,0 \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ u_{k-1} & ,u_{k-2} & ,u_{k-3} & ,\ldots,u_0 \end{bmatrix} \tag{2.8}$$

(where $u_{ii} = u_0$, etc., as defined by (2.8)) and

$$(1,0,0,\ldots,0) \longleftrightarrow I = \delta_{ij}, \text{ with}$$

$$\delta_{ij} = \begin{Bmatrix} 0, \text{ if } i \neq j \\ 1, \text{ if } i = j \end{Bmatrix}$$

defines an isomorphism between A and the k x k matrices of type U.

Proof. The correspondence is obviously one-to-one onto. Consider

$$(u_k) + (v_k) \longleftrightarrow U + V$$

by definition of matrix addition

$$U + V = [u_{ij}] + [v_{ij}] = [u_{ij} + v_{ij}]$$

which corresponds to $(u_k + v_k)$. Now

$$c(v_k) = (cv_k) \longleftrightarrow [cv_{ij}] = c[v_{ij}] = cV.$$

Therefore addition and scalar multiplication are preserved.

Suppose (u_k) and (v_k) belong to A. Now if multiplication $*$ is preserved under the correspondence then $(u_k) * (v_k) \longleftrightarrow UV$ where U and V are defined according to (2.8). Let $W = UV = [w_{ij}]$. Consider w_{ij} located in the i^{th} row and j^{th} column of W. Now the element w_{ij} is the result of the matrix multiplication of the i^{th} row of U and the j^{th} column of V, which according to the definition of matrix multiplication can be expressed

$$w_{ij} = \sum_{n=1}^{k} u_{in}v_{nj}.$$

But according to the correspondence (2.8) $u_{in} \longleftrightarrow u_{i-n}$ and $v_{nj} \longleftrightarrow v_{n-j}$ where the terms $u_{i-n} = 0$ for $n = i+1,\ldots,k$ and $v_{n-j} = 0$ for $n = 1,2,\ldots,j-1$. Thus

$$w_{ij} = \sum_{n=j}^{i} u_{i-n}v_{n-j}.$$

Now for a change of variables let $n-j = r$, then

$$w_{ij} = \sum_{r=0}^{s} u_{(i-j)-r}v_r.$$

For all $i < j$, $w_{ij} = 0$ and $w_{ii} = u_0v_0$. The subdiagonal elements

$$w_{i,i-1} = u_1v_0 + u_0v_1$$

and in general

$$w_{i,i-s} = \sum_{r=0}^{s} u_{s-r}v_r.$$

But these are the elements of W defined by (2.8) where

$$(u_k) * (v_k) = (w_k) = (u_0v_0, \ldots, \sum_{j=0}^{i} u_{i-j}v_j, \ldots).$$

Hence multiplication is preserved under this mapping. This concludes the proof of Theorem 2.3.

CHAPTER III

POLYNOMIAL GENERATING CONCEPT OF LINEAR RECURRING SEQUENCES

A one-to-one correspondence between the generating $(k+1)$-tuple $(a_0,\ldots,a_k)$, which generates G through the relation (2.1), and the polynomial $f(z)$ of degree k with $f(0) \neq 0$ may be established by the following

$$(a_0,\ldots,a_k) \longleftrightarrow f(z) = a_0 + a_1 z + \ldots + a_k z^k. \qquad (3.1)$$

Now any sequence $\{x_i\}_{i=0}^{\infty}$ satisfying (2.1) can be placed in a 1-1 correspondence with an infinite degree polynomial in z; i.e.,

$$\{x_i\}_{i=0}^{\infty} \longleftrightarrow h(z) = \sum_{i=0}^{\infty} x_i z^i. \qquad (3.2)$$

Let $G(f)$ denote the set of infinite degree polynomials generated by $g(z)/f(z)$ which is defined to be

$$G(f) = \Big\{ g(z)/f(z) \mid d(f(z)) = k \text{ and } d(g(z)) < k \text{ where } f,g \in I_p[z] \Big\}. \qquad (3.3)$$

<u>Theorem 3.1</u>. The set $G(f)$ is identical with $G(a_0,\ldots,a_k)$ through correspondence (3.2). (11, p. 33)

<u>Proof</u>. Suppose that $g(z) \in I_p[z]$ with $d(g(z)) < k$. Now the ratio

$$g(z)/f(z) = \sum_{i=0}^{\infty} x_i z^i = h(z) \text{ with } x_i \in I_p.$$

Then $g(z) = f(z)h(z) = \left(\sum_{r=0}^{k} a_r z^r\right)\left(\sum_{s=0}^{\infty} x_s z^s\right) = \sum_{i=0}^{\infty}\left(\sum_{j=0}^{k} x_{i-j} a_j\right) z^i.$

Now since $d(g(z)) < k$, then $\sum_{j=0}^{k} x_{i-j}a_j = 0$ $(i = k, k+1, \ldots)$. Therefore the sequence $\{x_i\}_{i=0}^{\infty}$ formed by the coefficients of $h(z)$ satisfies (2.1). Hence the set of all elements of $G(f)$ when considered as sequences is a subset of $G(a_0, \ldots, a_k)$. Now since both $G(f)$ and $G(a_0, \ldots, a_k)$ contain p elements and $G(f)$ is a subset of $G(a_0, \ldots, a_k)$, they must be identical within the correspondence (3.2).

Note that (3.2) is merely an abstract correspondence between sequences and infinite degree polynomials. And $f(z)$ is the generating polynomial of the long division process $g(z)/f(z)$ justified by Theorem 3.1, i.e., the polynomial generation of $G(f)$ is identical with $G(a_0, \ldots, a_k)$ generated by (2.1).

The following theorem proves the algebraic structure of $G(f)$ is a vector space.

Theorem 3.2. The set $G(f) = \{g(z)/f(z)\}$ defined by (3.3) forms a vector space.

Proof. Any two sequences $\{u_i\}_{i=0}^{\infty}$ and $\{h_i\}_{i=0}^{\infty}$ belonging to $G(f)$ have polynomial representations of $g(z)/f(z)$ and $q(z)/f(z)$, respectively, where $g(z) = \sum_{i=0}^{k-1} g_i z^i$, and $q(z) = \sum_{i=0}^{k-1} q_i z^i$, if the $d(f(z)) = k$. Now if we consider $g(z)/f(z)$ and $q(z)/f(z)$ as vectors defined over the field I_p, then sum of these two vectors is taken to be

$$\frac{g(z)}{f(z)} + \frac{q(z)}{f(z)} = \frac{\sum_{i=0}^{k-1} (g_i + q_i)z^i}{f(z)}$$

which is a unique vector of $G(f)$. Now it is evident that the vectors of $G(f)$ form an Abelian group with respect to addition and that the postulates of Definition 2.1 are satisfied if the field F is I_p. Hence $G(f)$ is a vector space.

CHAPTER IV

PERIODIC PROPERTIES

Definition 4.1. An infinite sequence of elements which after a finite number of terms, say s, becomes repetitive in the following sense

$$(u_0, u_1, \ldots, u_{s-1}, u_s, u_{s+1}, \ldots, u_{s+t-1}, u_s,$$
$$u_{s+1}, \ldots, u_{s+t-1}, \ldots)$$

will be defined as a "periodic sequence " of period t.

The least period of a periodic sequence $\{u_i\}_{i=0}^{\infty}$ is said to be the "characteristic number" of $\{u_i\}_{i=0}^{\infty}$--all other periods are multiples of this least period. (10, p. 600)

The "numeric" of $\{u_i\}_{i=0}^{\infty}$ is the number of nonrepeating terms at the begining of the sequence.

If the numeric of a sequence $\{u_i\}_{i=0}^{\infty}$ is zero, then $\{u_i\}_{i=0}^{\infty}$ is said to be "purely periodic."

A number which is a period of every sequence satisfying the difference equation (2.1) is said to be a "general period."

Let t be the least such general period and call it the "principal period" of (2.1).

Theorem 4.1. There are always solutions of (2.1) whose characteristic number is the principal period of (2.1). (10, pp. 603-604)

Proof. Suppose that $\{u_i\}_{i=0}^{\infty}$ and $\{v_i\}_{i=0}^{\infty}$ are any two distinct solutions of (2.1). If there are elements $b_1, b_2, \ldots, b_k$ belonging to

I_p which satisfy

$$u_m = b_1 v_m + b_2 v_{m+1} + \dots + b_k v_{m+k-1}, \qquad (4.1)$$

$(m = 0,1,2,\dots)$, then the characteristic number of $\{v_i\}_{i=0}^{\infty}$ is a multiple of the characteristic number of $\{u_i\}_{i=0}^{\infty}$. Because of the linear recurring nature of the elements beyond the first k elements of any solution of (2.1) and because the equations resulting from (4.1) are linear, it is only necessary to consider the first k equations of (4.1).

The linear simultaneous set of equations in matrix form

$$\begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ \cdot \\ \cdot \\ \cdot \\ u_{k-1} \end{bmatrix} = \begin{bmatrix} v_0 & v_1 & v_2 & \dots & v_{k-1} \\ v_1 & v_2 & v_3 & \dots & v_k \\ v_2 & v_3 & v_4 & \dots & v_{k+1} \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ v_{k-1} & v_k & v_{k+1} & \dots & v_{2k-1} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \cdot \\ \cdot \\ \cdot \\ b_k \end{bmatrix} \qquad (4.2)$$

has a unique solution for the b_i's if and only if the determinant of the coefficient matrix is nonzero.

Now consider the sequence $\{v_i\}_{i=0}^{\infty}$ whose first k components are $(v_k) = (1,0,0,\dots,0)$. The coefficient matrix of (4.2) becomes

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & v_k \\ 0 & 0 & 0 & \dots & v_k & v_{k+1} \\ \cdot & & & & & \\ \cdot & & & & & \\ \cdot & & & & & \\ 0 & v_k & v_{k+1} & \dots & v_{2k-2} & v_{2k-1} \end{bmatrix} \qquad (4.3)$$

and its determinant $(v_k)^{k-1}(-1)^k$ is nonzero. Since

$$v_k = -a_0^{-1} \sum_{j=1}^{k} v_{k-j} a_j = -a_0^{-1} a_k$$

is nonzero by hypothesis of (2.1). Thus for this sequence $\{v_i\}_{i=0}^{\infty}$, (4.2) determines a unique solution for the b_i's. In fact, if (4.3) is the coefficient matrix of (4.2) there is a unique solution of b_i's for every solution $\{u_i\}_{i=0}^{\infty}$ of (2.1). Now according to the original statement of the argument the characteristic number of $\{v_i\}_{i=0}^{\infty}$ is a multiple of the characteristic number of $\{u_i\}_{i=0}^{\infty}$ if there are elements $b_1, b_2, \ldots, b_k$ satisfying (4.1). We have shown that if (4.3) is the coefficient matrix of (4.2) there is a unique solution of b_i's for every $\{u_i\}_{i=0}^{\infty}$ divides the characteristic number of $\{v_i\}_{i=0}^{\infty}$. But the principal period of (2.1) is the smallest general period of every sequence satisfying (2.1), so it follows that the characteristic number of $\{v_i\}_{i=0}^{\infty}$ equals the principal period of (2.1). Thus Theorem 4.1 is proved, i.e., there is at least one solution of (2.1) whose characteristic number is the principal period of (2.1).

Let the first n terms of a sequence $\{u_i\}_{i=0}^{\infty}$, a solution of (2.1), be the coefficients of a polynomial u(z) of degree n-1, i.e.,

$$u(z) = u_0 + u_1 z + \ldots + u_{n-1} z^{n-1}. \qquad (4.4)$$

Now consider

$$\begin{aligned} f(z)u(z) = {} & \Big[(u_0 a_0) + (u_1 a_0 + u_0 a_1)z + \ldots \\ & + (u_{k-1} a_0 + \ldots + u_0 a_{k-1}) z^{k-1}\Big] \\ & + \Big[(u_k a_0 + \ldots + u_0 a_k) z^k \\ & + (u_{k+1} a_0 + \ldots + u_1 a_k) z^{k+1} + \ldots \\ & + (u_{n-1} a_0 + \ldots + u_{n-k-1} a_k) z^{n-1}\Big] \\ & + \Big[(u_{n-1} a_1 + \ldots + u_{n-k} a_k) z^n \\ & + (u_{n-1} a_2 + \ldots + u_{n-k+1} a_k) z^{n+1} + \ldots \\ & + (u_{n+k-1} a_k) z^{n+k-1}\Big] \end{aligned}$$

Note that the coefficients $\sum_{j=0}^{k} u_{i-j}a_j = 0$ for $i = k,k+1,\ldots,n-1$, so that the coefficients of $z^k, z^{k+1}, \ldots, z^{n-1}$ are zero.

Using this linear recurring relation, the coefficients of z^{n+s}, for $s = 0,1,\ldots,k-1$, may be expressed as follows:

$$\begin{aligned}
&(u_{n-1}a_{s+1} + \cdots + u_{n-k+s}a_k)z^{n+s} \\
&= z^{n+s}\sum_{j=s+1}^{k} u_{n+s-j}a_j \\
&= z^{n+s}\left[\sum_{j=0}^{k} u_{n+s-j}a_j\right] - z^{n+s}\left[\sum_{j=0}^{s} u_{n+s-j}a_j\right] \\
&= -z^{n+s}\left[\sum_{j=0}^{s} u_{n+s-j}a_j\right]
\end{aligned}$$

After applying this substitution $f(z)u(z)$ may be expressed in the following form.

$$\begin{aligned}
f(z)u(z) = &\left[(u_0a_0) + (u_1a_0 + u_0a_1)z + \cdots \right.\\
&\left. + (u_{k-1}a_0 + \cdots + u_0a_{k-1})z^{k-1}\right] \\
&-z^n\left[(u_na_0) + (u_{n+1}a_0 + u_na_1)z + \cdots \right.\\
&\left. + (u_{n+k-1}a_0 + \cdots + u_na_{k-1})z^{k-1}\right]
\end{aligned}$$

Denote the two polynomials in brackets by $u'(z)$ and $u''(z)$, respectively. Then

$$f(z)u(z) = u'(z) - z^n u''(z)$$

But $\quad f(z)u(z) \equiv 0 \pmod{f(z)}$

Therefore $\quad u'(z) - z^n u''(z) \equiv 0 \pmod{f(z)} \qquad (4.5)$

Now the following theorem can be proved.

Theorem 4.2. (Fundamental Theorem on Purely Periodic Sequences.) Let

$$u(z) = (u_0a_0) + (u_1a_0 + u_0a_1)z + \dots$$
$$+ (u_{k-1}a_0 + \dots + u_0a_{k-1})z^{k-1}$$
$$= \sum_{i=0}^{k-1} \sum_{j=0}^{i} u_{i-j}a_jz^i$$

where the u_i are the first k-1 terms of a sequence $\{u_i\}_{i=0}^{\infty}$ satisfying (2.1), and let f(z) be the polynomial associated with (2.1). Then $\{u_i\}_{i=0}^{\infty}$, a solution to the linear difference equation (2.1), is purely periodic with a period of n if and only if

$$(1 - z^n)u(z) \equiv 0 \pmod{f(z)}. \quad (10, \text{ p. } 606) \qquad (4.6)$$

<u>Proof</u>. If $\{u_i\}_{i=0}^{\infty}$ is purely periodic with period n, then

$$u''(z) = u'(z) \text{ since } u_0 = u_n,\ u_1 = u_{n+1}, \text{ etc.}$$

Then (4.5) becomes

$$(1 - z^n)u'(z) \equiv 0 \pmod{f(z)}$$

Conversely, suppose that there exists an n such that this congruence holds, then equating congruence (4.5) and (4.6) leads to the conclusion that $u'(z) = u''(z)$. Furthermore two polynomials in z are equal if coefficients of like powers of z are equal. This, of course implies $u_0 = u_n$, $u_1 = u_{n+1}$, etc. Therefore if (4.6) holds, $\{u_i\}_{i=0}^{\infty}$ is purely periodic of period n.

<u>Corollary 4.2</u>. Assume that $\{u_i\}_{i=0}^{\infty}$ is purely periodic. Then the least value of n such that congruence (4.6) is satisfied is the characteristic number of $\{u_i\}_{i=0}^{\infty}$. (10, p. 607)

<u>Theorem 4.3</u>. All sequences $\{u_i\}_{i=0}^{\infty}$ satisfying (2.1) where $u_i, a_i \in I_p$ are necessarily purely periodic. Furthermore, the principal period of (2.1) is the value of n for which $(z^n - 1) \equiv 0 \pmod{f(z)}$. (10, p. 607-608)

Proof. According to Theorem 3.1 the correspondence

$$\{u_i\}_{i=0}^{\infty} \longleftrightarrow u(z) = \sum_{i=0}^{\infty} u_i z^i = g(z)/f(z)$$

is an equivalent generating process to (2.1). Then

$$g(z) = \sum_{i=0}^{\infty}\left(\sum_{j=0}^{k} u_{i-j} f_j\right) z^i$$

which implies

$$g_i = \sum_{j=0}^{k} u_{i-j} f_j \text{ for } i = 0,\ldots,k-1. \tag{4.7}$$

Comparing (4.7) with the coefficients of u'(z) of Theorem 4.2 results in

$$g(z) = u'(z).$$

Then

$$\begin{aligned}(1 - z^n)u'(z) &= (1 - z^n)g(z)\\ &= (1 - z^n)u(z)f(z) \equiv 0 \pmod{f(z)}.\end{aligned}$$

Hence congruence (4.6) always holds for those $\{u_i\}_{i=0}^{\infty}$ defined by the hypothesis of the theorem, and by Theorem 4.2 the sequences $\{u_i\}_{i=0}^{\infty}$ are all purely periodic.

Since all sequences of G(f) are purely periodic, then there exists a sequence of G(f) whose characteristic number is the principal period of (2.1) (Theorem 4.1).

If a sequence is purely periodic, then (4.6) holds which becomes for this sequence

$$(1 - z^n)(f_0 + f_1 z + \ldots + f_{k-1} z^{k-1}) \equiv 0 \pmod{f(z)}.$$

This congruence may be expressed in the following form

$$(1 - z^n)f(z) \equiv (1 - z\ )f_k z^k \pmod{f(z)}. \tag{4.8}$$

The left side of (4.8) is congruent to zero. Now since $f_k \neq 0$ by assumption in definition (2.1) and z^k and $f(z)$ are relatively prime, then (4.6) becomes

$$(z^n - 1) \equiv 0 \pmod{f(z)}. \tag{4.9}$$

Then from Corollary 4.2 it follows that the least value of n such that (4.6) is satisfied is the principal period of (2.1). This completes the proof of the second part of the theorem. Consequently $z^n - 1$ is the smallest degree of such type polynomials for which $f(z) \mid z^n - 1$. This least n is defined as the "period" of the polynomial f(z) which will be represented by p(f). Thus the period of a polynomial f(z) is the principal period of all sequences in G(f) generated by f(z).

Denote the characteristic number of a sequence $\{u_i\}_{i=0}^{\infty}$ by p(u), which is sometimes called the period of the sequence $\{u_i\}_{i=0}^{\infty}$. Now the following may be concluded from the definition of a principal period of G(f) and the definition of the characteristic number of every $\{u_i\}_{i=0}^{\infty} \in G(f)$.

Corollary 4.3.1. For every $\{u_i\}_{i=0}^{\infty}$ G(f), $p(u) \mid p(f)$.

Corollary 4.3.2. $p(f) = \max\left\{p(u) \mid \{u_i\}_{i=0}^{\infty} \in G(f)\right\}$

The following theorem summarizes the argument on page 8 concerning the maximum period, or i.e., the maximum number of elements before which a sequence becomes repetitive.

Theorem 4.4. For every $\{u_i\}_{i=0}^{\infty} \in G(f)$, $p(u) \leq p^k$.

Sufficient concepts and background have now been developed to further consider some periodic properties of polynomials which generate the sequences of $G(f)$.

Theorem 4.5. Let the $G(f_i) = \left\{g_{ij}(z)/f_i(z)\right\}$ as defined by (2.3) be n vector spaces ($i = 1,2,\ldots,n$) over I_p.

Then the sum vector space is given by

$$\sum_{i=1}^{n} G(f_i) = \left\{g_j(z)/f(z)\right\} = G(f) \qquad (4.10)$$

where $f(z) = \text{l.c.m.}\left[f_1(z),f_2(z),\ldots,f_n(z)\right]$.

Proof. A member of the sum vector space $\sum_{i=1}^{n} G(f_i)$ is of type

$$\sum_{i=1}^{n} \frac{k_i g_{ij}(z)}{f_i(z)}$$

where the k_i's are over I_p. Reducing to a common denominator, the typical element becomes

$$\sum_{i=1}^{n} \frac{k_i r_i(z) g_{ij}(z)}{f(z)}$$

with $f(z) = \text{l.c.m.}\left[f_1(z),f_2(z),\ldots,f_n(z)\right]$ and $r_i(z) = f(z)/f_i(z)$.

Let $g_j(z) = \sum_{i=1}^{n} k_i r_i(z) g_{ij}(z)$.

Also denote the degree of a polynomial $s(z)$ by $\deg(s(z))$ or $d(s)$ when no confusion arises.

Then

$$\begin{aligned}\deg(g_j(z)) &\leq \max \deg(r_i(z)g_{ij}(z))\\ &= \max \deg(f(z)g_{ij}(z)/f_i(z)) < \deg(f(z)),\end{aligned}$$

since $\deg(g_{ij}(z)) < \deg(f_i(z))$ by definition.

Hence $(g_j(z)/f(z)) \in G(f)$, so that

$$\sum_{i=1}^{n} G(f_i) \subset G(f).$$

But since

$$\sum_{i=1}^{n} G(f_i) = g_j(z)/f(z)$$

is a vector space, $g_j(z)$ must of necessity range over all possible polynomials over I_p of degree up to and including $d(f(z)) - 1$.

Thus $\sum_{i=1}^{n} G(f_i)$ contains exactly $p^{d(f)}$ elements which is exactly the same number of elements in $G(f)$. Therefore

$$\sum_{i=1}^{n} G(f_i) = G(f)$$

where $f(z) = \text{l.c.m.}\left[f_1(z), f_2(z), \ldots, f_n(z)\right]$.

<u>Corollary 4.5.1</u>. If $(f_1, f_2) = 1$, then $G(f_1) + G(f_2) = G(f_1 f_2)$. This follows from Theorem 4.5 since if $(f_1, f_2) = 1$, then $\text{l.c.m.}(f_1, f_2) = f_1 f_2$. Furthermore, if $(f_i, f_j) = 1$ for $i, j = 1, 2, \ldots, n$ and $i \neq j$, then $\text{l.c.m.}\left[f_1, f_2, \ldots, f_n\right] = f_1 f_2 \ldots f_n$. Hence an extension of Corollary 4.5.1 is

<u>Corollary 4.5.2</u>. If $(f_i, f_j) = 1$ for $i, j = 1, 2, \ldots, n$ and $i \neq j$, then

$$\sum_{i=1}^{n} G(f_i) = G(\prod_{i=1}^{n} f_i).$$

Corollary 4.5.3. Let $g(z)f(z) \neq 0$. A necessary and sufficient condition for $G(f)$ to be a subset of $G(g)$ is that $f(z) \mid g(z)$.

Proof. Suppose $G(f) \subset G(g)$. Now since $G(f)$ is a subspace of $G(g)$, then $G(f) + G(q) = G(g)$ for some $q(z)$, so that $g = \text{l.c.m.}(f,q)$ by Theorem 4.5. Therefore $f(z) \mid g(z)$. Conversely, if $f(z) \mid g(z)$, then $g(z) = s(z)f(z)$ for some polynomial $s(z)$. Now consider any $\{u_i\}_{i=0}^{\infty} \in G(f)$, then for some polynomial $p(z)$, $u(z) = p(z)/f(z)$.

But then $u(z) = \frac{p(z)s(z)}{f(z)s(z)} = \frac{p(z)s(z)}{g(z)}$ which is an element of $G(g)$. Therefore $G(f) \subset G(g)$.

Theorem 4.6. $z^s - 1 \mid z^t - 1$ if and only if $s \mid t$ for $s,t > 0$. (11, p. 36)

Proof. If $s \mid t$, then $z^t - 1 = (z^s - 1)(z^{t-s} + z^{t-2s} + \ldots + 1)$. Thus we have the desired conclusion, $z^s - 1 \mid z^t - 1$. Conversely, if $z^s - 1 \mid z^t - 1$, then $G(z^s - 1) \subset G(z^t - 1)$ (Corollary 4.5.3). Now let $\{u_i\}_{i=0}^{\infty} \in G(z^s - 1)$ with $p(u) = s$, the principal period of $G(z^s - 1)$. Every sequence belonging to $G(z^t - 1)$ has a period that divides $p(z^t - 1) = t$. Hence $s \mid t$.

Theorem 4.7. If $f(z) \mid g(z)$, then $p(f) \mid p(g)$.

Proof. If $f(z) \mid g(z)$, then $G(f) \subset G(g)$ by Corollary 4.5.3. All $\{u_i\}_{i=0}^{\infty} \in G(f)$ have $p(u) \mid p(f)$, and for all such $\{u_i\}_{i=0}^{\infty}$, $p(u) \mid p(g)$. Since $\{u_i\}_{i=0}^{\infty} \in G(f) \subset G(g)$ and according to Corollary 4.3.1 $p(u) \mid p(g)$ for every $\{u_i\}_{i=0}^{\infty} \in G(g)$. Now suppose $\{v_i\}_{i=0}^{\infty} \in G(f)$ with $p(v) = p(f)$. The existence of such a sequence $\{v_i\}_{i=0}^{\infty}$ is guaranteed by Theorem 4.1. Then $p(v) = p(f)$ and $p(v) \mid p(g)$. Thus the desired conclusion $p(f) \mid p(g)$.

Corollary 4.7.1. A polynomial $f(z) \mid z^t - 1$ if and only if $p(f) \mid t$. (11, p. 36)

Proof. If $f(z) \mid z^t - 1$, then $p(f) \mid p(z^t - 1) = t$ by Theorem 4.6. But $f(z) \mid z^{p(f)} - 1$ (Theorem 4.3) and by the transitive property of divides, $f(z) \mid z^t - 1$.

Theorem 4.8. The set $G(z^t - 1)$ contains all the sequences of period t and all other sequences of periods t_i which divide t.

Proof. The set $G(z^t - 1)$ contains all of the sequences satisfying (2.1) through the correspondence (3.1) and (3.2) where $f(z) = z^t - 1$. There are p^t distinct sequences satisfying (2.1) so that $G(z^t - 1)$ has p^t distinct members. For every $\{u_i\}_{i=0}^{\infty} \in G(z^t - 1)$, $p(u) \mid t$.

The total number of distinct sequences of length t over I_p are p^t in number. If these p^t sequences of length t are repeated periodically, then this set of p^t sequences are all possible distinct sequences over I_p of period t and all other sequences of t_i which divide t. Hence $G(z^t - 1)$ contains all sequences of periods t_i that divide t.

Theorem 4.9. Every periodic sequence $\{u_i\}_{i=0}^{\infty} \in G(f)$ also belongs to a unique smallest set $G(g)$ where $(g_1, g) = 1$ if $g_1(z)/g(z)$ generates $\{u_i\}_{i=0}^{\infty}$. Furthermore $p(u) = p(g)$.

Proof. By assumption, $\{u_i\}_{i=0}^{\infty} \in G(f)$ so there is a polynomial $f_1(z)$ such that $d(f_1) < d(f)$ for which $f_1(z)/f(z) = u(z)$. Suppose $(f_1, f) = d$, then there are polynomials $g_1(z)$ and $g(z)$ with $d(g_1) < d(g)$ such that $f_1(z) = d(z)g_1(z)$ and $f(z) = d(z)g(z)$.

Hence

$$\frac{f_1(z)}{f(z)} = \frac{d(z)g_1(z)}{d(z)g(z)} = \frac{g_1(z)}{g(z)} = u(z) \text{ with } (g_1,g) = 1.$$

Now by (3.3) $\{u_i\}_{i=0}^{\infty} \in G(g)$, which by Corollary 4.5.3. is a subset of G(f) since $g(z) \mid f(z)$.

The degree of g(z) determines the number of elements in G(g). Since if d(g) = k, then there are p^k elements in G(g).

To show that G(g) is unique and the smallest set containing $\{u_i\}_{i=0}^{\infty}$, suppose $\{u_i\}_{i=0}^{\infty} \in G(h)$ where $d(h) < d(g)$. Then there is an $h_1(z)$ such that $h_1(z)/h(z) = u(z)$. Also $u(z) = g_1(z)/g(z)$ from which it follows that $h(z)g_1(z) = h_1(z)g(z)$, implying that $g(z) \mid h(z)$. This is only possible if g(z) and h(z) differ by a constant multiple in which case G(g) = G(h). Hence for every $\{u_i\}_{i=0}^{\infty} \in G(f)$ there exists a unique smallest G(g) and the generator $g_1(z)/g(z)$ of the sequence $\{u_i\}_{i=0}^{\infty}$ has the property that $(g_1,g) = 1$.

To show p(u) = p(g), consider $G(z^{p(u)} - 1)$. The sequence $\{u_i\}_{i=0}^{\infty}$ of period p(u) is an element of the set by Theorem 4.8. There exists a polynomial $f_1(z)$ such that $f_1(z)/(z^{p(u)} - 1) = u(z)$, which also equals $g_1(z)/g(z)$ with $(g_1,g) = 1$. Hence $g(z)f_1(z) = g_1(z)(z^{p(u)} - 1)$, from which it follows $g(z) \mid z^{p(u)} - 1$. Thus one may concluded from Theorem 4.7 that $p(g) \mid p(u)$. But since $\{u_i\}_{i=0}^{\infty}$ is an element of G(g), $p(u) \mid p(g)$, thus implying that p(u) = p(g). This concludes the proof of Theorem 4.9.

Analysis and synthesis require a knowledge of the root fields of the polynomials discussed in this chapter. The root fields of polynomials over I_p are suitable extension fields of I_p. Thus, Chapter V is an attempt to develop sufficient background material about extension fields in general so that the exact nature of the root fields of polynomials over I_p will follow naturally. However, since generators of infinite periodic sequences over the field I_p, are the topic of this thesis, the developement given is not too extensive.

CHAPTER V

EXTENSION FIELDS

I. DEFINING CONCEPTS AND PROPERTIES

Definition 5.1. A field K is said to be an "extension field" of the field F if F is a subfield of K. Notation: $F \subseteq K$.

For example, if R is the field of real numbers, then the field of complex numbers C is an extension field of R.

From the definition of an extension field K of a field F, it follows that K forms a vector space over the field F. If K forms an n-dimensional vector space over F, the extension field K over F is said to be of finite degree n over F.

Consider an element $k \in K$ and form all polynomials of the type $a(k) = a_0 + a_1 k + \dots + a_n k^n$ with all $a_i \in F$.

Define addition and multiplication in the usual way as for polynomials in an indeterminate z. This set of polynomials in k is closed with respect to addition and multiplication, and they form a polynomial domain in k denoted by $F[k]$. This set of polynomials forms a subdomain of K. The rational expressions of the type $a(k)/b(k)$ where $b(k) \neq 0$ may be formed as with the polynomials in an indeterminate z. Represent this system of rational expressions by F(k).

$F[k]$ is a subset of F(k) where $F[k]$ forms an integral domain. Every nonzero element $a(k)/b(k) \in F(k)$ obviously has an inverse. Consequently F(k) is a field, so that F(k) is an extension field of F.

Definition 5.2. If $k \in K$, then the extension field $F(k)$ formed by the single element k is called a "simple extension" of its subfield F. An element k of an extension field K over F is called "algebraic" if k satisfies a polynomial equation

$$a(k) = a_0 + a_1k + \ldots + a_nk^n = 0$$

with all $a_i \in F$ and not necessarily all $a_i \neq 0$. Otherwise k is called a "transcendental" element of K over F.

The following theorem indicates the nature of simple algebraic extensions if k is transcendental.

Theorem 5.1. If k is a transcendental element of K over F, then the simple algebraic extension $F(k)$ of F is isomorphic to the quotient field $F(z)$ of rational polynomials in an indeterminate z with coefficients in F. The correspondence is $k \longleftrightarrow z$ and $a \longleftrightarrow a$ for each a in F. (4, p. 375)

Theorem 5.2. Every "algebraic" element k of K over F is a root of a unique minimum degree irreducible polynomial

$$f(z) = f_0 + f_1z + \ldots + f_nz^n,\ f_n = 1;\ \text{i.e.,}$$

$f(z)$ is a monic polynomial, and all $f_i \in F$. This polynomial $f(z)$ will be called the minimum function of k. Furthermore, every polynomial $g(z)$ such that $g(k) = 0$, is a multiple of $f(z)$. (4, p. 376)

Definition 5.3. The degree of this minimum function $f(z)$ of the algebraic element k of K over F will be defined as the degree of the algebraic element k, denoted $[k,K]$.

Using the vector space concept, the following may be proved.

Theorem 5.3. Let $F[k]$ be the simple extension field, where k is an algebraic element of K over F and f(z) is the minimum function of k of degree n. Then $F[k]$ forms a vector space of dimension n over F with the linearly independent set of elements $1,k,k^2,\ldots,k^{n-1}$ forming the basis of $F[k]$. (4, p. 384)

This result is rather obvious since every polynomial belonging to $F[k]$ can be expressed as a polynomial of degree at nost n-1 where the degree of the algebraic element k is n.

As a corollary it could be shown that every element of a simple extension $F[k]$ is algebraic over F.

Thus far it has been postulated that if k is an algebraic element of K over F, then certain conclusions may be derived. The following theorem enables us to determine which extensions contain only algebraic elements.

Theorem 5.4. Every element of a finite extension field of F is algebraic over F. Moreover, the minimum function of every element $k \in K$ is of degree at most n where $n = [K;F]$, the degree of the finite extension. (4, p. 385)

The following theorem may be proved.

Theorem 5.5. If the set of elements $\{k_1,k_2,\ldots,k_m\}$ forms a basis of the extension of K over F, and the set $\{s_1,s_2,\ldots,s_n\}$ forms a basis of the extension N over K, then all mn products $k_i l_j$ for $i = 1,2,\ldots,m$ and $j = 1,2,\ldots,n$, form a basis for N over F. (4, p. 388)

II. ROOT FIELDS OF A POLYNOMIAL AND ALGEGRAIC COMPLETE EXTENSION FIELDS

Definition 5.4. A root field M of a polynomial f(z) over a field F is an extension field over F in which f(z) can be factored into a product of linear factors, i.e.,

$$f(z) = c(z - a_1)(z - a_2)\dots(z - a_n)$$

for d(f) = n, $c \in F$, and the root field M is a multiple extension of F generated by the roots, i.e., $M = F(a_1, a_2, \dots, a_n)$.

Now the existence of a root field of any polynomial can be proved.

Theorem 5.6. Every polynomial f(z) over a field F has a root field. (4, p. 410)

Theorem 5.7. Every field F has an algebraically complete (closed) extension field. (1, p. 280)

Corollary 5.7. Every field of prime characteristic has an algebraically complete extension.

This is analogous to the fundamental theorem of algebra where the polynomials f(z) are defined over the real field and the algebraically complete extension is the field of complex numbers.

A polynomial over a field F may or may not have repeated roots in its extension field. Some generalizations may be based on the following definition.

Definition 5.5. A polynomial f(z) is separable if it is factorable over its root field into linear factors of n distinct roots if d(f) = n. Otherwise, f(z) is said to be inseparable. A finite extension N of F is said to be separable if every element of

N satisfies a separable polynomial over F.

Let a formal derivative of $f(z) = f_0 + f_1z + \dots + f_nz^n$, all $f_i \in F$ where F is any field be defined as

$$f'(z) = f_1 + (2f_2)z + \dots + (nf_n)z^{n-1} \qquad (5.1)$$

where mf_i is the m^{th} multiple of f_i.

Theorem 5.8. If the greatest common divisor of f(z) and f'(z) is one, then f(z) is separable. Otherwise, f(z) is inseparable. (4, p. 419)

III. FINITE FIELDS

Definition 5.6. Any field which contains a finite number of elements will be called a "finite field". Denote a finite field of q elements by F_q.

Definition 5.7. The smallest positive integer n such that $n \times a = 0$ for every $a \in F$ is said to be the "characteristic" of the field F. If no such positive integer exists then the field is said to have characteristic zero.

Now if $p > 0$ is the characteristic of a field, then p is a prime. (3, p. 54)

Consider any finite field F_q of characteristic p, $q > p$. Its prime subfield is I_p, the field of integers modulo p. Since F_q is a finite extension over I_p, then every element of F_q is algebraic. So let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the basis of F_q over I_p. Every element β of F_q may be expressed as a linear combination of its base elements, i.e.,

$$\beta = a_1\alpha_1 + a_2\alpha_2 + \dots + a_n\alpha_n, \text{ all } a_i \in I_p.$$

Each a_i can assume only p distinct values, thus $q = p^n$. These results may be summarized in the following

Theorem 5.9. Every prime subfield of a field of characteristic p is a finite field I_p of p elements and every finite extension F_q of I_p is also finite with q elements, where $q = p^n$ for some positive integer n. (4, p. 429)

The nonzero elements of any field form a multiplicative group.

Definition 5.8. The "order" of a group G is the number of elements in the group. The "period" (often called order) of an element $a \in G$ is the least positive integer k such that $a^k = 1$. It is a well known result that every element of a finite group G has period which is a divisor of the order of G. For a finite field F_q of q elements, the q-1 nonzero elements form a multiplicative group of order q-1. Therefore every nonzero element of F_q satisfies $z^{q-1} = 1$, or $z^q - z = 0$. Now the derivative of $z^q - z$ as defined by (5.1) is $(z^q - z)' = qz^{q-1} - 1 = -1$. Hence $(f(z), f'(z)) = 1$ so that $z^q - z$ has q distinct roots by Theorem 5.8.

Let $a_1, a_2, \dots, a_q$ be the q elements of any finite field F_q. Since each nonzero element satisfies $z^{q-1} = 1$, $(z - a_1)(z - a_2)\dots(z - a_q)$ divides $z^q - z$, but each is a monic polynomial with $z^q - z$ having q distinct roots. Therefore they must be $a_1, a_2, \dots, a_q$, and hence $(z^q - z) = (z - a_1)(z - a_2)\dots(z - a_q)$. This proves

Theorem 5.10. The elements of any finite field F_q of q elements are elements of the root field of $z^q - z$. (4, p. 429)

Now since any two root fields are isomorphic the following is true.

Corollary 5.10. Any two finite fields with equal numbers of elements are isomorphic. (4, p. 429)

The only finite fields F_q of q elements that exist are those for which q is expressible as a power of a prime. These finite fields are often called Galios Fields with p^n elements denoted $GF(p^n)$. Of course, $GF(p^n)$ is an extension of its prime subfield GF(p). (6, p. 430)

Theorem 5.11. The nonzero elements of a $GF(p^n)$ form a cyclic group under multiplication. (4, pp. 430-431)

All of the subfields of a given finite field $GF(p^n)$ may be determined by the following.

Theorem 5.12. The necessary and sufficient condition that $GF(p^k)$ be a subfield of $GF(p^n)$ is that $k \mid n$. (2, p. 127)

IV. STRUCTURE OF ROOT FIELDS OF POLYNOMIALS OF PRIME CHARACTERISTIC

In this section some properties of irreducible polynomials which are factors of $z^q - z$, the generator GF(q), will be stated.

Theorem 5.13. Every irreducible polynomial g(z) of degree n over GF(p) is a factor of $z^{p^n} - z$. (5, p. 257)

Theorem 5.14. For every polynomial g(z) of degree m in GF(p), which is a factor of $z^{p^t} - z$ in GF(p), $m \mid t$. (5, p. 257)

Corollary 5.14.1. Every irreducible factor g(z) of $z^{p^n} - z$ in GF(p) is of degree less than or equal to n.

This is obvious, since degree of $g(z)$ must divide n by Theorem 5.14.

Corollary 5.14.2. The smallest extension field of GF(p) that will include all of the roots of an irreducible polynomial $f(z)$ of degree n over GF(p) is $GF(p^n)$.

Proof. Suppose $GF(p^k)$ with $k<n$ is a root field of $f(z)$. Now all roots of $z^{p^k} - z$ are elements of $GF(p^k)$. Since $GF(p^k)$ is the root field of $f(z)$, then $f(z) \mid z^{p^k} - z$. However, by Corollary 5.14.2, $f(z)$ must be of degree less than or equal to k. This contradicts the assumption that $k<n$. Therefore $GF(p^n)$ is the minimal root field of any $f(z)$ of degree n over GF(p).

Theorem 5.15. Let $f(z)$ be an irreducible polynomial of degree n over GF(p). Any root α of $f(z)$ has a period e that is a divisor of p^n-1 and no p^k-1 where $k<n$.

Proof. The fact that the root α must have a period e which is a divisor of p^n-1 is obvious. Since α is a root of $f(z)$, an irreducible polynomial of degree n over GF(p), then α is an element of $GF(p^n)$ (Corollary 5.14.2). Now the nonzero elements of $GF(p^n)$ form a multiplicative group of order p^n-1. It is a well known theorem that the period of an element of such a group divides the order of the group.

Now suppose $e \mid p^k-1$ where $k<n$. This implies that α is an element of $GF(p^k)$ and that $f(z) \mid z^{p^k} - z$. But according to Corollary 5.14.2, $GF(p^n)$ is the smallest extension field of GF(p) that contains all of the roots of $f(z)$.

Theorem 5.16. If α is a root of $f(z)$, an irreducible polynomial of degree n over the extension field $GF(p^n)$, then $\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$ are all the other distinct roots of $f(z)$. (8, p. 118)

Theorem 5.17. If $f(z)$ is an irreducible polynomial, then every root of $f(z)$ has the same period.

Proof. Suppose α is a root of $f(z)$ over $GF(p)$, then all of the roots of $f(z)$ are contained in $GF(p^n)$ and according to Theorem 5.16 they are $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$. Now suppose the period of the root α is t, i.e., t is the least positive integer such that $\alpha^t = 1$ where $t \mid p^n-1$. Then

$$(\alpha^{pk})^t = (\alpha^t)^{pk} = 1 \text{ for } k = 0,1,2,\ldots,n-1.$$

Thus it is only necessary to show that no positive integer s exists such that

$$(\alpha^{pk})^s = 1 \text{ where } s < t.$$

Suppose that there does exist such an s. Then

$$(\alpha^{pk})^s = (\alpha^{pk})^t.$$

Which implies $s \mid t$. But this contradicts the assumption that t is the period of α. Therefore all roots of $f(z)$ have the same period.

Theorem 5.18. Let $f(z)$ be any irreducible polynomial over $GF(p)$ of period t. If α is a root of $f(z)$ over its root field, then the period of the root α equals the period of the polynomial $f(z)$.

Proof. Let $d(f) = n$, and $p(f) = t$. If α_1 is a root of $f(z)$ over the root field $GF(p^n)$, then

$$f(z) = c(z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n),\ c \in GF(p).$$

Now according to Theorem 5.16 $\alpha_2 = \alpha_1^p$, $\alpha_3 = \alpha_1^{p^2}$, $\alpha_4 = \alpha_1^{p3}, \ldots,$ $\alpha_n = \alpha_1^{p^{n-1}}$. By partial fraction decomposition

$$\frac{1}{f(z)} = \frac{\beta_1}{\alpha_1 - z} + \frac{\beta_2}{\alpha_2 - z} + \ldots + \frac{\beta_n}{\alpha_n - z} \text{ with } \beta_i \in GF(p^n).$$

The sequence generated by $\dfrac{\beta_i}{\alpha_i - z}$ is

$$\beta_i\left[(\alpha_i)^{-1}, (\alpha_i)^{-2}, (\alpha_i)^{-3}, \ldots\right].$$

If α_i has period e, so has α_i^{-1}, and the period of the above is e. Now since every root of α_i of f(z) has the same period (Theorem 5.17), then the sequence generated by $\dfrac{\beta_i}{\alpha_i - z}$, $i = 1, \ldots, n$

has period e. Sequences of the same period e added termwise result in a sequence whose period is a divisor of e. By hypothesis the period of f(z) was t. From Corollary 4.3.1 the period of the Sequence generated by 1/f(z) divides the period of f(z). Now since (1,f(z)) = 1, then e = p(f) = t (Theorem 4.9), thus proving the theorem.

<u>Theorem</u> <u>5.19</u>. If $t \not\equiv 0 \pmod p$ for t any integer and p a prime, then $z^t - 1$ is a separable polynomial and conversely.

<u>Proof</u>. Suppose $t \not\equiv 0 \pmod p$, then p is not a factor of t. The formal derivative of $f(z) = z^t - 1$ is $f'(z) = tz^{t-1}$ which is not congruent to zero. Therefore (f,f') = 1, and by Theorem 5.8 $z^t - 1$ is separable.

Conversely, suppose $t \equiv 0 \pmod p$, then $p \mid t$ or pr = t, for some integer r. Consequently $f'(z) \equiv 0 \pmod p$ and over GF(p) (f,f') = 1. Applying Theorem 5.8, one concludes $z^t - 1$ is inseparable. This is obvious since $z^t - 1 = z^{pr} - 1 = (z^r - 1)^p$. Hence the theorem is proved.

Theorem 5.20. If $z^t - 1$ is separable over GF(p), then the smallest root field of $z^t - 1$ is GF(p^k) where k is the smallest integer such that $t \mid p^k-1$.

Proof. The polynomial $z^t - 1$ has as divisors all polynomials g(z) with distinct factors for which $p(g) \mid t$. By hypothesis, $z^t - 1$ is over GF(p). Thus $z^t - 1 \mid z^{p^{k-1}} - 1$ for some smallest integer k. This is true since every polynomial of finite degree over GF(p) has a root field which is a finite extension field of GF(p). But all finite extension fields are of the type GF(p^k) for some k whose nonzero elements are roots of $z^{p^{k-1}} - 1$. Since the roots of $z^t - 1$ belong to GF(p^k), then $z^t - 1 \mid z^{p^{k-1}} - 1$ which is true if and only if $t \mid p^k-1$. Thus some k exists and the smallest integer k such that $t \mid p^k-1$ gives the smallest root field. For all subfields GF(p^n) of GF(p^k) require that $n \mid k$ or equivalently $p^n-1 \mid p^k-1$. However, by assumption k is the smallest integer for which $t \mid p^k-1$. Therefore GF(p^k) is the minimal size root field of $z^t - 1$.

V. CONSTRUCTION OF THE ELEMENTS OF GF(p^n)

In the previous section the smallest root field of any irreducible polynomial f(z) over GF(p) has been expressed explicitly in terms of the period of f(z). These extension fields of GF(p) are finite fields of the form GF(p^n). For later use it will be necessary to readily generate the elements of GF(p^n).

The nonzero elements of GF(p^n) form a cyclic group with the operation multiplication. Hence given any generator of the group one may easily obtain all the elements of the group. In order to determine the periods of the members of $GF(p^n)$, the following result is helpful.

Theorem 5.21. Let G be a cyclic group of order h and α a generator element of G (i.e., α has period or order h). Every element α^u is also a generator of G if and only if $(u,h) = 1$. (8, p. 57)

Euler's ϕ-function. Define the function $\phi(h)$ as the number of positive integers relatively prime to h and less than h. (8, pp. 112-113)

In a cyclic group G of order h with α a member of G, such that $p(\alpha) = h$, all elements α^u where $(u,h) = 1$ are also of period h. So that $\phi(h)$ is also the number of distinct generators of a cyclic group (or the number of primitive elements of G).

A computational expression for $\phi(h)$ can readily be derived to be

$$\begin{aligned}\phi(h) &= \phi(p_1^{e1})\phi(p_2^{e2})\ldots\phi(p_n^{en})\\ &= p_1^{e1}(1 - \frac{1}{p_1})p_2^{e2}(1 - \frac{1}{p_2})\ldots p_n^{en}(1 - \frac{1}{p_n})\\ &= h \prod_{p_i | h} (1 - \frac{1}{p_i})\end{aligned}$$

where the positive integer $h = p_1^{e1}p_2^{e2}\ldots p_n^{en}$, a unique product of powers of prime integers.

One method of determining the elements of $GF(p^n)$ and classifying the elements according to orders could proceed as follows. Since the nonzero elements of $GF(p^n)$ form a cyclic group, assume α is a primitive element, i.e., $p(\alpha) = p^n-1$. For n = 1, such an element is p^n-1; and for $n > 1$, α is a root of a minimum function. Considering the latter cases, the nonzero members of $GF(p^n)$ are

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p^{n-1}}.$$

All α^i $i = 1,2,\ldots,p^n-1$ for which $(i,p^n-1) = 1$ are of period p^n-1. Suppose $t_j \mid p^n-1$. Then all α^i for $i = 1,2,\ldots,p^n-1$ such that $(i,t_j) = 1$ are of period t_j. By Euler's $\emptyset$-function, there are $\emptyset(t_j)$ elements of period t_j. This follows since all roots α^i of period t_j are also roots of $z^{t_j} - 1$. Hence the periods of each of the elements of $GF(p^n)$ can be determined.

The element α of period p^n-1 is the root of an irreducible polynomial, f(z), of degree n (f(z) is a minimum function of α). In fact, α can be assigned to be a root of any n^{th} degree irreducible monic polynomial of period p^n-1. Suppose any such f(z) is chosen, then

$$f(\alpha) = 0 = \alpha^n + f_{n-1}\alpha^{n-1} + \ldots + f_1\alpha + f_0$$

and $$\alpha^n = -(f_{n-1}\alpha^{n-1} + \ldots + f_0).$$

Thus every element $\alpha^i \in GF(p^n)$ where $i \geq n$ may be reduced to a polynomial in α of degree less than n, whose coefficients $f_i \in GF(p)$. This is one way of representing the elements of $GF(p^n)$.

If another n^{th} degree irreducible monic polynomial g(z) of period p^n-1 where chosen, a root of g(z), call it β, could generate all the elements of $GF(p^n)$. An equivalent reduction of all β^i for $i \geq n$ could be performed as indicated above. But since all finite fields containing the same number of elements are isomorphic, then all such representations of $GF(p^n)$ as previously generated are isomorphic.

Cyclotomic Polynomials. (8, pp. 113-115) Suppose the $\phi(t_i)$ elements of $GF(p^n)$, where $t_i \mid p^n-1$, are all roots of a polynomial $\Psi t_i(z)$. This polynomial $\Psi t_i(z)$ is called a cyclotomic polynomial (circle-dividing) of period (order) t_i.

All irreducible polynomials $f_j(z)$ of period t_i divide $z^{t_i} - 1$. Since $t_i \not\equiv 0 \pmod p$, then $z^{t_i} - 1 \mid z^{p^n-1} - 1$ for some smallest integer n so that all the roots of any irreducible polynomial $f_j(z)$ with $p(f_j) = t_i$ are members of a $GF(p^n)$. Thus $\Psi t_i(z)$ contains as irreducible polynomial factors all distinct irreducible polynomials $f_j(z)$ of period t_i. Therefore if cyclotomic polynomials are easily generated and factored over GF(p), then this is a systematic way of obtaining all irreducible polynomials of a given period. That is, $z^t - 1$ can be factored over GF(p).

In order to illustrate the usefulness of several of the previous theorems and concepts, consider the factorization of $z^t - 1$ into cyclotomic polynomials of periods $t_i \mid t$. Each cyclotomic polynomial $\Psi t_i(z)$ of period t_i has as factors all the irreducible polynomials (minimum functions) whose roots are of order t_i where $t_i \mid t$ over GF(p).

If the number of roots of $\Psi t_i(z)$ is $\phi(t_i)$ (Euler's ϕ-function), then the number of irreducible polynomials in each $\Psi t_i(z)$

is $\phi(t_i)/m$, where m is the degree of each minimum function. The integer m is the smallest integer such that $t_i \mid p^m - 1$ (Theorem 5.15). The degree of $\Psi t_i(z)$ equals the number of roots which is $\phi(t_i)$.

In particular consider the following example. Let $t = 20$ and $p = 3$. Then $z^{20} - 1$ is completely factorable in $GF(3^4)$ since $k = 4$ is the smallest k such that $20 \mid 3^k - 1$. Thus $GF(3^4)$ is the minimal root field for $z^{20} - 1$.

The polynomials $z - 1$, $z^2 - 1$, $z^4 - 1$, $z^5 - 1$, $z^{10} - 1$ all divide $z^{20} - 1$. The cyclotomic polynomials $\Psi t_i(z)$ of period t_i are

$$\Psi_1(z) = z - 1 \qquad \text{(degree 1)}$$

$$\Psi_2(z) = \frac{z^2 - 1}{\Psi_1(z)} \qquad \text{(degree 1)}$$

$$\Psi_4(z) = \frac{z^4 - 1}{\Psi_1(z)\Psi_2(z)} \qquad \text{(degree 2)}$$

$$\Psi_5(z) = \frac{z^5 - 1}{\Psi_1(z)} \qquad \text{(degree 4)}$$

$$\Psi_{10}(z) = \frac{z^{10} - 1}{\Psi_1(z)\Psi_2(z)\Psi_5(z)} \qquad \text{(degree 4)}$$

$$\Psi_{20}(z) = \frac{z^{10} - 1}{\Psi_1(z)\Psi_2(z)\Psi_4(z)\Psi_5(z)\Psi_{10}(z)} \qquad \text{(degree 8)}$$

The number of roots of order 20, for example is also given by $\phi(20) = \phi(2^2 \cdot 5) = 20(1 - 1/2)(1 - 1/5) = 8$, which checks with the degree of $\Psi_{20}(z)$.

to determine the number of irreducible polynomials in each $\Psi t_i(z)$, make use of Theorem 5.15. For

$$\Psi_2(z) : 2 \mid 3^m - 1 \quad \text{implies } m = 1$$
$$\Psi_4(z) : 4 \mid 3^m - 1 \quad \text{implies } m = 2$$
$$\Psi_5(z) : 5 \mid 3^m - 1 \quad \text{implies } m = 4.$$

Since $m \leq k$, $\Psi_{10}(z)$ and $\Psi_{20}(z)$ are composed of irreducible factors of degree 4 each. $\Psi_{20}(z)$ consists of two fourth degree irreducible factors of period 20.

Completing the factorization gives

$$\Psi_1(z) = z + 2$$
$$\Psi_2(z) = z + 1$$
$$\Psi_4(z) = z^2 + 1$$
$$\Psi_5(z) = z^4 + z^3 + z^2 + z + 1$$
$$\Psi_{10}(z) = z^4 + 2z^3 + z^2 + 2z + 1$$
$$\begin{aligned}\Psi_{20}(z) &= z^8 + 2z^6 + z^4 + 2z^2 + 1\\ &= (z^4 + z^3 + 2z + 1)(z^4 + 2z^3 + z + 1).\end{aligned}$$

CHAPTER VI

DECOMPOSITION OF PERIODIC SEQUENCES INTO THEIR GENERATING POLYNOMIALS

I. UNIQUE DECOMPOSITION OF A PERIODIC SEQUENCE INTO A MINIMUM DEGREE GENERATING FUNCTION

If a periodic sequence $\{h_i\}_{i=0}^{\infty}$ is specified where $\{h_i\}_{i=0}^{\infty}$ belongs to a known $G(f)$, then the minimum degree ratio of polynomials generating $\{h_i\}_{i=0}^{\infty}$ can be determined by the following theorem.

<u>Theorem</u> <u>6.1</u>. Let $\{h_i\}_{i=0}^{\infty} \in G(f)$, where $f(z) = f_0 + f_1 z + \ldots + f_k z^k$, $f_0 f_k \neq 0$, and $f_i \in I_p$. If $f(z)$ has distinct roots $a_0, \ldots, a_{k-1}$ in the root field K of $f(z)$, then for every such linear recurring sequence $\{h_i\}_{i=0}^{\infty}$ there exists a unique set $\{b_0, \ldots, b_{k-1}\}$, $b_i \in K$, which are determined by

$$h_r = \sum_{i=0}^{k-1} b_i \alpha_i^r \quad (r = 0, 1, \ldots\ ) \tag{6.1}$$

with $\alpha_i = a_i^{-1}$. Conversely, for a set $\{b_0, \ldots, b_{k-1}\}$, $b_i \in K$, such that all the h_i defined by (6.1) belong to I_p, then $\{h_i\}_{i=0}^{\infty}$ belongs to $G(f)$.

<u>Proof</u>. Suppose $\{h_i\}_{i=0}^{\infty} \in G(f)$. Then $h(z) = g(z)/f(z)$ for some $g(z)$. Over K, the root field of $f(z)$, $f(z)$ is factorable into distinct linear factors by hypothesis. That is,

$$f(z) = f_k(z - a_0)(z - a_1)\ldots(z - a_{k-1})$$

or

$$f(z) = f_k(-1)^k(a_0 - z)\ldots(a_{k-1} - z). \tag{6.2}$$

By partial fraction decomposition,

$$\frac{g(z)}{f(z)} = \frac{(f_k^{-1})(-1)^k\ g(z)}{(a_0 - z)(a_1 - z)\ \ldots\ (a_{k-1} - z)} \tag{6.3}$$

may be decomposed into a sum of linear factors

$$\frac{g(z)}{f(z)} = \frac{b_0}{a_0 - z} + \frac{b_1}{a_1 - z} + \ldots + \frac{b_{k-1}}{a_{k-1} - z}\ . \tag{6.4}$$

In series form

$$\frac{b_i}{a_i - z} = b_i \sum_{j=0}^{\infty} (a_i^{-1})^j\ z^j = b_i \sum_{j=0}^{\infty} \alpha_i^j\ z^j$$

The polynomial corresponding to $\{h_i\}_{i=0}^{\infty}$ is

$$h(z) = \sum_{i=0}^{\infty} h_i z^i$$

Thus equating the two series representations of h(z),

$$h(z) = \sum_{i=0}^{\infty} h_i z^i = \sum_{i=0}^{\infty} (b_0 \alpha_0^i + b_1 \alpha_1^i + \ldots + b_{k-1}\alpha_{k-1}^i) z^i \tag{6.5}$$

Two power series in z are equal if and only if the coefficients of like powers in z are equal, which implies

$$h_r = \sum_{j=0}^{k-1} b_j \alpha_j^r$$

or in matrix form

$$\begin{bmatrix} h_0 \\ h_1 \\ \cdot \\ \cdot \\ \cdot \\ h_{k-1} \end{bmatrix} = \begin{bmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{k-1} \\ \alpha_0^2 & \alpha_1^2 & \ldots & \alpha_{k-1}^2 \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ \alpha_0^k & \alpha_1^k & \ldots & \alpha_{k-1}^k \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_{k-1} \end{bmatrix}$$

Alternately this may be written as h = Mb', i.e.,

$$\begin{bmatrix} h_0 \\ h_1 \\ \cdot \\ \cdot \\ \cdot \\ h_{k-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_0 & \alpha_1 & \dots & \alpha_{k-1} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \dots & \alpha_{k-1}^{k-1} \end{bmatrix} \begin{bmatrix} b_0' \\ b_1' \\ \cdot \\ \cdot \\ \cdot \\ b_{k-1}' \end{bmatrix} \tag{6.6}$$

where $b_i' = \alpha_i b_i$.

Thus there exists a unique solution of the b_i' if and only if M is nonsingular, but M is the transpose of the Vandermonde matrix, and it is nonsingular if $\alpha_0, \dots, \alpha_{k-1}$ are distinct. (7, p. 134) This is satisfied by the hypothesis of the theorem. Therefore the first part of the theorem is proved.

In application the determinant of the matrix M may be calculated in order to determine M^{-1}. Since M is the transpose of the Vandermonde matrix its determinant may be written

$$\begin{aligned} \det[M] = (\alpha_{k-1} - \alpha_{k-2})(\alpha_{k-1} - \alpha_{k-3})\dots(\alpha_{k-1} - \alpha_1)(\alpha_{k-1} - \alpha_0)\ x \\ x\ (\alpha_{k-2} - \alpha_{k-3})\dots(\alpha_{k-2} - \alpha_1)(\alpha_{k-2} - \alpha_0)\ x \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ x\ (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_0)\ x \\ x\ (\alpha_1 - \alpha_0)\ . \end{aligned}$$

Which may be written more briefly in the form

$$\det[M] = \prod_{i,j=0}^{k-1} (\alpha_i - \alpha_j),\ i > j, \tag{6.7}$$

i.e., the determinant M is equal to the product of differences $\alpha_i - \alpha_j$, where i,j assume values 0,1,...,k-1 in such a way that $i > j$.

Now returning to the proof of the above theorem, we are ready to prove the converse. That is, for any arbitrary set $\{b_0, \dots, b_{k-1}\}$, $b_i \in K$, the resulting $\{h_i\}_{i=0}^{\infty}$ defined by (6.1) will in general have its elements in K. Now

$$\sum_{j=0}^{k} f_j h_{r-j} = \sum_{j=0}^{k}\left(f_j \sum_{i=0}^{k-1} b_i \alpha_i^{r-j}\right)$$

$$= \sum_{i=0}^{k-1} b_i \alpha^{r-k} \sum_{j=0}^{k} f_j \alpha_i^{k-j}. \qquad (6.8)$$

To show that $\sum_{j=0}^{k} f_j \alpha_i^{k-j} = 0$ for all i, consider the polynomial

$$f'(z) = f_k + f_{k-1}z + \ldots + f_1 z^{k-1} + f_0 z^k$$

which is factorable into the form

$$f'(z) = f_0(z - \beta_0)\ldots(z - \beta_{k-1}) \qquad (6.9)$$

where the β_i are over an appropriate root field K'. But

$$f(z) = z^k f'(1/z) = z^k f_0(1/z - \beta_0)\ldots(1/z - \beta_{k-1})$$

$$= f_0(1 - \beta_0 z)(1 - \beta_1 z)\ldots(1 - \beta_{k-1} z)$$

$$= f\ (\beta_0 \ldots \beta_{k-1})(\beta_0^{-1} - z)(\beta_1^{-1} - z)\ldots(\beta_{k-1}^{-1} - z). (6.10)$$

By assumption of the factorization of f(z) and the fact that factorization is unique over a root field, then from (6.2) and (6.10)

$$\beta_i^{-1} = a_i = \alpha_i^{-1} \ (i = 0,\ldots,k-1)$$

and
$$(f_0)(\beta_0 \ldots \beta_{k-1}) = (-1)^k f_k.$$

Therefore the root field of f(z) and f'(z) coincide, and any root a_i of f(z) has $a_i^{-1} = \alpha_i$ as corresponding root of f'(z). Hence (6.8) is zero, implying that the $\{h_i\}_{i=0}^{\infty}$ resulting from the arbitrarily chosen $b_0,\ldots,b_{k-1}$ satisfy a recurring relation of the type (2.1). Hence if the resulting h_i all belong to I_p, then the $\{h_i\}_{i=0}^{\infty} \in G(f)$ by definition of G(f).

The minimal size G(f) which contains all sequences of period t is specified by

Theorem 6.2. Let the polynomial $f(z)$ be defined over $GF(p)$ and let $G(f)$ be over $GF(p)$. The minimal degree polynomial $f(z)$ such that $G(f)$ contains all sequences of period t is the polynomial $f(z) = z^t - 1$.

Proof. Theorem 4.8 states that $G(z^t - 1)$ contains all sequences of periods t_i which divide t. The minimality of the degree of $z^t - 1$ is obvious. For consider the sequence $\{u_i\}_{i=0}^{\infty}$ generated by $\dfrac{g(z)}{1 - z^t}$ where $(g, z^t - 1) = 1$. Since $(g, z^t - 1) = 1$, then $p(u) = t$ and $\{u_i\}_{i=0}^{\infty}$ cannot belong to any other $G(f)$ where $d(f) < t$ (Theorem 4.9).

The results of Theorems (6.1) and (6.2) allow the minimum degree generating function to be computed for any periodic sequence $\{h_i\}_{i=0}^{\infty}$ over $GF(p)$ of period t provided that $t \not\equiv 0 \pmod p$. If $t \not\equiv 0 \pmod p$, then any purely periodic sequence $\{h_i\}_{i=0}^{\infty}$ over $GF(p)$ with $p(h) = t$ belongs to $G(z^t - 1)$, where $z^t - 1$ is separable.

The roots of $z^t - 1$ are elements of the extension field $GF(p^n)$ where $t \mid p^n - 1$. Hence the roots of $z^t - 1$ may be found so that (6.1) may be solved for the b_i', $i = 0, \ldots, k-1$.

Consider the following problem to illustrate the use of Theorems (6.1) and (6.2) with respect to computing a minimal degree generating function from a given periodic sequence $\{h_i\}_{i=0}^{\infty}$. Suppose the given sequence is

$$\{h_i\}_{i=0}^{\infty} = \{2,1,2,0,2,1,2,0,\ldots\}.$$

This sequence of numbers is periodic with period $t = 4$. Since the maximum element is two, then a field of characteristic three, $GF(3)$ would adequately represent the set of elements contained in the sequence with $t = 4 \not\equiv 0 \pmod 3$. The sequence $\{h_i\}_{i=0}^{\infty}$ must belong to the set $G(f)$ where $f(z) = z^t - 1$. Since $t \not\equiv 0 \pmod p$, then the polynomial $z^4 - 1$ has $GF(3^2)$ as its root field. For $z^4 - 1 \mid z^{3^{k-1}} - 1$ for $k = 2$ and no smaller k, and thus the elements of $z^{3^2} - z$ form the minimum extension field of $GF(3)$ in which $z^4 - 1$ is completely factorable.

In order to apply Theorem 6.2 for obtaining the generating function $g(z)/f(z) = h(z)$, the polynomial $z^4 - 1$ must be factored over its root field. The irreducible factors of $z^4 - 1$ will be factors of $z^{3^2} - z$, whose factorization may be accomplished through use of cyclotomic polynomials.

$$\Psi_1(z) = z - 1 = z + 2$$

$$\Psi_2(z) = \frac{z^2 - 1}{\Psi_1(z)} = z + 1$$

$$\Psi_4(z) = \frac{z^4 - 1}{\Psi_1(z)\Psi_2(z)} = z^2 + 1$$

$$\Psi_8(z) = \frac{z^8 - 1}{\Psi_1(z)\Psi_2(z)\Psi_4(z)} = z^4 + 1$$

Each $\Psi t_i(z)$ consists of all irreducible polynomials of period t_i. Since $z^{3^2} - z$ contains irreducible factors of degree ≤ 2, then $z^4 + 1$ is factorable into two second degree polynomials which are

$$z^4 + 1 = (z^2 + z + 2)(z^2 + 2z + 2).$$

Both of these polynomials have roots of period $p^k - 1 = 3^2 - 1$. The nonzero elements of $GF(3^2)$ may be formed by the $p^k - 1 = 8$ powers of a primitive element of $GF(3^2)$. Suppose "a" is a root of $z^2 + 2z + 2$, then $a^2 = a + 1$ and the elements of $GF(3^2)$ are

$$\begin{aligned} &0 \\ a^0 &= 1 \\ a^1 &= a \\ a^2 &= a + 1 \\ a^3 &= 2a + 1 \\ a^4 &= 2 \\ a^5 &= 2a \\ a^6 &= 2a + 2 \\ a^7 &= a + 2 \\ a^8 &= 1 \end{aligned}$$

Equivalently a root of $z^2 + z + 2$ might have been chosen in order to form a field isomorphic to the one exhibited above.

Returning to the problem at hand, it is necessary to factor $z^4 - 1$ into linear factors. Over GF(3)

$$z^4 - 1 = (z - 1)(z - 2)(z^2 + 1).$$

The roots of $z^2 + 1$ are of order 4, which are

$$a^2 = a + 1, \; a^6 = 2a + 2.$$

Therefore

$$z^2 + 1 = (z - a - 1)(z - 2a - 2) = (z - a^2)(z - a^6).$$

From (6.6)

$$\begin{bmatrix} 2 \\ 1 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \alpha_4^3 \end{bmatrix} \begin{bmatrix} b_1' \\ b_2' \\ b_3' \\ b_4' \end{bmatrix}.$$

where $\alpha_1 = (1)^{-1} = 1$, $\alpha_2 = (2)^{-1} = 2 = a^4$, $\alpha_3 = (a^2)^{-1} = a^6$, $\alpha_4 = (a^6)^{-1} = a^2$.

The vandermonde matrix becomes

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & a^6 & a^2 \\ 1 & 1 & a^4 & a^4 \\ 1 & 2 & a^2 & a^6 \end{bmatrix}$$

By definition, the inverse of the matrix M is

$$M^{-1} = 1/\det M \cdot \operatorname{adj} M$$

$$= a^2 \begin{bmatrix} a^6 & a^6 & a^6 & a^6 \\ a^6 & a^2 & a^6 & a^2 \\ a^6 & a^0 & a^2 & a^6 \\ a^6 & a^4 & a^2 & a^0 \end{bmatrix}$$

$$= \begin{bmatrix} a^0 & a^0 & a^0 & a^0 \\ a^0 & a^4 & a^0 & a^4 \\ a^0 & a^2 & a^4 & a^6 \\ a^0 & a^6 & a^4 & a^2 \end{bmatrix}$$

$$\begin{bmatrix} b_1' \\ b_2' \\ b_3' \\ b_4' \end{bmatrix} = \begin{bmatrix} & & \\ & M^{-1} & \\ & & \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 2 \\ 0 \end{bmatrix}$$

so that the solution of the b_i' are

$$b_1' = 2, \; b_2' = 0, \; b_3' = a^2, \; b_4' = a^6$$

and $\quad b_i = b_i' \alpha_i^{-1}$

which gives $\quad b_1 = 2, \; b_2 = 0, \; b_3 = 2, \; b_4 = 2.$

Therefore the decomposed form of the desired generating function is

$$\frac{g(z)}{f(z)} = \frac{2}{1 - z} + \frac{0}{2 - z} + \frac{2}{a^2 - z} + \frac{a^6}{a^6 - z} = \frac{1}{z + 2} + \frac{2z}{z^2 + 1}$$
$$= \frac{z + 1}{z^3 + 2z^2 + z + 2} .$$

Checking the result by long division gives

$$\frac{g(z)}{f(z)} = \frac{z + 1}{z^3 + 2z^2 + z + 2} = h(z) = 2 + z + 2z^2 + 0z^3 + 2z^4 + z^5 + 2z^6 + 0z^7 + \ldots .$$

Hence the sequence generated is $\{2, 1, 2, 0, 2, 1, 2, 0, \ldots\}$ and the desired result has been achieved--that of determining the minimum degree function which generates $\{h_i\}_{i=0}^{\infty}$.

II. AN ALTERNATIVE METHOD OF DETERMINING THE MINIMUM DEGREE GENERATING FUNCTION

An alternative calculation procedure can be developed for determining the minimum degree generating function of a given periodic sequence. In fact, any given periodic sequence $\{h_i\}_{i=0}^{\infty}$ of period t has a polynomial representation of $h(z) = q(z)/(1 - z^t)$ for some q(z) where $d(q) \leq t - 1$. So

$$q(z) = (1 - z^t)(h + h z + \ldots + h_{t-1}z^{t-1} + h_t z^t + h_{t+1}z^{t+1} + \ldots)$$
$$= (h_0 + h_1 z + \ldots + h_{t-1}z^{t-1}) + (h_t - h_0)z^t + (h_{t+1} - h_1)z^{t+1} + \ldots \qquad (6.11)$$

If $q(z) = q_0 + q_1 z + \ldots + q_{t-1}z^{t-1}$, it follows from the above equality that

$$q_i = h_i \text{ for } i = 0,1,\ldots,t-1$$

Now if $(q(z), z^t - 1) = q_1(z) \neq 1$, then the factor $q_1(z)$ may clearly be eliminated, yielding

$$h(z) = \frac{q(z)}{z^t - 1} = \frac{q_1(z)\ q_2(z)}{q_1(z)\ p(z)} = \frac{q_2(z)}{p(z)} \tag{6.12}$$

which is minimal. This bypasses the necessity of determining the roots.

The theory of cyclotomic polynomials and their irreducible factors becomes quite valuable as a systematic method of reducing (6.12) to the lowest degree. In fact, this method may be used to handle both the distinct root case when $t \not\equiv 0 \pmod{p}$ and the multiple root case where $t \equiv 0 \pmod{p}$.

Either of these two procedures determines the same minimum degree representation of a periodic sequence when the period t of the sequence is not congruent to zero modulo p. However, for the multiple root case, $t \equiv 0 \pmod{p}$, the alternative calculation method may be applied very systematically while the method of Theorem 6.1 does not apply.

CHAPTER VII

SUMMARY

For a given (k+1)-tuple $(f_0, f_1, \ldots, f_k)$, the solutions of

$$\sum_{j=0}^{k} f_j h_{i-j} = 0, \ (i = k, \ k+1, \ \ldots \ )$$

are members of the set $G(f_0, f_1, \ldots, f_k)$ which forms a vector space.

The members of this set are equivalently generated by elements of

$$G(f) = h(z) = \left\{ g(z)/f(z); \ d(g) < d(f) \text{ and } g_i \in GF(p) \right\}$$

where the correspondence is

$$f(z) = f_0 + f_1 z + \ldots + f_k z^k \longleftrightarrow (f_0, f_1, \ldots, f_k)$$

and

$$h(z) = \sum_{i=0} h_i z^i \longleftrightarrow (h_0, h_1, \ldots \ ) = \{h_i\}_{i=0}^{\infty}.$$

The inherent property of a solution, $\{h_i\}_{i=0}^{\infty}$, is that it is a purely periodic sequence whose period is a divisor of the period of the polynomial $f(z)$.

It was shown that any purely periodic sequence, $\{x_i\}_{i=0}^{\infty}$, of period t belongs to $G(z^t - 1)$ and that the minimum degree ratio of polynomials $g(z)/f(z)$, where $G(f) \subseteq G(z^t - 1)$ could be determined.

BIBLIOGRAPHY

A. BOOKS

1. Albert, A. Adrian. Modern Higher Algebra. Chicago: The University of Chicago Press, 1937.

2. Albert, A. Adrian. Fundamental Concepts of Higher Algebra. Chicago: The University of Chicago Press, 1956.

3. Artin, Emil. Galois Theory. Second edition. Notre Dame, Indiana: University of Notre Dame, 1942.

4. Birkhoff, Garrett and Sanders MacLane. A Survery of Modern Algebra. New York: Macmillan, 1941.

5. Carmicheal, Robert D. Introduction to the Theory of Groups of Finite Order. Boston: Ginn, 1937.

6. McCoy, Neal H. Introduction to Modern Algebra. Boston: Allyn and Bacon, 1960.

7. Mostowski, Andrzej and M. Stark. Introduction to Higher Algebra. International Series of Monographs on Pure and Applied Mathematics, Translated by Dr. J. Musielak. New York: Macmillan, 1964.

8. Waerden, B. L. van der. Modern Algebra. Vol. I, translated by Fred Blum. New York: Frederick Ungar Publishing Co., 1949.

B. PERIODICALS

9. Brenner, J. L. "Linear Recurrence Relations," American Mathematical Monthly, 61:171-173, March, 1954.

10. Ward, Morgan. "The Arithmetical Theory of Linear Recurring Sequences," Transactions of the American Mathematical Society, 35:600-628, July, 1933.

11. Zierler, Neal. "Linear Recurring Sequences," Journal for the Society of Industrial and Applied Mathematics, 7:31-48, March, 1959.