Periodic Functions
over
Fields of Characteristic p

Thesis by
Jonathan Dean Swift

In Partial Fulfilment of the Requirements
for the Degree of Doctor of Philosophy,
California Institute of Technology
1947

Acknowledgement

I wish to express my sincere appreciation of the help and guidance given me by the staff of the Department of Mathematics of the California Institute of Technology. In particular, I wish to thank Professors Bell and Ward for their interest in, and encouragement of my work. The suggestions and assistance given by Professor Ward in the preparation of this thesis have been invaluable.

Summary

A function from a field of characteristic p into the same field is called periodic with period modulus M, if $f(x+\mu) = f(x)$, where μ is any element of M.

For a Galois Field, $GF(p^t)$, there exist non-constant functions, periodic with any proper sub-modulus of the field. For any field of characteristic p, and any set, $a_1, a_2, \ldots, a_{n-1}, a_n$, of elements, linearly independent with respect to the prime sub-field Π, $n < t$, the functions:

$$f(a_1;x) = x^p - a_1^{p-1}x$$

$$f(a_1,a_2;x) = f(f(a_1;a_2); f(a_1;x))$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots$$

$$f(a_1,a_2,\ldots,a_n;x) = f(f(a_1,\ldots,a_{n-1};a_n); f(a_1,\ldots,a_{n-1};x))$$

form a set of periodic functions with moduli: $(a_1),(a_1,a_2),\ldots (a_1,\ldots,a_n)$. These functions are additive, linear with respect to Π, and symmetric in the a_i. Any function periodic with the modulus M_n in a $GF(p^t)$ may be represented by:

$$\sum_{i=0}^{s-1} b_i [f(M_n;x)]^i, \qquad s = p^{t-n}$$

where $f(M_n;x) = f(a_1,\ldots,a_n;x)$, $M_n = (a_1,\ldots,a_n)$ and the b_i are elements of the $GF(p^t)$.

The latter part of the thesis is devoted to the consideration of other possible bases for representation of all periodic functions over Galois fields. A definition of an orthogonal representation is given and sets satisfying the

definition are exhibited for certain special cases, in particular for t even and n = t - 1. More generally, it is shown that, if the $GF(p^t)$ is imbedded in the splitting field of a certain equation, a set of polynomials exist such that their values for elements of the $GF(p^t)$ are in the latter field and are orthogonal with respect to that field, although the polynomials require, for their simplest expression in terms of the $f^i(M;x)$, coefficients from the superfield.

TABLE OF CONTENTS

1. Fields of Characteristic p. Basic Concepts and Definitions.

All fields contain one and only one prime field, Π. This prime field is either isomorphic to a residue class modulo a prime integer p, or to the field of all rational numbers. In the first case, the field is said to have characteristic p; in the second, characteristic 0. If a field of characteristic p has a finite number of elements, it is called a Galois field. All such fields of given order are abstractly identical and have p^t elements where t is a positive integer; t is the "index" of the field, $GF(p^t)$.(3)*

The majority of the theorems to be deduced will concern Galois fields. Theorems applicable to all commutative fields of characteristic p will be specifically noted. The following equations, valid in any field of characteristic p, will be used in the sequel without further comment:

$$\left(\sum_i a_i\right)^{p^f} = \sum_i a_i^{p^f},$$

$$(a_1 - a_2)^{p-1} = \sum_{j=0}^{p-1} a_1^j a_2^{p-1-j}$$

Here the a_i are any elements of the field.

The $GF(p^t)$ may be constructed by selecting a polynomial, irreducible modulo p, of degree t, and considering the p^t

---

* Numbers in parentheses refer to the corresponding entry in the bibliography.

residues modulo the polynomial and p. A tabulation of all quadratic and cubic fields, ($t = 2,3$) such that $p^t < 100$, is given in an appendix.

The additive group of the $GF(p^t)$ is of type $(p,p,\ldots p)$. Thus the subgroups are composed of p^k elements, $k \leq t$, and are generated from a basis, $(a_1,\ldots,a_k)$, of any k elements linearly independent with respect to Π.(2)

The multiplicative group of the field is cyclic. If $p^t = q$, all members of the $GF(p^t)$ satisfy the equation: $x^q - x = 0$. Each element of the field possesses one and only one p^{th} root, and, thus, one and only one p^{kth} root. Further, if $d = (m,q-1)$, exactly $(q-1)/d$ elements are m^{th} powers (i.e. have m^{th} roots) in the field.(1)

2. Periodic Functions.

In this section the notion of periodic functions over a field of characteristic p will be defined and some general properties of these functions will be discussed. The discussion will, of course, be confined completely to algebraic properties. Although a formal derivative exists, the lack of a valuation makes an analytic discussion impossible. In general, very little attention has been paid to the existence and algebraic properties of periodic functions in fields outdise of the customary real and complex number domains, although functions analogous to the common periodic functions,

but not necessarily periodic in the new domain, have been studied.(27,28,29)

A large amount of work has been done, particularly by Carlitz, on the properties of special classes of polynomials in a Galois field.(4)-(26) inc. In general, this work has dealt with the polynomial domain itself, using the literal elements as indeterminates. In the present work, a special class of polynomials is considered not only for its own properties as polynomials, but also from the standpoint of the values attained when the variables are replaced by elements of the field.

For Galois fields the limitation of the functions considered to polynomials is no real restriction since all functions defined for all members of the field with values in the same field may be represented by polynomials with coefficients in the $GF(p^t)$.

Definition 2.1: A function, $f(x)$, defined over a field of characteristic p with values in the same field, is called periodic if an element a of the field exists such that $f(x+a) = f(x)$. The element 'a' is called a period of the function.

Definition 2.2: A function $f(x)$, defined as above, is k-tuply periodic, with periods $a_1, a_2, \ldots a_k$, if $f(x + m_1 a_1 + m_2 a_2 + \ldots + m_k a_k) = f(x)$, where the m_i are arbitrary

members of the prime sub-field, Π, and the a_i are linearly independent with respect to Π.

The definitions have been phrased in the above manner to preserve the analogy with the ordinary case. However, it is clear that, if a is a period, the elements 2a, 3a,..., (p - 1)a are also periods. That is, instead of a single elementary period, there exists a period modulus M, where M is the modulus generated by $a_1,\ldots,a_k$. Since the field is unordered, there is no particular period singled out from the modulus as the period of f(x). We thus have:

Definition 2.3: The largest modulus generated by the periods of a periodic function is designated the period modulus, M, of the function. For any μ in M, $f(x+\mu) = f(x)$, for every x of the GF, and for any μ not in M, $f(x+\mu) \neq f(x)$ for at least one x of the GF. If the modulus consists of p^k elements, the function is said to be k-tuply periodic. Any linearly independent set of k elements of M is called a (complete) set of periods.

Theorem 2.1: A non-constant function, f(x), over a $GF(p^t)$ has at most t - 1 independent periods.

Proof: If the function had t periods, M would contain p^t elements, and would thus include every element of the $GF(p^t)$. Since $f(x+\mu) = f(x)$, $\mu \in M$, f(x) would be constant.

Theorem 2.2: Given any proper submodulus, M, of the

$GF(p^t)$, there exists a (at least one) function, f(x), such that M is the period modulus of f(x).

Proof: We construct such a function as follows: Let the order of M be p^k. Choose a complete set of periods, $a_1,\ldots,a_k$, and choose t - k other elements, $a_{k+1},\ldots,a_t$, such that the set, $a_1,\ldots,a_t$, form a linearly independent set, that is, each x of the $GF(p^t)$ may be uniquely represented as $x = \sum_i m_i a_i$.

We then define f(x) by: $f(x) = \sum_{i=k+1}^{t} m_i a_i$.

This is a function of the required type for, clearly, the addition of an element of M to the argument does not change the corresponding value of the function, while for any modulus $M' \supset M$, the value is changed by addition of an element of M' which is not in M.

The appendix contains a description of a notation which facilitates the choices described above, and illustrations of functions using this notation. It is clear that, in general, many other functions of period modulus M exist. For example, a constant could be added to the value of the function for each argument.

3. Singly Periodic Functions.

The special theory, developing representations for all periodic functions over a modulus M_1 consisting of p elements will now be developed as a basis for the general theory

covering arbitrary moduli. Let a be a generating element of M. Then:

Theorem 3.1: $x^p - a^{p-1}x$ is periodic with modulus M over any commutative field of characteristic p.

Proof: Let $\mu \in M$, i.e. $\mu = ma$, $m \in \Pi$, then:

$$\begin{aligned}
&(x+\mu)^p - a^{p-1}(x+\mu) \\
&= (x+ma)^p - a^{p-1}(x+ma) \\
&= x^p - a^{p-1}x + m^p a^p - ma^p; \quad m^p = m \\
&= x^p - a^{p-1}x.
\end{aligned}$$

Corollary: $x^{p^k} - a^{p^k-1}x$ is periodic with modulus M.

The question arises as to whether a multiple periodicity may be concealed by the use of the above function. That is, is M the actual period modulus?

If M is not the period modulus, there is a $b \notin M$ such that:

$$\begin{aligned}
(x+b)^{p^k} - a^{p^k-1}(x+b) &= x^{p^k} - a^{p^k-1}x \\
b^{p^k} - a^{p^k-1}b &= 0 \\
b^{p^k-1} &= a^{p^k-1}.
\end{aligned}$$

If $k=1$, this states that $\left(\frac{b}{a}\right)^{p-1} = 1$ or $\frac{b}{a} \in \Pi$, which contradicts the assumption, $b \notin M$. If $k > 1$, the necessary condition that $b^{p^k-1} = a^{p^k-1}$, and $b \neq ma$ in a $GF(p^t)$ is that $(p^t-1, p^t-1) > p-1$. In this case there exists a

sub-field of order p^k, and here the second type of function may be multiply periodic. This question will be returned to when the general doubly periodic function is obtained; the above function will then appear as a special case.

Notation: From this point on, the notation, f( ) will be reserved for certain specific types of functions of which the function of Th. 3.1 forms the first example:

$$f(a;x) = x^p - a^{p-1}x.$$

Theorem 3.2: $f(a;bx) = b^p f(\frac{a}{b};x)$.

Proof: $b^p x^p - a^{p-1}bx = b^p(x^p - (\frac{a}{b})^{p-1}x)$.

(Note the analogy with the sine or cosine function of ordinary analysis. I.e. sin bx has a period 1/b of the basic period.)

Theorem 3.3: f(a;x) is 1) additive, and 2) linear with respect to Π.

Proof: Evident on expansion of f(a;x+y) and f(a;mx).

Theorem 3.4: $\sum_{i=0}^{k} b_i [f(a;x)]^i$ is periodic, with period a, where the b_i are arbitrary elements of the field, and where, for convenience of expression now and in the sequel, the convention $[f(a;x)]^0 \equiv 1$ is adopted.

Proof: Clear.

Theorem 3.5: Any function which is periodic with

modulus M ⊃ a, over a GF(pt), may be represented in the form:

$$\sum_{j=0}^{s-1} b_j [f(a;x)]^j \qquad \text{where } s = p^{t-1}.$$

Proof: Let g(x) be a periodic function with a as a period. Select, from the field, elements, $a_2,\ldots,a_t$, such that $a, a_2,\ldots,a_t$ form a linearly independent set. The sums, $\sum_{i=2}^{t} m_{ik} a_i$, where the m_{ik} range over Π, form a set of p^{t-1} distinct elements which includes no element of M except 0. For these non-zero elements, $f(a;x) \neq 0$; for, otherwise, $x^p = a^{p-1}x$, $x^{p-1} = a^{p-1}$, and $\frac{x}{a} \in \Pi$, a contradiction.

The values of the function for the elements of the generated set completely determine the function. We thus have a set of equations:

$$g\left(\sum m_{ik} a_i\right) = \sum_{j=0}^{s-1} b_j \left[f\left(a;\sum m_{ik} a_i\right)\right]^j.$$

This is a set of s equations to be solved for s values of the b_j. The determinant of these equations is clearly of the Vandermonde type:

$$\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & f(a;\sum m_{i,1} a_i) & [f(a;\sum m_{i,1} a_i)]^2 & \cdots & [f(a;\sum m_{i,1} a_i)]^{s-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & f(a;\sum m_{i,s-1} a_i) & [f(a;\sum m_{i,s-1} a_i)]^2 & \cdots & [f(a;\sum m_{i,s-1} a_i)]^{s-1} \end{vmatrix}.$$

The value of this determinant is then:

$$\prod_k f(a;\Sigma m_{ik} a_i) \prod_{k \neq j} [f(a;\Sigma m_{ij} a_i) - f(a;\Sigma m_{ik} a_i)].$$

This product is clearly non-zero, if:

$$f(a;\Sigma m_{ij} a_i) \neq f(a;\Sigma m_{ik} a_i), \quad j \neq k.$$

But: $f(a;\Sigma m_{ij} a_i) = \Sigma m_{ij} f(a;a_i)$ by Th. 3.3.

Suppose: $\Sigma m_{ij} f(a;a_i) = \Sigma m_{ik} f(a;a_i)$

$$\Sigma (m_{ij} - m_{ik}) f(a;a_i) = 0.$$

Let $m_{ij} - m_{ik} = m_{il}$: $\Sigma m_{il} f(a;a_i) = 0$

$$f(a;\Sigma m_{il} a_i) = 0$$

and, thus, all $m_{il} = 0$. This contradicts the assumption that $j \neq k$. Therefore the determinant is non-zero, and the solution is possible.

We have now exhibited a complete set of functions, $1, f(a;x), f^2(a;x), \ldots, f^{s-1}(a;x)$, which suffice for the linear representation (with respect to the complete field) of any periodic function whose period modulus contains a. The specific set is chosen since it arises naturally from the important function: $x^p - x = f(1;x)$; $f(a;x) = a^p f(1;x/a)$. The properties of these and other complete sets for representation will be investigated after the development

of the theory of representations for the complete period modulus. (The theory of multiply periodic functions.)

4. The Doubly Periodic Function.

Before proceeding to the general case, the modulus of order p^2 will be discussed. This case will serve as a guide to the higher orders, and is also interesting as the last in which the basic functions may conveniently be displayed in their entirety.

Theorem 4.1: Let (a,b) be a basis of the modulus M, of order p^2, then:

$$x^{p^2} - \frac{b^{p^2-1} - a^{p^2-1}}{b^{p-1} - a^{p-1}} x^p + a^{p-1}b^{p-1}(b^{p-1} - a^{p-1})^{p-1} x$$

is periodic with period modulus M.

Proof: Denote the function by f(a,b;x). Then, for $m,n \in \Pi$: $f(a,b;x + ma + nb) =$

$$(x+ma+nb)^{p^2} - \frac{b^{p^2-1} - a^{p^2-1}}{b^{p-1} - a^{p-1}} (x+ma+nb)^p$$

$$+ a^{p-1}b^{p-1}(b^{p-1} - a^{p-1})^{p-1} (x+ma+nb)$$

$$= x^{p^2} + ma^{p^2} + nb^{p^2} - \frac{b^{p^2-1} - a^{p^2-1}}{b^{p-1} - a^{p-1}} (x^p + ma^p + nb^p)$$

$$+ a^{p-1}b^{p-1}(b^{p-1} - a^{p-1})^{p-1} (x+ma+nb)$$

$$= x^{p^2} - \frac{b^{p^2-1} - a^{p^2-1}}{b^{p-1} - a^{p-1}} x^p + a^{p-1} b^{p-1} (b^{p-1} - a^{p-1})^{p-1} x$$

$$+ m\left(a^{p^2} - \frac{a^p b^{p^2-1} - a^{p^2+p-1}}{b^{p-1} - a^{p-1}} + a^p b^{p-1} (b^{p-1} - a^{p-1})^{p-1}\right)$$

$$+ n\left(b^{p^2} - \frac{b^{p^2+p-1} - a^{p^2-1} b^p}{b^{p-1} - a^{p-1}} + a^{p-1} b^p (b^{p-1} - a^{p-1})^{p-1}\right)$$

$$= f(a,b;x)$$

$$+ m\left(\frac{a^{p^2} b^{p-1} - a^{p^2+p-1} - a^p b^{p^2-1} + a^{p^2+p-1} + a^p b^{p^2-1} - a^{p^2} b^{p-1}}{b^{p-1} - a^{p-1}}\right)$$

$$+ n\left(\frac{b^{p^2+p-1} - a^{p-1} b^{p^2} - b^{p^2+p-1} + a^{p^2-1} b^p + a^{p-1} b^{p^2} - a^{p^2-1} b^p}{b^{p-1} - a^{p-1}}\right)$$

$$= f(a,b;x).$$

Remarks: 1) At least formally, the requirement that a and b be independent, is unnecessary. Let $c = a^{p-1}$ and $d = b^{p-1}$ in the original expression of the function; the fraction is then: $\frac{d^{p+1} - c^{p+1}}{d-c} = d^p + d^{p-1}c + \cdots + dc^{p-1} + c^p$. Now, if $c = d$, each term is c^p, and the sum is c^p. Therefore the function is, formally, $x^{p^2} - a^{p^2-p} x^p = [f(a;x)]^p$ which is clearly periodic with periods a and $b = ma$.

2) It will be noted that the reserved notation was used for the function just established as doubly periodic. The reason for this notation will be apparent in the immediate sequel.

3) (Cf. remarks following Th. 3.1.) If $a^{p^2-1} = b^{p^2-1}$, $a^{p-1} \neq b^{p-1}$, the middle, or x^p, term will drop out. The final coefficient: $a^{p-1} b^{p-1} (b^{p-1} - a^{p-1})^{p-1}$

$$= a^{p-1} b^{p-1} \left(\frac{b^{p^2-p} - a^{p^2-p}}{b^{p-1} - a^{p-1}} \right) = \frac{a^{p-1} b^{p^2-1} - a^{p^2-1} b^{p-1}}{b^{p-1} - a^{p-1}}$$

$$= - a^{p^2-1}.$$

Thus the function reduces to the degenerate case: $x^{p^2} - a^{p^2-1} x$ of the singly periodic type considered in the corollary.

<u>Theorem 4.2</u>: $f(a,b;x)$ is identically equal to

$$f(f(a;b); f(a;x)) \quad , \text{ i.e. to:}$$

$$(x^p - a^{p-1}x)^p - (b^p - a^{p-1}b)^{p-1} (x^p - a^{p-1}x).$$

Proof: If $a^{p-1} = b^{p-1}$, the theorem is trivial. The term: $(b^p - a^{p-1}b)^{p-1} = 0$, and the formal reduction of $f(a,b;x)$ to $[f(a;x)]^p$ has already been demonstrated.

Now: $(x^p - a^{p-1}x)^p - (b^p - a^{p-1}b)^{p-1} (x^p - a^{p-1}x)$

$$= x^{p^2} - a^{p^2-p} x^p - b^{p-1} (b^{p-1} - a^{p-1})^{p-1} x^p$$

$$+ a^{p-1} b^{p-1} (b^{p-1} - a^{p-1})^{p-1} x$$

$$= x^{p^2} - a^{p^2-p}x^p - b^{p-1}\left(\frac{b^{p^2-p} - a^{p^2-p}}{b^{p-1} - a^{p-1}}\right)x^p$$

$$+ a^{p-1}b^{p-1}(b^{p-1} - a^{p-1})^{p-1}x$$

$$= x^{p^2} - \left(\frac{a^{p^2-p}b^{p-1} - a^{p^2-1} + b^{p^2-1} - a^{p^2-p}b^{p-1}}{b^{p-1} - a^{p-1}}\right)x^p$$

$$+ a^{p-1}b^{p-1}(b^{p-1} - a^{p-1})^{p-1}x$$

$$= x^{p^2} - \left(\frac{b^{p^2-1} - a^{p^2-1}}{b^{p-1} - a^{p-1}}\right)x^p + a^{p-1}b^{p-1}(b^{p-1} - a^{p-1})^{p-1}x$$

$$= f(a,b;x).$$

The function, f(a,b;x), as originally written, is clearly symmetric in a and b if p is odd. The symmetry is also immediate when p = 2 since, in this case, the - signs may be replaced by + signs. The symmetry of the second formulation is not directly evident but is established by the identity just proven.

Corollary: $f(a,b;x) = f(f(a;b);f(a;x)) = f(f(b;a);f(b;x))$.

The substitution operation used here may be compared to the basic operation used by O. Ore[21] in connection with his work on polynomials over a finite field. The polynomials here are p-polynomials in the sense of Ore with coefficients in a finite field. For p^t-polynomials,

Ore defined: $F(x) \times G(x) = F(G(x))$. Here, a double substitution on the two arguments of a single function, $f(a;x)$, is used.

5. The Basic General Periodic Function.

Continuing the process by which $f(a,b;x)$ was obtained from $f(a;x)$ or $f(b;x)$, an extended set of functions may be obtained:

Notation: 1) $f(a_1;x) = x^b - a^{b-1}x$

2) $f(a_1,a_2;x) = f(f(a_1;a_2);f(a_1;x))$

3) $f(a_1,a_2,a_3;x) = f(f(a_1,a_2;a_3);f(a_1,a_2;x))$

. ...

n) $f(a_1,\cdots,a_n;x) = f(f(a_1,\cdots,a_{n-1};a_n);f(a_1,\cdots,a_{n-1};x))$.

Theorem 5.1: $f(a_1,\ldots,a_n;x)$ is independent of the ordering of the a_i; i.e. symmetric in the a_i.

Proof: The theorem has already been noted for the case $n = 2$; assume the theorem proved for all cases $\leq n - 1$, and consider $f(a_1,\ldots,a_n;x)$ and $f(b_1,\ldots,b_n;x)$ where the b's are a new ordering of the a's. Now, $f(b_1,\ldots,b_n;x) =$

$$[f(b_1,\cdots,b_{n-1};x)]^b - [f(b_1,\cdots,b_{n-1};b_n)]^{b-1}\, f(b_1,\cdots,b_{n-1};x).$$

Hence, by the induction hypothesis, the b_i, $i < n$, may be rearranged to fall in the same order as the a's. If $a_i = b_n$, the rearrangement may be carried out so that:

$f(b_1,\ldots,b_n;x) = f(a_1,a_2,\ldots,a_{i-1},a_{i+1},\ldots,a_n,a_i;x)$; and the original function may, by the same reasoning, be rearranged so that: $f(a_1,\ldots,a_n;x) = f(a_1,a_2,\ldots,a_{i-1},a_{i+1},\ldots,a_{n-1},a_i,a_n;x)$. If we designate the two rearranged functions 1) and 2):

$$1) = [f(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n;x)]^p - [f(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n;a_i)]^{p-1} f(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n;x).$$

$$2) = [f(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_{n-1},a_i;x)]^p - [f(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_{n-1},a_i;a_n)]^{p-1} f(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_{n-1},a_i;x).$$

Now let $g(x) = f(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_{n-1};x)$, and expand:

$$1) = [g^p(x) - g^{p-1}(a_n)g(x)]^p - [g^p(a_i) - g^{p-1}(a_n)g(a_i)]^{p-1}[g^p(x) - g^{p-1}(a_n)g(x)].$$

$$2) = [g^p(x) - g^{p-1}(a_i)g(x)]^p - [g^p(a_n) - g^{p-1}(a_i)g(a_n)]^{p-1}[g^p(x) - g^{p-1}(a_i)g(x)].$$

Let $r = [g^{p-1}(a_i) - g^{p-1}(a_n)]$.

Then $1) - 2) = g^p(x)r^p - g^{p-1}(a_i)r^{p-1}[g^p(x) - g^{p-1}(a_n)g(x)] + g^{p-1}(a_n)r^{p-1}[g^p(x) - g^{p-1}(a_i)g(x)]$

$$= r^{p-1}g(x)[g^{p-1}(x)r - g^{p-1}(a_i)g^{p-1}(x) + g^{p-1}(a_i)g^{p-1}(a_n) + g^{p-1}(a_n)g^{p-1}(x) - g^{p-1}(a_n)g^{p-1}(a_i)]$$

$$= r^{p-1} g^p(x) [r - g^{p-1}(a_i) + g^{p-1}(a_n)]$$

$$= r^{p-1} g^p(x) [(r - r)]$$

$$= 0.$$

Thus, since 1) and 2) were (identically) equal to the original functions considered, these functions are also identical, and the theorem is proved.

Theorem 5.2: $f(a_1, \ldots, a_n; x)$ is additive, and linear with respect to Π.

Proof: The theorem has been proved for n = 1; suppose it true for n - 1, and consider $f(a_1, \ldots, a_n; m(x+y))$

$$= [f(a_1, \ldots, a_{n-1}; m(x+y)]^p - [f(a_1, \ldots, a_{n-1}; a_n)]^{p-1} f(a_1, \ldots, a_{n-1}; m(x+y))$$

$$= [mf(a_1, \ldots, a_{n-1}; x) + mf(a_1, \ldots, a_{n-1}; y)]^p$$

$$- [f(a_1, \ldots, a_{n-1}; a_n)]^{p-1} [mf(a_1, \ldots, a_{n-1}; x) + mf(a_1, \ldots, a_{n-1}; y)]$$

$$= mf^p(a_1, \ldots, a_{n-1}; x) + mf^p(a_1, \ldots, a_{n-1}; y)$$

$$- m[f(a_1, \ldots, a_{n-1}; a_n)]^{p-1} [f(a_1, \ldots, a_{n-1}; x) + f(a_1, \ldots, a_{n-1}; y)]$$

$$= m\{f^p(a_1, \ldots, a_{n-1}; x) - [f(a_1, \ldots, a_{n-1}; a_n)]^{p-1} f(a_1, \ldots, a_{n-1}; x)$$

$$+ f^p(a_1, \ldots, a_{n-1}; y) - [f(a_1, \ldots, a_{n-1}; a_n)]^{p-1} f(a_1, \ldots, a_{n-1}; y)\}$$

$$= m[f(a_1, \ldots, a_n; x) + f(a_1, \ldots, a_n; y)].$$

Theorem 5.3: $f(a_1,\ldots,a_n;x)$ is periodic with the period modulus generated by the a_i as basis.

Proof: By Th. 5.2:

$$f(a_1,\ldots,a_n;x+m_1a_1+m_2a_2+\cdots+m_na_n)$$

$$= f(a_1,\ldots,a_n;x)+\sum m_i f(a_1,\ldots,a_n;a_i).$$

Now: $f(a_1,a_2,\ldots,a_n;a_n)$

$$= f^p(a_1,\ldots,a_{n-1};a_n) - f^{p-1}(a_1,\ldots,a_{n-1};a_n)\, f(a_1,\ldots,a_{n-1};a_n)$$

$$= 0.$$

But, by Th. 5.1, $f(a_1,\ldots a_n;x)$ is symmetric in the a_i and, thus, any a_i may be placed in the final position of the period group. Therefore:

$$f(a_1,a_2,\ldots,a_n;a_i) = 0$$

and $$f(a_1,\ldots,a_n;x+\sum m_i a_i) = f(a_1,\ldots,a_n;x).$$

6. The General Representation Theorem.

In the last section, a function, periodic with any desired period modulus, has been exhibited. The further problem of exhibiting all periodic functions with a given period modulus will now be considered together with the relationship between a function periodic over a modulus, M, and one with an associate modulus, bM, where b is an arbitrary non-zero element of the field.

Notation: Let M_n be the modulus generated by $a_1, \ldots, a_n$.

$$f(a_1, \ldots, a_n; x) \equiv f(M_n; x).$$

Theorem 6.1: $f(M_n; cx) = c^{p^n} f(c^{-1} M_n; x)$; c is an arbitrary non-zero element of the field.

Proof: The theorem has been proved for n = 1; assume it for n - 1. $f(a_1, \ldots, a_n; cx)$

$$= [f(a_1, \ldots, a_{n-1}; cx)]^p - [f(a_1, \ldots, a_{n-1}; a_n)]^{p-1} f(a_1, \ldots, a_{n-1}; cx)$$

$$= [c^{p^{n-1}} f(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; x)]^p - [f(a_1, \ldots, a_{n-1}; a_n)]^{p-1} c^{p^{n-1}} f(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; x)$$

$$= c^{p^n} f^p(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; x) - c^{p^{n-1}} f^{p-1}(a_1, \ldots a_{n-1}; a_n) f(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; x).$$

But, $[f(a_1, \ldots, a_{n-1}; a_n)]^{p-1} = [f(a_1, \ldots, a_{n-1}; c\,\tfrac{a_n}{c})]^{p-1}$

$$= [c^{p^{n-1}} f(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; \tfrac{a_n}{c})]^{p-1} = c^{p^n - p^{n-1}} [f(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; \tfrac{a_n}{c})]^{p-1}.$$

Thus, $f(a_1, \ldots, a_n; cx)$

$$= c^{p^n} f^p(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; x) - c^{p^{n-1}} c^{p^n - p^{n-1}} f^{p-1}(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; \tfrac{a_n}{c}) f(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; x)$$

$$= c^{p^n} \left\{ f^p(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; x) - f^{p-1}(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; \tfrac{a_n}{c}) f(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; x) \right\}$$

$$= c^{p^n} f(\tfrac{a_1}{c}, \ldots, \tfrac{a_{n-1}}{c}; x).$$

Theorem 6.2: $\sum_{i=0}^{k} b_i [f(M_n; x)]^i$ is periodic with modulus M_n.

Proof: Evident.

Theorem 6.3: $f(M_n;x) \neq 0$, if $x \notin M$.

Proof: The theorem has been noted for n = 1 in the proof of Th. 3.5. Assume it for n - 1. By the method previously used, if: $f(a_1,\ldots,a_n;b) = 0$,

$f(a_1,\ldots,a_{n-1};b) = mf(a_1,\ldots,a_{n-1};a_n)$.

Then: $f(a_1,\ldots,a_{n-1};b - ma_n) = 0$ by Th. 5.2

and $b - ma_n \in (a_1,\ldots,a_{n-1})$, by induction hyp.;

or $b \in (a_1,\ldots,a_n)$.

Remarks: 1) To this point the theorems deduced in the last two sections have 1) been valid for any commutative field of characteristic p, and 2) not depended on the independence of the a_i. If dependent a_i are included, the resulting function will, in general, be a p^k power of the basic function for the modulus, but the content of the theorems is unchanged.

The following general representation theorem, however, makes use of the elementary fact that a minimal basis exists (components linearly independent with respect to Π), and is valid only over the $GF(p^t)$. This theorem is a generalization of Th. 3.5 in that it gives a constructive method for the representation of any function with a given period modulus in terms of the basic f-function for the modulus.

Th. 3.5, of course, gives a complete representation

theory in the sense that any periodic function over any modulus whatsoever can be represented. The purpose of the next theorem is to provide a representation in terms of functions appropriate to the full modulus.

Theorem 6.4: Any function, $g(x)$ whose period modulus has the basis, $a_1, a_2, \ldots, a_n$, over the $GF(p^t)$, may be represented by:

$$g(x) = \sum_{i=0}^{s-1} b_i [f(a_1, \ldots, a_n; x)]^i, \qquad s = p^{t-n}.$$

Proof: Select a complete basis for the field: $a_1, a_2, \ldots, a_n, c_1, c_2, \ldots, c_{t-n}$. The values of $g(x)$ are completely determined by the values assigned to the p^{t-n} elements: $\sum_{j=1}^{t-n} m_{jk} c_j$, $m_{jk} \in \Pi$. This yields p^{t-n} equations with exactly the same conditions for linearity and non-vanishing determinants as obtained in Th. 3.5. The theorem then follows in precisely the same manner.

7. Other Basic Sets of Functions.

The functions $f(M_w; x)$ used in the previous investigations as the basic functions were chosen for the following reasons:

1) They arise naturally from the important, and 'primitive', periodic function: $x^p - x$.

2) The powers of the f-functions are easily shown

to form a complete basis by means of the Vandermonde determinants which arise.

3) The operation of changing the modulus to a more inclusive one results in a simple and interesting operation on the basic functions.

However, of course, other bases exist. In general, a set, $\phi_1, \ldots, \phi_s$, $s = p^{t-n}$:

$$\phi_j = \sum_{i=0}^{s-1} c_{ji} f^i(M_n; x)$$

will be a basis over M_n if and only if the determinant of the c_{ji} is not zero. If this condition is met, the f^i can be solved for in terms of the ϕ_j. Then, clearly, any function expressed in the f's can be expressed in the ϕ's. On the other hand, if the determinant is zero, the ϕ_j cannot form a complete set since some periodic functions, e.g. the f^i cannot be expressed in terms of the ϕ's.

In the development of general sets of ϕ's, the Vandermonde type of determinant is of greatest interest since this type furnishes a guaranteed non-vanishing condition and, due to the peculiar behavior of additive operations in a GF, is essentially the only such type available.

The primary question regarding a basis for the representation of periodic functions is: "Is the basis orthogonal?" That is, is there an analogue of the fundamental

properties of a set of orthogonal functions in analysis:

$\int \phi_i \phi_j = \delta_{ij}$?

Definition 7.1: A set of functions, $\phi_i(x)$, periodic with a modulus M_n, will be called a completely orthogonal set if:

1) The set forms a complete basis for the representation of all periodic functions with M_n as modulus, and

2) $\sum_{GF} \phi_i \phi_j = 0$ if $i \neq j$, and $\sum_{GF} \phi_i^2 \neq 0$,

the sum being taken over all elements of the $GF(p^t)$.

Theorem 7.1: No completely orthogonal set exists.

Proof: Consider any member of the set, ϕ_i. Since ϕ_i is periodic with M_n as modulus, ϕ_i^2 is also. But then $\sum_{GF} \phi_i^2(x) = 0$, for each value which ϕ_i^2 takes on is assumed p^n times by reason of the periodicity.

This result, however, remains analogous to the results with the usual periodic functions. The orthogonality principle for sin nx, for example, applies solely to integrals (sums) taken over the range of a period, rather than over the whole field.

In this case, a 'period' will correspond to a maximal set for which the function takes on no repeated values which are induced by the periodicity. That is, a set of elements b_i such that no two elements, b_i, b_j, are 'congruent mod M_n'; $b_i - b_j \in M$ implies $i = j$.

The simplest such set is a complement of $M_n, \overline{M_n}$, obtained by writing a complete basis of the field: $a_1, \ldots, a_n, b_1, \ldots, b_{t-n}$, and considering the modulus, $(b_1, \ldots, b_{t-n})$.

Definition 7.2: A period interval is a set of p^{t-n} elements such that the difference of no two of the elements is contained in M_n.

Theorem 7.2: If $\phi(x)$ is any periodic function with modulus M_n, and if $d_1, \ldots, d_{p^{t-n}}$ is any set forming a period interval, then the sum of the values of $\phi(x)$ over the set of the d_i, is equal to the sum over $\overline{M_n} = (b_1, \ldots, b_{t-n}) = b_1, \ldots, b_{p^{t-n}}$.

Proof: It will be sufficient to prove that $\phi(b_i) = \phi(d_i)$ where the d's are, if necessary, reordered.

Now $d_i = b_i + a_i$, where a_i is a member of the M_n, since the complete modulus of the field is the direct sum of M_n and $\overline{M_n}$. Therefore, $\phi(d_i) = \phi(b_i + a_i) = \phi(b_i)$ by the periodicity. Furthermore, the set of b's must be exhausted; for, suppose $d_i = b_i + a_i$, and $d_j = b_i + a_j$, then $d_i - d_j \in M$ contradicting the assumption.

Thus, in the further work, the interval for summation, corresponding to $(-\pi, \pi)$ for sin nx, will be the set $\overline{M_n}$.

Definition 7.3: A basic interval is a complementary group to $M_n, \overline{M_n}$.

Definition 7.4: A set of functions, $\phi_i(x)$, with period modulus M_n, is said to be orthogonal if:

1) The set forms a complete basis for representation of periodic functions with modulus M_n, and

$$2) \quad \sum_{\overline{M_n}} \phi_i(x)\,\phi_j(x) = 0, \qquad i \neq j\,; \quad \sum_{\overline{M_n}} \phi_i^2(x) \neq 0,$$

the summation being taken over all elements of $\overline{M_n}$.

This definition, as will be shown in the next section, is non-vacuous. Orthogonal systems, as defined, exist.

8. Orthogonal Systems of Functions.

Theorem 8.1: The set: $\phi_i(x) = f^{i-1}(M_n;x)$ is not an orthogonal set.

Proof: If the set consists of more than two functions, select i and j so that $i + j = 2k$. Then, if:

$$\sum f^{i+j-2}(M_n;x) = 0 = \sum \phi_i(x)\,\phi_j(x),$$

$$\sum \phi_k^2(x) = \sum f^{2k-2}(M_n;x) = \sum f^{i+j-2}(M_n;x) = 0,$$

contradicting the basic condition. If there are only two functions, 1 and $f(M_n;x)$, theorem 6.4 shows that $f^2(M_n;x)$ is a simple multiple of $f(M_n;x)$ and, thus, the sum of $\phi_1\,\phi_2$ and of ϕ_2^2 will vanish or not vanish together, which is again a contradiction.

Theorem 8.2: For the case $t = 2$, the following set

of functions is orthogonal:

$$\phi_k = \sum_{i=1}^{p} (ka)^{p(p-i)} f^{i-1}(a;x), \qquad k = 1,\ldots,p$$

where we define $0^0 = 1$ to simplify the notation. I.e.,

$$\phi_p = f^{p-1}(a;x).$$

To aid the proof of this theorem, two lemmas will be proved. The first of these is also valid when $t > 2$.

Lemma 1: For all $i < p - 1$, $\sum_{\bar{M}} f^i(a;x) = 0$.

Proof: Select a sub-set of $\bar{M}$, consisting of the multiples of a single element, say b_j, by the elements of Π. Subdivide $\bar{M}$ into mutually exclusive classes whose representatives are $b_k + mb_j$.

The sum of $f^i(a;x)$ over each class is equal to 0, for:

$$\begin{aligned}\sum_{m=0}^{p-1} f^i(b_k + mb_j) &= \sum_{m=0}^{p-1} [f(b_k) + mf(b_j)]^i \\ &= \sum_{m=0}^{p-1} [f^i(b_k) + imf^{i-1}(b_k) f(b_j) + \cdots] \\ &= pf^i(b_k) + if^{i-1}(b_k) f(b_j) \sum m \\ &\quad + \frac{i(i-1)}{2} f^{i-2}(b_k) f^2(b_j) \sum m^2 + \cdots\end{aligned}$$

and $\sum_{m=0}^{p-1} m^j$ is divisible by p when $j < p - 1$.

Lemma 2: For $t = 2$, $\sum_{\bar{M}} f^{p-1}(a;x) \neq 0$.

Proof: If the sum were zero, then, for any function, $g(x)$, with modulus $M = (a)$,

$$\sum_{\bar{M}} g(x) = \sum_{\bar{M}} \sum_{i=0}^{p-1} \alpha_i f^i(a;x) = \sum_i \alpha_i \sum_{\bar{M}} f^i(a;x) = 0.$$

But this is impossible since a function, g(x), periodic with modulus M can be constructed so that the function over $\bar{M}$ has any assigned values whatsoever.

The proof of the original theorem will now be given for p odd. The case 2^2 can be proved in an analogous manner, or simply verified.

1) The set is a basis. The determinant is:

$$\begin{vmatrix} a^{p(p-1)} & a^{p(p-2)} & a^{p(p-3)} & \cdots & 1 \\ (2a)^{p(p-1)} & (2a)^{p(p-2)} & (2a)^{p(p-3)} & \cdots & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ [(p-1)a]^{p(p-1)} & [(p-1)a]^{p(p-2)} & [(p-1)a]^{p(p-3)} & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} = \prod_{m>n} [(m-n)a^p] \neq 0.$$

2) $f^p(a;x) = -a^{p^2-p} f(a;x) = -a^{1-p} f(a;x).$

For, $$(x^p - a^{p-1}x)^p = x^{p^2} - a^{p^2-p}x^p = x - a^{p^2-p}x^p$$

$$= -a^{p^2-p}(x^p - a^{p-1}x).$$

Thus, $f^{2(p-1)}(a;x) = f^p(a;x) f^{p-2}(a;x) = -a^{p^2-p} f^{p-1}(a;x).$

3) $\sum_{\bar{M}} f^i(a;x) = 0, \qquad (p-1) \nmid i$

$\sum_{\bar{M}} f^i(a;x) \neq 0, \qquad (p-1) \mid i.$

The lemmas have shown this for $i \leq p-1$, but 2) demonstrates that all powers of $f(a;x)$ are reducible to powers $\leq p-1$, and that only those powers which are multiples of $p-1$ reduce to $f^{p-1}(a;x)$.

4) Thus, in the expansions of $\phi_k \phi_l$, and ϕ_k^2, reduced by the use of 2), only the coefficients of $f^{p-1}(a;x)$ need be considered. In ϕ_k^2, this coefficient is:

$$\underbrace{2(ka)^{p(p-1)} + 2(ka)^{p(p-1)} + \cdots + 2(ka)^{p(p-1)}}_{\frac{p-1}{2} \text{ terms}} + (ka)^{p(p-1)} - a^{p^2-p}$$

$$= -a^{p^2-p} \neq 0.$$

In $\phi_k \phi_l$, the coefficient is:

$$(ka)^{p(p-1)} + (ka)^{p(p-2)}(la)^p + \cdots + (la)^{p(p-1)} - a^{p^2-p}$$

$$= k^{p-1} a^{p^2-p} + k^{p-2} l a^{p^2-p} + \cdots + l^{p-1} a^{p^2-p} - a^{p^2-p}$$

$$= \frac{k^p - l^p}{k-l} a^{p^2-p} - a^{p^2-p} = 0, \text{ if neither } k \text{ nor } l \text{ is } p.$$

If $k = p$, the coefficient is:

$$(l^{p(p-1)} - 1) a^{p^2-p} = (l^{p-1} - 1) a^{p^2-p} = 0.$$

5) Therefore, $\sum_{\bar{M}} \phi_k^2(x) = \sum_{\bar{M}} (-a^{p^2-p} f^{p-1}(a;x)) \neq 0,$

and $\sum_{\bar{M}} \phi_k(x) \phi_l(x) = 0.$

Thus an orthogonal set has been exhibited for the special case, $n = 1$, $t = 2$. It will be noted that, in place

of the constant which usually begins such a set, there is here the function, $f^{p-1}(a;x)$, which is a constant equal to $-a^{p^2-p}$, by 2) of the above proof, except over the modulus M, where the value is zero.

A complete generalization of this theorem does not exist. The statement is, however, capable of some extension. The simplest case occurs when $\mathbf{M}_n = M_{t-1}$; for then $\bar{M}_{t-1}$ consists of only p elements, and the expansion of $\phi(x)$ in terms of $f(M_{t-1};x)$ also has at most p terms. The following theorem may be obtained:

Theorem 8.3: If t is even, the set:

$$\phi_k = \sum_{i=0}^{p} (k\alpha)^{p-i} f^{i-1}(M_{t-1};x)$$

forms an orthogonal set where α is a fixed element of the $GF(p^t)$.

For the proof of this theorem, lemmas which are extensions of Lemmas 1 and 2 are needed:

Lemma 3: The first p - 2 powers of $f(M_{t-1};x)$ have sum zero over $\bar{M}_{t-1}$, while $f^{p-1}(M_{t-1};x)$ has a non-zero sum.

Proof: $\bar{M}_{t-1}$ consists of the multiples of a single element, b_1, by the elements of Π.

$$f(M_{t-1};mb_1) = mf(M_{t-1};b_1)$$

$$\sum_{\bar{M}_{t-1}} f^i(M_{t-1};mb_1) = \sum_{m} f^i(M_{t-1};mb_1)$$

$$= f^i(M_{t-1};b_1)\sum_m m^i = 0, \quad i < p-1$$

$$\neq 0, \quad i = p-1.$$

Lemma 4: $f^p(M_{t-1};x) = \alpha_0^{p-1} f(M_{t-1};x)$ where α_0 is a fixed element of the $GF(p^t)$.

Proof: By Th. 6.4:

$$f^p(M_{t-1};x) = \sum_{i=0}^{p-1} \beta_i f^i(M_{t-1};x).$$

Clearly, $\beta_0 = 0$, since f^p has no constant term. The highest power of x in: $f^p(M_{t-1};x) = (x^{p^{t-1}} + \gamma_1 x^{p^{t-2}} + \cdots)^p$

is evidently p^{t-1}. If a power higher than the first of $f(M_{t-1};x)$ were present in the expansion of f^p, a higher power of x would occur. Thus:

$$\beta_i = 0, \quad i \neq 1; \quad \text{and} \quad \beta_1 = \gamma_1^p.$$

In the field-identity, $f^p(M_{t-1};x) = \beta_1 f(M_{t-1};x)$, choose a value of x not in M_{t-1}, so that $f(M_{t-1};x) \neq 0$. Then:

$$f^{p-1}(M_{t-1};x) = \beta_1 \text{ and, thus } \beta_1 = \alpha_0^{p-1}.$$

Note: It can easily be shown, though it is not germane to the present theorem, that:

$$\gamma_1 = -\left(a_1^{p^{t-1}-p^{t-2}} + f^{p^{t-2}-p^{t-3}}(a_1;a_2) + f^{p^{t-3}-p^{t-4}}(a_1,a_2;a_3) + \cdots + f^{p-1}(a_1,\ldots,a_{t-2};a_{t-1})\right)$$

where $(a_1,\ldots,a_{t-1})$ is the basis of M_{t-1}.

If and only if t is even, there exists an (at least one) element, c, of the $GF(p^t)$, such that $c^{p-1} = -1$, when p is odd. Let $c\alpha_0 = \alpha$. With this remark, the main theorem is ready for proof:

1) The set forms a basis. This is proved precisely as in Th. 8.2.

2) Again, as in the previous theorem:

$$f^{2(p-1)}(M_{t-1};x) = \alpha_0^{p-1} f^{p-1}(M_{t-1};x)$$

$$= -\alpha^{p-1} f^{p-1}(M_{t-1};x).$$

and $$\sum_{\bar{M}_{t-1}} f^i(M_{t-1};x) = 0, \quad p-1 \nmid i,$$

$$\sum_{\bar{M}_{t-1}} f^i(M_{t-1};x) \neq 0, \quad p-1 \mid i.$$

3) The reduction of $\sum \phi_k^2 \neq 0$, and $\sum \phi_k \phi_l = 0$, again proceed in the manner of Th. 8.2.

This method is clearly not applicable to the case where p and t are odd since no arrangement of the type used can possibly result in a cancellation in the summation of $\sum \phi_k \phi_l$ while retaining a fixed, non-zero, sum in the $\sum \phi_k^2$. The lack of a (p - 1)st root of -1 in these cases has an analogue in the necessary introduction of $i = \sqrt{-1}$ in ordinary analysis. If the $GF(p^t)$ is imbedded in a field where the (p - 1)st root of -1 exists, then the expansion of periodic functions of the given modulus over

the original field is possible in terms of a set of ϕ_k similar to the above, but with coefficients from the super field.

These remarks are not intended to indicate that no orthogonal set exists in the case where t is odd, but merely that the simple sets of Theorems 8.2 and 8.3, yielding Vandermonde determinants in terms of the f's, fail to exist. However, as previously remarked, the Vandermonde determinants offer the only method known to the writer to yield sets which for general values of p and t are guaranteed bases.

Theorem 8.4: When t is odd, no orthogonal set, with a Vandermonde determinant in the f-functions, exists for the representation of functions with modulus M_{t-1}.

Proof: Assume the existence of the set:

$$\phi_k = \beta_k^{p-1} + \beta_k^{p-2} f + \cdots + f^{p-1}.$$

Then the coefficient of f^{p-1} after the reduction of f^{2p-2} in $\phi_k \phi_1$ is:

$$\beta_k^{p-1} + \beta_k^{p-2}\beta_1 + \cdots + \beta_1^{p-1} + \alpha_0^{p-1}$$

which must be zero.

$$\frac{\beta_k^p - \beta_1^p}{\beta_k - \beta_1} + \alpha_0^{p-1} = 0,$$

$$(\beta_k - \beta_1)^{p-1} + \alpha_0^{p-1} = 0.$$

Let $(\beta_k - \beta_1) = x : x^{p-1} = -\alpha_0^{p-1}\,;\, \left(\frac{x}{\alpha_0}\right)^{p-1} = -1,$

which is impossible when t odd for odd primes p.

It might, however, be possible to obtain an orthogonal basis by taking a smaller period modulus. This problem may be illustrated by the case t = 3, n = 1, which will be worked out in detail.

Lemma 5: If t = 3, all powers of f(a;x) less than $p^2 - 1$ have sum zero over $\bar{M}$.

Proof: Let the basis of $\bar{M}$ be (b_1, b_2).

$$f(a; mb_1 + nb_2) = mf(a;b_1) + nf(a;b_2)$$

$$= mc + nd.$$

$$f^i(a; mb_1 + nb_2) = (mc + nd)^i = \sum_{j=0}^{i} \binom{i}{j} c^j d^{i-j} m^j n^{i-j}$$

$$\sum_{\bar{M}} f^i(a; mb_1 + nb_2) = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \sum_{j=0}^{i} \binom{i}{j} c^j d^{i-j} m^j n^{i-j}$$

$$= \sum_{j=0}^{i} \binom{i}{j} c^j d^{i-j} \sum_{m} m^j \sum_{n} n^{i-j}.$$

$\sum m^i = 0$ if $p - 1 \nmid i$, and thus the only cases of concern occur when j and i - j are both divisible by p - 1. This implies that i itself is divisible by p - 1. Let $i = k(p-1)$, and consider $\binom{k(p-1)}{l(p-1)}$, $k > 1$, $k \leq p$.

In the numerator, $[k(p-1)]!$, p will appear k - 1

times, as p, 2p,...,(k - 1)p. In the denominator, p will appear (l - 1) + (k - l - 1) times, or k - 2 times. Therefore the binomial coefficient is divisible by p, and, thus, zero, in the field. The lemma then follows since the smallest power which is not affected by the argument is given by k = p + 1, or i = p^2 - 1.

For this power, the sum over $\bar{M}$ is clearly not zero by an argument of the same type as that given for the (p - 1)st powers in the earlier theorems.

Lemma 6: When t = 3,

$$f^{p^2}(a;x) = -a^{p^3-p^2}f^p(a;x) - a^{p^3-p}f(a;x) = -\frac{f^p(a;x)}{a^{p^2-1}} - \frac{f(a;x)}{a^{p-1}}.$$

Proof: $f^{p^2}(a;x) = x^{p^3} - a^{p^3-p^2}x^{p^2} = -a^{p^3-p^2}x^{p^2} + x.$

$$-a^{p^3-p^2}f^p(a;x) = -a^{p^3-p^2}x^{p^2} + a^{p^3-p}x^p.$$

$$-a^{p^3-p}f(a;x) = -a^{p^3-p}x + x$$

and the lemma follows.

If $\phi_k(x) = \beta_k^{p^{2-1}} + \beta_k^{p^{2-2}}f(a;x) + \cdots + f^{p^{2-1}}(x)$,

these lemmas give sufficient information to obtain the coefficients of interest in the expansion of $\phi_k\phi_1$. When the product is reduced by the application of Lemma 6, the coefficient of $f^{p^{2-1}}(a;x)$ will be:

$$\beta_k^{p^2-1} + \beta_k^{p^2-2}\beta_1 + \cdots + \beta_1^{p^2-1} + \left(-\frac{1}{a^{p^2-1}}\right)\left(\beta_k^{p-1} + \cdots + \beta_1^{p-1}\right) + \left(\frac{-1}{a^{p-1}}\right),$$

which must be zero.

Then

$$\frac{\beta_k^{p^2} - \beta_1^{p^2}}{\beta_k - \beta_1} - \frac{1}{a^{p^2-1}}\left(\frac{\beta_k^p - \beta_1^p}{\beta_k - \beta_1}\right) - \frac{1}{a^{p-1}} = 0$$

or there exist elements, x, such that:

$$x^{p^2-1} - \frac{1}{a^{p^2-1}}\, x^{p-1} - \frac{1}{a^{p-1}} = 0.$$

It is easy to show that this equation is not, in general, solvable in the $GF(p^3)$. In fact, considering the case $a = 1$, and multiplying by x:

$$x^{p^2} - x^p - x = 0 \quad \text{or} \quad x^{p^2} = x^p + x,$$

and

$$x^{p^3} - x^{p^2} - x^p = 0 \quad \text{or} \quad x^{p^2} = -x^p + x.$$

Subtracting,

$$2x^p = 0 \quad \text{or} \quad x = 0,$$

which does not satisfy the original equation.

That the condition $\sum \phi_k^2 \neq 0$ is met by the system is clear if $\beta_k = \beta_1$ in the above. The resulting coefficient is $-a^{p^3-p}$. The set has been chosen in such a way that if $\beta_k \neq \beta_1$, $k \neq 1$, the ϕ_k automatically form a basis. Furthermore, the equation $x^{p^2} - cx^p - dx = 0$ clearly has no

multiple roots in any superfield, and the roots in the splitting field of the equation form a modulus.

Thus, if the $GF(p^3)$ is imbedded in the splitting field of: $x^{p^2}-a^{p^3-p^2}x^p - a^{p^3-p}x = 0$, as a superfield, an orthogonal set will be given by the indicated set of ϕ_k if the β_k are taken as the roots of the equation.

The $\phi_k(x)$ in this case, considered as functions over the original field, are periodic functions with the given modulus, and are then within the scope of Th. 3.5. There is, therefore, a representation of the $\phi_k(x)$ in terms of the $f(a;x)$ with coefficients in the <u>original</u> $GF(p^3)$. Hence, in a sense, an orthogonal set has been demonstrated, although the actual form of the function has not been presented within the given field.

Although the detailed work has been carried out only for the case $t = 3$, the generalization is immediate, and gives as the final major theorem:

<u>Theorem 8.5</u>: In the case $n = 1$, p odd, there exists, in general, no orthogonal set of the type:

$$\phi_k = \sum_{i=1}^{p^{t-1}} \beta_k^{p^{t-1}-i} f^{i-1}(a;x)$$

with β_k in the $GF(p^t)$. However, if the original field is imbedded in the splitting field of:

$$x^{p^{t-1}} - \frac{x^{p^{t-2}}}{a^{p^{t-1}-1}} - \frac{x^{p^{t-3}}}{a^{p^{t-2}-1}} - \cdots - \frac{x}{a^{p-1}} = 0,$$

and the β_k chosen as the roots of this equation, the resulting set furnishes an orthogonal system with respect to the original field for the representation of periodic functions whose modulus contains a, over the GF(p^t).

It may be noted that, in this case, no special results obtain for the even values of t. If t = 4, and a = 1, the defining equation becomes: $x^{p^3} - x^{p^2} - x^p - x = 0$ which, on raising to the p^{th} power, yields:

$$x^{p^4} - x^{p^3} - x^{p^2} - x^p = 0.$$

Thus:

$$x^{p^3} = x^{p^2} + x^p + x$$

$$x^{p^3} = -x^{p^2} - x^p + x$$

$$0 = 2x^{p^2} + 2x^p$$

or $x^{p^2} = -x^p$, and $x^{p^3} = -x$.

Substituting in the original equation:

$$-x + x^p - x^p - x = 0,$$

or x = 0 is the only solution in the field.

9. Miscellaneous Results.

In this section, several results will be presented which, while they have no direct connection with the

development of the main theory, are interesting in themselves or illustrative of that theory.

a. The analogue of the sin nx system.

In the set:

$$\phi_k(x) = (k\alpha)^{p-1} + (k\alpha)^{p-2} f(M;x) + \cdots + f^{p-1}(M;x),$$

a reordering may be made as follows:

$$\begin{aligned}
\psi_0(x) &= && f^{p-1}(M;x) \\
\psi_1(x) &= \alpha^{p-1} + \alpha^{p-2} f(M;x) + \cdots && + f^{p-1}(M;x) \\
\psi_2(x) &= \alpha^{p-1} + 2\alpha^{p-2} f(M;x) + \cdots && + f^{p-1}(M;x) \\
&\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\
\psi_k(x) &= \alpha^{p-1} + k\alpha^{p-2} f(M;x) + k^2\alpha^{p-3} f^2(M;x) + \cdots + f^{p-1}(M;x) \\
&\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots .
\end{aligned}$$

The reordering is made so that for $k \neq 0$, the new ψ_k is equal to the original ϕ_1, where $1 = \frac{1}{k}$ in Π. It is immediately apparent that the above set is identical with the $\phi_k(x)$, and, also, that for $k \neq 0$, $\psi_k(x) = \psi_1(kx)$. Thus an analogy is established between the function, sin x, and $\psi_1(x)$, with the previously noted difference in the replacement of a constant term by the semi-constant, $f^{p-1}(x)$. The function, $\psi_1(x)$, is, in general, neither odd nor even since it is used to represent all periodic functions of the given modulus.

b. The number of periodic functions for given p and t.

The total number of distinct polynomials which may be written for a GF(p^t), subject to the identity, $x^q = x$, where $q = p^t$, is q^q. The question may be asked: How many of these are periodic?

In the expansion of the singly periodic functions, there occur p^{t-1} summands, and the coefficients of each summand may take on p^t values; there are $\frac{p^t-1}{p-1}$ distinct moduli. Thus, there are $\frac{p^t-1}{p-1}(p^t)^{p^{t-1}}$ periodic functions. If the p^t constant functions are discarded, the remainder may be grouped into classes of essentially distinct periodic functions. There are classes of associates, each with $p^t - 1$ members, the classes of functions differing only in the constant term containing p^t members. There then remain:

$$\frac{p^t-1}{p-1}\ \frac{(p^t)^{p^{t-1}}-p^t}{(p^t-1)\,p^t} = \frac{(p^t)^{p^{t-1}}-p^t}{(p-1)\,p^t}.$$

The discussion has included all periodic functions. It is easily seen that, for a given modulus, the number of periodic functions whose modulus contains the given one is $(p^t)^{p^{t-n}}$, where n is the index of the modulus. A similar argument with respect to division into classes may be made. A tabulation for the purpose of comparison is presented in the appendix.

c. Derivatives of periodic functions:

Again in analogy to the usual theory of periodic

functions where the derivatives are also periodic, the question may be raised: Are the formal derivatives of the periodic polynomials over a field of characteristic p also periodic?

This question may easily be answered for Galois fields by consideration of the formal derivative of $f^i(M_n;x)$ which is $i \cdot f^{i-1}(M_n;x) \cdot Df(M_n;x)$. But $Df(M_n;x)$ is simply the coefficient of x in $f(M_n;x)$ since the latter is a p-polynomial. Call that coefficient β, and the result is $i\beta f^{i-1}(M_n;x)$. Since all periodic functions may be expressed as $\sum_i f^i(M_n;x)$, it is clear that the formal derivative of any periodic function is also a periodic function with the same or a more inclusive modulus.

It is pointless to discuss the formal integral of a periodic function since the integral of such a function is not merely indefinite to the point of a constant but to any polynomial consisting of terms of the type x^{np}.

10. Unsolved and Unfinished Problems.

There follows a partial list of problems left unfinished or unsolved by this thesis.

1) Application of the results to higher congruences and diophantine equations.

2) Extension of the representation theory to more general fields of characteristic p. This will require

discussion of the convergence of infinite series of the functions used in this paper in finite sums.

3) Completion of the orthogonal set theory and possible application to algebraically complete fields of characteristic p.

4) Matric discussion of the operators involved and the application of matrices to the orthogonal set theory.

5) The possible existence of a more 'natural' set of functions than the present f-functions for description and representation of the properties of periodic functions. (The ψ_1 function does not meet the condition since it does not exist for all fields and is inherently more complicated than the f's.)

6) The group-theoretic problem in which the functions are considered as endomorphism operators. This problem is closely allied to the first and fourth.

APPENDIX

In this appendix some specific and numerical examples will be given of the functions covered by the main body of the thesis, and a convenient tabulation of the simpler finite fields is presented.

a. Table of finite fields

The following table gives for all p, t = 2, 3, $p^t < 100$, a complete tabular presentation of the $GF(p^t)$ in a double notation for convenience of both addition and multiplication. For each field, an irreducible polynomial of degree t is given in terms of x and as a vector, e.g., $x^2 + x + 1$: (1,1,1). The left hand table gives the vector form of the residues of the basic irreducible polynomial which form the $GF(p^t)$, followed by the first primitive element occuring in the tabulation (designated by 'a') raised to the corresponding exponent. For simplicity both commas and initial zeros are omitted from the vectors, e.g. $x + 1$ is represented by 11. The right hand table gives the exponent of 'a' followed by the vector representation. The two tables thus form a set of 'logs' and 'antilogs' for multiplication, while addition may be performed on the vector set by ordinary addition, reduced for each digit mod p. Starred elements are primitive.

The vector representation also yields a convenient

method for choosing linearly independent sets. Any set of elements, each with a different number of digits in the tabulation, is linearly independent, and any linearly imdependent set is equivalent to a set of this type. These statements may readily be verified by considering the residues which the vectors represent.

Square Fields

2^2:

Vector	Exponent
0	
1	a^3
*10	a
*11	a^2

$x^2 + x + 1$: (1,1,1)

Exponent	Vector
1	10
2	11
3	1

3^2:

Vector	Exponent
0	
1	a^8
2	a^4
10	a^6
*11	a
*12	a^7
20	a^2
*21	a^3
*22	a^5

$x^2 + 1$: (1,0,1)

Exponent	Vector
1	11
2	20
3	21
4	2
5	22
6	10
7	12
8	1

5^2:

Vector	Exponent
0	
1	a^{24}
2	a^{18}
3	a^{6}
4	a^{12}
10	a^{16}
11	a^{20}
*12	a
13	a^{3}
*14	a^{17}
20	a^{10}
21	a^{21}
22	a^{14}
*23	a^{11}
*24	a^{19}
30	a^{22}
*31	a^{7}
*32	a^{23}
33	a^{2}
34	a^{9}
40	a^{4}
*41	a^{5}
42	a^{15}
*43	a^{13}
44	a^{8}

$x^2 + x + 1$: (1,1,1)

Exponent	Vector
1	12
2	33
3	13
4	40
5	41
6	3
7	31
8	44
9	34
10	20
11	23
12	4
13	43
14	22
15	42
16	10
17	14
18	2
19	24
20	11
21	21
22	30
23	32
24	1

7^2:

Vect.	Exp.
0	
1	a^{48}
2	a^{32}
3	a^{40}
4	a^{16}
5	a^{8}
6	a^{24}
10	a^{12}
11	a^{22}
*12	a
*13	a^{29}
*14	a^{35}
*15	a^{31}
16	a^{34}
20	a^{44}
*21	a^{19}
22	a^{6}
23	a^{15}
24	a^{33}
25	a^{18}
*26	a^{13}
30	a^{4}
*31	a^{23}
32	a^{21}
33	a^{14}

Vect.	Exp.
34	a^{26}
35	a^{27}
*36	a^{41}
40	a^{28}
*41	a^{17}
42	a^{3}
43	a^{2}
44	a^{38}
45	a^{45}
*46	a^{47}
50	a^{20}
*51	a^{37}
52	a^{42}
53	a^{9}
54	a^{39}
55	a^{30}
*56	a^{43}
60	a
61	a
*62	a^{7}
*63	a^{11}
*64	a^{5}
*65	a^{25}
66	a^{46}

$x^2 + 1$: (1,0,1)

Exp.	Vect.
1	12
2	43
3	42
4	30
5	64
6	22
7	62
8	5
9	53
10	61
11	63
12	10
13	26
14	33
15	23
16	4
17	41
18	25
19	21
20	50
21	32
22	11
23	31
24	6

Exp.	Vect.
25	65
26	34
27	35
28	40
29	13
30	55
31	15
32	2
33	24
34	16
35	14
36	60
37	51
38	44
39	54
40	3
41	36
42	52
43	56
44	20
45	45
46	66
47	46
48	1

Cubic Fields

2^3: $x^3 + x + 1 : (1,0,1,1)$

Vect.	Exp.
0	
1	a^7
*10	a
*11	a^3

Vect.	Exp.
*100	a^2
*101	a^6
*110	a^4
*111	a^5

Exp.	Vect.
1	10
2	100
3	11

Exp.	Vect.
4	110
5	111
6	101
7	1

3^3: $x^3 + 2x + 1 : (1,0,2,1)$

Vect.	Exp.
0	
1	a^{26}
2	a^{13}
*10	a
*11	a^9
*12	a^3
20	a^{14}
21	a^{16}
22	a^{22}
100	a^2
*101	a^{21}
102	a^{12}
110	a^{10}
111	a^6

Vect.	Exp.
*112	a^{11}
120	a^4
121	a^{18}
*122	a^7
*200	a^{15}
*201	a^{25}
202	a^8
*210	a^{17}
211	a^{20}
*212	a^5
*220	a^{23}
221	a^{24}
*222	a^{19}

Exp.	Vect.
1	10
2	100
3	12
4	120
5	212
6	111
7	122
8	202
9	11
10	110
11	112
12	102
13	2

Exp.	Vect.
14	20
15	200
16	21
17	210
18	121
19	222
20	211
21	101
22	22
23	220
24	221
25	201
26	1

b. The theory applied to the fields, $GF(3^2)$ and $GF(3^3)$.

In the notation of part a of the appendix, choose $M_2 = (11,101)$, $\bar{M}_2 = \Pi$. Also choose $F(0) = 0$, $F(1) = 1$, $F(2) = 2$, and the doubly periodic function becomes:

x	:	0	1	2	10	11	12	20	21	22
F(x):		0	1	2	2	2	1	1	1	2
x	:	100	101	102	110	111	112	120	121	122
F(x):		2	0	1	1	2	0	0	1	2
x	:	200	201	202	210	211	212	220	221	222
F(x):		1	2	0	0	1	2	2	0	1

If the first line only is considered, a periodic function over the $GF(3^2)$ is represented with $M_1 = (11)$; $\bar{M}_1 = \Pi$.

The basic function for the $GF(3^2)$ case is: $x^3 - (11)^2x = x^3 - (20x) = x^3 + (10)x$. The function actually represented is $(12)(x^3 + (10x))$.

The basic function for the $GF(3^3)$ case is:

$$x^9 - \frac{(101)^8 - (11)^8}{(101)^2 - (11)^2} x^3 + (11)^2(101)^2[(101)^2 - (11)^2]^2 x$$

$$= x^9 - \frac{(102) - (211)}{(21) - (121)} x^3 + (121)(21)[(21) - (121)]^2 x$$

$$= x^9 - \frac{(221)}{(200)} x^3 + (202)(120)x$$

$$= x^9 - (11)x^3 + (102)x$$

$$= x^9 + (22)x^3 + (102)x.$$

The function presented is: $(222)[x^9 + (22)x^3 + (102)x]$.

Returning to the $GF(3^2)$,

$f((11);x) = x^3 + (10)x$,

$f^2((11);x) = x^6 + (20)x^4 + 2x^2$.

The orthogonal set, using the ψ -functions, is:

$$\psi_0(x) = f^2((11);x) = x^6 + (20)x^4 + 2x^2$$

$$\psi_1(x) = f^2((11);x) + (11)^3 f((11);x) + (11)^6$$

$$= x^6 + (20)x^4 + (21)x^3 + 2x^2 + (11)x + (10)$$

$$\psi_2(x) = \psi_1(2x)$$

$$= x^6 + (20)x^4 + (12)x^3 + 2x^2 + (22)x + (10).$$

The f-functions, in terms of the ψ -functions, are:

$$1 = (10)(\psi_0 + \psi_1 + \psi_2)$$

$$f((11);x) = (22)(\psi_2 - \psi_1)$$

$$f^2((11);x) = \psi_0.$$

The values of the ψ -functions for $\bar{M}_1$ are:

x	ψ_0	ψ_1	ψ_2	ψ_0^2	ψ_1^2	ψ_2^2	$\psi_0\psi_1$	$\psi_0\psi_2$	$\psi_1\psi_2$
0	0	(10)	(10)	0	2	2	0	0	2
1	(20)	2	1	2	1	1	(10)	(20)	2
2	(20)	1	2	2	1	1	(20)	(10)	2
Totals:				1	1	1	0	0	0

Thus the orthogonal properties are verified for the ψ-functions of the given modulus.

c. The number of periodic functions for certain fields.

Field	Polynomials	Periodic Functions	Classes (Cf. 9b)
2^2	256	48	3
3^2	387,420,489	2916	40
5^2	$8.8 \cdot 10^{34}$	58,593,750	97,656
7^2	$6.6 \cdot 10^{82}$	5,425,784,582,792	2,306,881,200
2^3	16,777,216	28672	511
3^3	$4.4 \cdot 10^{38}$	99,132,767,304,831	141,214,768,240

The table displays the relative rarity of the periodic functions more clearly than the literal relation given in Section 9b. It also shows the large number of functions involved for all but the simplest fields and the rapid increase with the complexity of the field.

BIBLIOGRAPHY

General References

1) Dickson, L. E. - Linear Groups - B. G. Teubner, 1901

2) Speiser, A. - Die Theorie der Gruppen von Endliche Ordnung - Springer, 1927; Dover, 1943

3) van der Waerden, B. L. - Moderne Algebra - Springer, 1931, 1937, 1940; Ungar, 1943

Polynomials over a Finite Field

4) Carlitz, L. - The arithmetic of polynomials in a Galois field - Proc. Nat. Acad. Sci. 17, (120-122) (1931)

5) _____, Am. J. Math. 54, 39-50 (1932)

- On polynomials in a Galois field - Bull. Amer. Math. Soc. 38, 736-744, (1932)

7) - On a theorem of higher reciprocity - Bull. Amer. Math. Soc. 39, 155-160, (1933)

8) - On the representation of polynomials in a Galois field as the sum of an even number of squares - Trans. Amer. Math. Soc. 35, 397-410, (1933)

9) - On polynomials in a Galois field: Some formulae involving divisor functions. Proc. London Math. Soc. IIs 38, 116-124, (1934)

10) Carlitz, L. - On certain functions connected with polynomials in a Galois field - Duke Math. J., 1, 137-168, (1935)

11) - On the representation of polynomials in a Galois field as the sum of an odd number of squares - Duke Math. J., 1, 298-315, (1935)

12) - A theorem on higher congruences - Bull. Amer. Math. Soc., 41, 844-846, (1935)

13) - On certain higher congruences - Bull. Amer. Math. Soc., 41, 907-914, (1935)

14) - On factorable polynomials in several indeterminates - Duke Math. J., 2, 660-670, (1936)

15) - Some formulas for factorable polynomials in several indeterminates. Bull. Amer. Math. Soc., 43, 299-304, (1937)

16) - Criteria for certain higher congruences - Amer. J. Math., 59, 618-628, (1937)

17) - An analogue of the von Staudt-Clausen theorem - Duke Math. J., 3, 503-517, (1937)

18) - Some sums involving polynomials in a Galois field - Duke Math. J., 5, 941-947, (1939)

19) Carlitz, L. - A set of polynomials - Duke Math. J., 6, 486-504, (1940)

20) - Linear forms and polynomials in a Galois field - Duke Math. J., 6, 735-749, (1940)

21) Ore, O. - Contributions to the theory of finite fields - Trans. Amer. Math. Soc., 36, 243-274, (1934)

22) Paley, R. E. A. C. - Theorems on polynomials in a Galois field - Quart. J. Math., Oxford Series 4, 52-63, (1933)

23) Wade, L. I. - Certain quantities transcendental over $GF(p^n,x)$ - Duke Math. J., 701-720, (1941)

24) - _____, II - Duke Math. J., 10, 587-594, (1943)

25) - Two types of function-field transcendental numbers - Duke Math. J., 11, 755-758, (1944)

26) Whiteman, A. - On a theorem of higher reciprocity - Bull. Amer. Math. Soc., 43, 567-572, (1937)

Analogues of Periodic Functions

27) Bell, E. T. - Transcendental numerical functions - to be published in Nat. Math. Mag.

28) Ward, M. - A Calculus of Sequences - Amer. J. Math., 58, 255-266, (1936)

29) Weil, A. - Sur les fonctions elliptiques p-adic - C. R. Acad. Sci., Paris 203, 22-24, (1936)