POLYNOMIAL ISOMORPHISMS OF CAYLEY OBJECTS
OVER A FINITE FIELD

DISSERTATION

Presented to the Graduate Council of the
University of North Texas in Partial
Fulfillment of the Requirements

For the Degree of

DOCTOR OF PHILOSOPHY

By

Hong Goo Park, B.S., M.A.
Denton, Texas
December, 1989
Let $p > 2$ denote the characteristic of the finite field $\text{GF}(p^n)$ for some positive integer $n$. In this dissertation the Bays–Lambossy theorem is generalized to $\text{GF}(p^n)$. The Bays–Lambossy theorem states that if two Cayley objects each based on $\text{GF}(p)$ are isomorphic then they are isomorphic by a multiplier map. We generalize this result to Cayley objects over $\text{GF}(p^n)$ by characterizing all polynomials $f(x)$ of the finite field with the property that for each $\alpha \in \text{GF}(p^n)$ there is an element $\beta \in \text{GF}(p^n)$ such that $f(x) + \alpha = f(x + \beta)$.

We use this characterization to show that under certain conditions two isomorphic Cayley objects over $\text{GF}(p^n)$ must be isomorphic by a function on $\text{GF}(p^n)$ of a particular type. A polynomial representation over $\text{GF}(p^n)$ of the isomorphism is given.

As a special case, two Cayley objects over $\text{GF}(p^2)$ satisfying certain conditions are isomorphic by a quadratic type permutation polynomial over $\text{GF}(p^2)$. 

Park, Hong Goo, *Polynomial Isomorphisms of Cayley Objects over a Finite Field*. Doctor of Philosophy (Mathematics), December, 1989, 60 pp., bibliography, 35 titles.
ACKNOWLEDGMENTS

My first thanks go to my father and my mother. Without their encouragement, I would not have accomplished this work.

I also wish to thank my dissertation advisor N. Brand whose numerous suggestions and criticisms resulted in substantial improvements.

My wife and our two sons, Saechun and Saeil, deserve an accolade for their patience during the time the dissertation was being written.
TABLE OF CONTENTS

Chapter I General Introduction......................... 1
Chapter II Permutations over a Finite Field........... 8
Chapter III Composition with Affine Linear
Polynomials over a Finite Field................. 23
Chapter IV Polynomial Isomorphisms of Cayley
Objects over a Finite Field.................. 41
Bibliography................................................. 57
CHAPTER I

GENERAL INTRODUCTION

The purpose of this dissertation is to study the isomorphisms of two combinatorial objects over a finite field, respectively the polynomial representation of isomorphisms of the objects. First, we introduce the basic definitions which will be employed throughout the chapter.

We denote a combinatorial object of a vertex set \( V \) by a pair \( \mathcal{G} = [V, S] \) where \( V \) is a set called the vertex set, and \( S \) is a subset \( S \subseteq V \cup 2^V \cup 2^2V \cup \ldots \), called the structure. If \( \mathcal{G} \) and \( \mathcal{H} \) are both combinatorial objects, then an isomorphism between \( \mathcal{G} \) and \( \mathcal{H} \) is a bijective function from the vertex set of \( \mathcal{G} \) to the vertex set of \( \mathcal{H} \) which also preserves the structures. An isomorphism from \( \mathcal{G} \) to itself is called an automorphism of \( \mathcal{G} \). It is clear that the set \( \text{Aut}(\mathcal{G}) \) of all automorphisms of \( \mathcal{G} \) constitutes a group under the operation of composition and is a subgroup of the symmetric group \( S_V \) on the vertex set \( V \).

Let \( V \) be a finite group and \( T \) the group of all right translations \( t_\alpha : V \to V \) defined by \( t_\alpha(x) = x + \alpha \) for \( \alpha \in \cdots \)
Then a combinatorial object $\mathcal{G}$ of $V$ is called a Cayley object of $V$ if $\text{Aut}(\mathcal{G}) \supseteq T$ (see Babai [2] for the similar definition).

Bays–Lambossy Theorem and Generalization. In 1930–1931, the first polynomial representation of isomorphisms between two objects was found by Bays [4] and Lambossy [21]. In [4] and [21], they show that

if two Cayley objects of $\text{GF}(p)$ are isomorphic,
then they are isomorphic by multiplier maps; that is, maps of the form $f(x) = ax$ for $a \in \text{GF}(p) \setminus \{0\}$.

To generalize this result, it may be natural to drop the condition that $p$ is a prime in the theorem. In [1], Alspach and Parsons improve the theorem in the case of graphs and digraphs with the vertex set $\mathbb{Z}_{pq}$ for distinct primes $p$ and $q$. There are many papers verifying that the Bays–Lambossy theorem is still true for certain non-prime numbers [2, 16, 17, 31, 32]. From [1, 3, 5, 8, 16, 32], we can see many examples of specific combinatorial objects (or Cayley objects) in which some assumption on $p$ is necessary. Palfy [31] in 1987 solved the problem of determining when the Bays–Lambossy theorem generalizes to arbitrary Cayley objects. He shows in [31] that

the condition "two Cayley objects of a finite group $V$ are isomorphic if and only if
they are isomorphic by a group
automorphism" is satisfied exactly when the
vertex set \( V \) is a group of order 4 or cyclic
of order \( m \) with \( \gcd(m, \phi(m)) = 1 \), where
\( \phi(m) \) is the Euler's \( \phi \)-function.

Isomorphism Problem of Combinatorial Objects. When do
the Bays–Lambossy theorem generalize to a specific Cayley
object such as graphs, digraphs, or designs? The aim of
this dissertation is to investigate the polynomial
representation of isomorphisms between two combinatorial
objects over a finite field in the case that Pálfiy's
conditions are not satisfied; that is, \( \gcd(m, \phi(m)) \neq 1 \) in
Pálfiy's result.

Let a vertex set \( V \) be a finite field \( \text{GF}(p^n) \) with
order \( p^n \) where \( p \) is a prime number > 2 and \( n \) is some
positive integer. Let \( A \) be the group of all invertible
affine linear transformations of \( \text{GF}(p^n) \) viewed as a vector
space over \( \text{GF}(p) \).

Suppose \( \mathcal{G} \) and \( \mathcal{G}' \) are isomorphic Cayley objects over
\( \text{GF}(p^n) \) and \( T \leq P \leq A \), where \( P \) is a Sylow \( p \)-subgroup of
\( \text{Aut}(\mathcal{G}) \). We define a linear operator \( \phi : \text{GF}(p^n) \rightarrow \text{GF}(p^n) \)
by \( \phi(x) = x^p - x \) for all \( x \in \text{GF}(p^n) \).

In a design, the existence of such automorphism groups
was found by Brand ([7, Proposition 3.1]).

Result A. Let \( n = 2 \) and \( p > 2 \). Then, \( \mathcal{G} \) and \( \mathcal{G}' \) with
the above condition are isomorphic by a (permutation) polynomial over \(\text{GF}(p^2)\) of the form
\[
f(x) = a[\phi(\lambda x)]^2 + w(x),
\]
where both \(a\) and \(\lambda\) are some elements of \(\text{GF}(p^2)\), and \(w(x)\) is a polynomial over \(\text{GF}(p^2)\) representing an invertible affine linear transformation over the prime subfield.

Let \(K = \text{GF}(p^n)\) and \(F = \text{GF}(p)\). Then we define an absolute trace \(\text{Tr} = \text{Tr}_{K/F}\) of \(\alpha \in K\) over \(F\) by
\[
\text{Tr}(\alpha) = \sum_{j=0}^{n-1} \alpha^p^j.
\]
From the definition, the absolute trace function \(\text{Tr}\) has the following properties:

(a) \(\text{Tr}(\alpha) \in \text{GF}(p)\), for all \(\alpha \in \text{GF}(p^n)\).

(b) \(\text{Tr}(\alpha^{p^n}) = \text{Tr}(\alpha)\), for all \(\alpha \in \text{GF}(p^n)\).

(c) \(\text{Tr}\) is a linear transformation over the prime subfield.

For an arbitrary \(n\) and \(p > 2\), consider a mapping from \(\mathcal{S}\) to \(\mathcal{S}'\) where \(\mathcal{S}\) and \(\mathcal{S}'\) are both Cayley objects over \(\text{GF}(p^n)\).

Let \(W\) denote the set of all polynomials \(w(x) = \beta + x + \text{Tr}(\gamma x)\) of \(\text{GF}(q)\) where \(\beta \in \text{GF}(p^n)\) and \(\gamma \in \text{Ker}(\text{Tr})\), the kernel of \(\text{Tr}\). We denote by \(\text{Sym}(p^n)\) the symmetric group on the finite field. Suppose that \(\Psi\) is a permutation group in \(\text{Sym}(p^n)\).

A combinatorial object \(\mathcal{S} = [\text{GF}(p^n), S]\) is called a Cayley \(\Psi\)-object over \(\text{GF}(p^n)\) if there exists a Sylow
p-subgroup $P$ of $\text{Aut}(\mathcal{C})$ such that $T \leq P \leq \Psi$. Denote by $f_\varepsilon(x)$ the sum of all even degree terms in a polynomial $f(x)$ over the finite field, and by $f_\sigma(x)$ the sum of all odd degree terms in $f(x)$. Let $\mathcal{F}$ be the set of all polynomials $f(x) \in \text{GF}(p^n, x]$ determined by the following condition:

For each $\alpha \in \text{GF}(p^n)$, there is an element $c \in \text{GF}(p)$ such that $2 \cdot f_\varepsilon(\alpha) = -f_\sigma(c)$.

Result B. Suppose $\mathcal{O}$ is a Cayley $W$–object over $\text{GF}(p^n)$. Then an isomorphism between $\mathcal{O}$ and $\mathcal{Q}$ can be represented by a (permutation) polynomial $f(x)$ in $T_0\mathcal{K}$. 

Idea and Method. We characterize the isomorphism by finding a certain class of permutations (or permutation polynomials of $\text{GF}(p^n)$) on the given finite field such that $\mathcal{O}$ and $\mathcal{Q}$ are necessarily isomorphic by an automorphism in the class. 

Let $P$ be a Sylow p–subgroup of $\text{Aut}(\mathcal{O})$ and $Q \leq \text{Aut}(\mathcal{O})$ be a p–group. Then it is proven in Chapter IV that $\mathcal{O}$ and $\mathcal{O}$ are isomorphic by a permutation in

$$H_Q(P) = \{\pi \in \text{Sym}(p^n) \mid \pi^{-1}Q\circ\pi \leq P\}.$$ 

From the above criteria, we can make sure that there might be an isomorphism between two Cayley objects $\mathcal{O}$ and $\mathcal{O}$ over $\text{GF}(p^n)$ which is in $H_T(P)$.

The idea of the characterization is to construct an
appropriate Sylow p–subgroup $P < \text{Aut}(\mathcal{G})$ and determine the polynomial representation of $\pi$ by reformulating the condition in $H_T(P)$ by means of permutation polynomials of the finite field.

In particular, when $n = 2$ and $p > 2$, the polynomial representation of $\pi$ can be obtained by characterizing all polynomials $f(x)$ of $\text{GF}(p^2)$ such that

$$f(x) + \alpha = f(x + \beta)$$

for fixed $\alpha, \beta \in \text{GF}(p^2)$.

Next we summarize the contents of each chapter.

In chapter II, we study the polynomial representation of permutations over a finite field, respectively cycle permutations. A certain type of regular permutation polynomials in the Betti–Mathieu group $B[p^n,x]$ (see [23, pp. 361–362]) will be studied to construct a $p$–subgroup of $B[p^n,x]$ which may be useful to investigate the cycle structure of the Betti–Mathieu group $B[p^n,x]$.

Chapter III contains mainly combinatorial problems and computational techniques to characterize polynomials $f(x)$ of $\text{GF}(p^n)$ for which $\text{deg}(f) < p^n$ and

$$f(bx + a) = b \cdot f(x) + c$$

for fixed $a, b, c \in \text{GF}(p^n)$. Also the number of such polynomials $f(x)$ satisfying the above conditions will be calculated by using the additive character of the finite
field as an additive group and a result from the wreath product. By Lagrange's Interpolation Formula [15, pp 55], any function from GF($p^n$) to itself can be written by a unique polynomial with degree $< p^n$ (see Dickson [14]). This will be used to characterize the above polynomial $f(x)$.

In Chapter IV, we state and prove the main results as mentioned before by constructing an appropriate Sylow $p$-subgroup $P$ and calculating $H_T(P)$, assuming $\pi(0) = 0$ for $\pi \in H_T(P)$. 
CHAPTER II

PERMUTATIONS OVER A FINITE FIELD

1. Introduction. Let GF(q) denote a finite field with order q, where q = p^n for some prime p and some positive integer n. From the Lagrange Interpolation Formula, it is well-known that any function from GF(q) to GF(q) can be represented by a unique polynomial

\[ f(x) = \sum_{i=0}^{q-1} a_i x^i, \]

where each \( a_i \in GF(q) \). The polynomial \( f(x) \) in (1) is called a permutation polynomial of GF(q) if \( f \), as a function, permutes the elements of GF(q). The set of permutation polynomials of degree \( < q \) under the operation of composition and reduction modulo \( (x^q - x) \), forms a group isomorphic to the symmetric group Sym(q) on GF(q). We denote the ring of all polynomials of GF(q) by GF[q,z].

A number of natural questions arise in connection with permutation polynomials of GF(q). One of the nontrivial problems related to this is the determination of permutation polynomials over finite fields. In general, it is rather complicated to characterize the conditions on
the coefficients for an arbitrary \( f(x) \) in (1) to be a permutation polynomial. Despite many papers on permutation polynomials of a finite field, there are surprisingly few which study the above problem. To deal with this problem, it is natural to seek a polynomial expression of cycle permutations on GF(q). From [24] we can also find many interesting unsolved problems related to permutation polynomials of finite fields.

In section 2, we will describe the polynomial representation of cycle permutations over a finite field by considering a result from Dickson [14, pp. 69–70].

In the same paper, Dickson studied the following polynomial

\[
g(x) = x + a \cdot \sum (bx)^p \in GF[q, x]
\]

initiated by Mathieu [25]. In section 3, by using the additive character of a finite field, we will again characterize the polynomials \( g(x) \). Also an interesting \( p \)-subgroup \( K \) in the Betti–Mathieu group is constructed from \( g(x) \) for \( a = 1 \) and \( b \in \text{Ker}(\text{Tr}) \), i.e., \( K \) consists of polynomials \( g(x) \) which represent regular permutations on \( p^n - p^{n-1} \) elements of GF(q) with \( |K| = p^{n-1} \).

2. Cycle Permutations on GF(q). The first polynomial representation of a transposition on GF(q) appeared in Carlitz [11], 1953. From his paper, we can express every
transposition \((0 \alpha)\) in the symmetric group \(\text{Sym}(q)\) on \(\text{GF}(q)\) as the following polynomial

\[
f(x) = -\alpha^2[[(x - \alpha)^{q-2} + (1/\alpha)]^{q-2} - \alpha]^{q-2}.
\]

In general, by Theorem 2, we can construct the polynomial representations \(f(x)\) of cycle permutations on \(\text{GF}(q)\) for which \(\deg(f) < q - 1\). Before stating the theorem we will require the following known properties of finite fields (see [22]). Recalling that \(c^q = c\) for every \(c \in \text{GF}(q)\), one can readily verify that if a polynomial \(f(x) = 1 - \sum_{i=0}^{q-1} c^{q-1-i}x^i\) then

\[
(2) \quad f(x) = \begin{cases} 1, & \text{for } x = c \\ 0, & \text{for } x \neq c. \end{cases}
\]

From (2) it can be proved that

\section*{Lemma 1 ([22, PP. 191])}

Let \(c_0, c_1, \ldots, c_{q-1}\) be any family of elements in \(\text{GF}(q)\). Then those elements are pairwise distinct if and only if

\[
\sum_{i=0}^{q-1} c_i^t = \begin{cases} 0, & \text{if } t = 0, 1, \ldots, q - 2 \\ -1, & \text{if } t = q - 1 \end{cases}.
\]

\section*{Theorem 2}

Let \(\pi = (c_1 \ldots c_t)\) be a \(t\)-cycle permutation on \(\text{GF}(q)\). For \(0 \leq i \leq q - 2\) and \(1 \leq t \leq q\), let

\[
\delta_i = \sum_{c \in \Delta} \{c - \pi(c)\}c^{q-1-i} \quad \text{and} \quad \sigma_i = \sum_{c \in \Delta} \{\pi(c) - c\}c^{q-1-i},
\]

where \(\Delta = \{c_k \in \text{GF}(q) | 1 \leq k \leq t\}\). Then,

(a) the polynomial representation of \(\pi\) is

\[
f(x) = x + \sum_{i=0}^{q-2} \delta_i x^i,
\]
(b) the polynomial representation of $\pi^{-1}$ is

$$g(x) = x + \sum_{i=0}^{q-2} \sigma_i x^i.$$ 

Proof. Suppose that a polynomial $f(x)$ in (1) represents $\pi$. We put $\Delta' = \{GF(q) \setminus \Delta\}$ and $F = GF(q)$. Dickson showed in his dissertation [14, pp. 69–70] that every permutation polynomial of $GF(q)$ has the degree $\leq q - 2$ and each coefficient of $x^i$-term in (1) can be written by

$$(3) \quad a_i = - \sum_{c \in F} f(c)c^{q-1-i}.$$ 

Since $\Delta'$ is invariant under the permutation $\pi$, (3) implies that

$$(4) \quad a_i = - \sum_{c \in \Delta'} \pi(c)c^{q-1-i} - \sum_{c \in \Delta} \pi(c)c^{q-1-i}$$

$$= - \sum_{c \in \Delta'} \pi(c)c^{q-1-i} + \delta_i,$$ 

Hence, by Lemma 1, $a_i = 1 + \delta_i$ and $a_i = \delta_i$ for $i \neq 1$.

It can be easily checked by (2) that $f(c) = c$ for all $c \in \Delta'$ and

$$f(c_k) = \begin{cases} c_{k+1}, & \text{for } 1 \leq k \leq t-1 \\ c_1, & \text{for } k = t \end{cases}$$

Therefore, $f(x) = x + \sum_{i=0}^{q-2} \delta_i x^i$ is a permutation polynomial of $GF(q)$ and represents a $t$-cycle $\pi \in \text{Sym}(q)$.

Suppose that a polynomial $g(x) \in GF[q,x]$ represents $\pi^{-1}$. 
Since \( \tau^{-1} = (c_t \ldots c_t) \), we can see that if \( b_i \) is the coefficient of \( x^i \)-term in \( g(x) \) with \( 0 \leq i \leq q - 2 \), then

\[
b_i = \begin{cases} 
1 + \sigma_i, & \text{for } i = 1 \\
\sigma_i, & \text{otherwise}
\end{cases} \]

By the same way in the proof of (a), we can see that \( g(x) \) expresses \( \tau^{-1} \). This proved the theorem. \( \square \)

For an example, consider a transposition \( (0\alpha) \in \text{Sym}(q) \). Then \( \delta_i = (\alpha - 0)\alpha^{q-1-i} = \alpha^{q-i} \) for \( i = 0, 1, \ldots, q - 2 \). If \( i = q - 2 \), then \( \delta_{q-2} = \alpha^2 \neq 0 \). So \( (0\alpha) \) can be expressed by a unique permutation polynomial

\[
f(x) = x + (1 + \alpha)x + \alpha^{q-2}x^2 + \alpha^{q-3}x^3 + \ldots + \alpha^{2}x^{q-2} \\
= x + \sum_{i=0}^{q-2} (\alpha^{-1}x)^i.
\]

In general, if a permutation polynomial \( f(x) \) represents a transposition \( (\alpha\beta) \) in \( \text{Sym}(q) \), then \( \deg(f) = q - 2 \) since \( \delta_{q-2} = (\alpha - \beta)^2 \neq 0 \) from Theorem 2. Thus a transposition over a finite field can be expressed by a unique polynomial with degree \( q - 2 \).

**Lemma 3.** Let \( \tau = \prod_{j=1}^{m} \pi_j \), where \( m \) is a positive integer and \( \pi_j \)'s are pairwise disjoint cycles in \( \text{Sym}(q) \). Let \( f_j(x) \) be the permutation polynomial of \( \text{GF}(q) \), representing \( \pi_j \) for \( j = 1, 2, \ldots, m \). Then \( \tau \) can be written by the following permutation polynomial of \( \text{GF}(q) \):

\[
f(x) = (1 - m)x + \sum_{j=1}^{m} f_j(x).
\]
Proof. Suppose that a polynomial \( f(x) \) in (1) represents \( \pi \). Let \( \pi_j = (c_{j,1} \ldots c_{j,t_j}) \in \text{Sym}(q) \) with order \( t_j \) for \( j = 1, 2, \ldots, m \). We denote the orbit of \( \pi_j \) by \( \Delta_j \subset \text{GF}(q) \) and \( \delta_{ij} = \sum_{c \in \Delta_j} \{c - \pi_j(c)\}c^{q^i-1} \).

Then, Theorem 2 implies
\[
\sum_{i=0}^{q^2-2} \delta_{ij} x^i = \sum_{c \in \Delta_j} \{c - \pi_j(c)\}x^i = f_j(x) - x
\]
for each \( j \). By the similar procedure in (4) we can see that if \( \Delta' = \text{GF}(q) \setminus \bigcup_{j=1}^m \Delta_j \) and \( b_i \) is the coefficient of \( x^i \) in \( f(x) \) then
\[
b_i = -\sum_{c \in \Delta'} \pi(c)c^{q^i-1} - \sum_{j=1}^m \sum_{c \in \Delta_j} \{c - \pi_j(c)\}c^{q^i-1} = -\sum_{c \in \Delta'} c^{q^i-1} + \sum_{j=1}^m \delta_{ij}.
\]

By using Lemma 1, \( b_1 = 1 + \sum_{j=1}^m \delta_{ij} \) and \( b_i = \sum_{j=1}^m \delta_{ij} \) for all \( i \neq 1 \). Thus
\[
f(x) = x + \sum_{j=1}^m \{f_j(x) - x\} = (1 - m)x + \sum_{j=1}^m f_j(x).
\]

Remark 1. The polynomial \( f(x) \) in Lemma 3 is a permutation polynomial of \( \text{GF}(q) \) which represents a product of \( m \) disjoint cycles in \( \text{Sym}(q) \). So every permutation over a finite field can be reduced by Theorem 2 and Lemma 3.
Remark 2. Consider a permutation \( \mu \in \text{Sym}(q) \). Then \( \mu \) can be written by a unique product \( \mu_1 \cdots \mu_d \) of disjoint cycles. The type of \( \mu \) is the \( s \)-tuple of integers 
\[
\text{a}(\mu) = (a_1(\mu), a_2(\mu), \ldots, a_s(\mu)),
\]
where each \( a_j(\mu) \) is the number of disjoint cycle factors of length \( j \) in the cycle decomposition. Let 
\[
(5) \quad \sum_{j=1}^{s} j \cdot r_j = r,
\]
where each \( r_j = a_j(\mu) \). Thus the permutation \( \mu \) moves exactly \( r \) elements in \( \text{GF}(q) \). Let \( P_j \) be the product of \( r_j \) cycles of length \( j \) in the decomposition. If \( \mu_{j,k} \) is the \( k \)-th \( j \)-cycle factor in \( P_j \), then
\[
(6) \quad \mu = \prod_{j=1}^{s} P_j = \prod_{j=1}^{s} \prod_{k=1}^{r_j} \mu_{j,k}.
\]
We put \( f_{j,k}(x) \) be a permutation polynomial corresponding to \( \mu_{j,k} \) for each \( j \) and \( k \). To determine a polynomial representation \( f(x) \) of \( \pi \), it is sufficient to find a polynomial representation \( g_j(x) \) of \( P_j \). Note that \( f_{j,k}(x) = x \) for all \( k = 1, \ldots, r_j \). Then, by using Lemma 3,
\[
f(x) = (1 - s)x + \sum_{j=1}^{s} g_j(x)
\]
\[
= (1 - s) \sum_{j=1}^{s} r_j x + \sum_{j=1}^{s} \sum_{k=1}^{r_j} f_{j,k}(x).
\]

3. Regular permutations in the Betti–Mathieu group.
Consider a polynomial
\[
(7) \quad f(x) = \sum_{s=0}^{n-1} \alpha_s x^{2^s} \in \text{GF}[q,x].
\]
The polynomial in (7) is called a p-polynomial of GF(q), and the linear operator on the vector space GF(q) over the prime subfield can be induced by $f(x)$.

The set of all such (linearized) p-polynomials constitutes a subalgebra of the algebra of linear transformations of GF(q) over the prime subfield. The polynomials in (7) were intensively studied by Ore [27] and [28]. Assuming each $\alpha \in GF(p)$, the set of such polynomials is a commutative algebra over GF(p) under the modulo $x^q - x$ operations of addition and composition of functions, and scalar multiplication by elements of GF(p) (see [28]). By Ore [28] it is true that the commutative algebra is isomorphic to $GF[p,x]/(x^n - 1)$. In [9], Ore's result is generalized to an arbitrary subfield of GF(q) under a certain condition on the dimension of the subfield.

It is well-known that the p-polynomial in (7) is a permutation polynomial of GF(q) if and only if the determinant $|\left(\alpha_i^j\right)| \neq 0$ of the following $n \times n$ matrix

\[
\begin{bmatrix}
\alpha_0 & \alpha_1^p & \cdots & \alpha_1^{p^n} \\
\alpha_1 & \alpha_2^p & \cdots & \alpha_2^{p^n} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_{n-1} & \alpha_{n-2}^p & \cdots & \alpha_{n-2}^{p^n}
\end{bmatrix},
\]

where $\alpha_i = \alpha_{n+i}$ for $0 \leq i, j \leq n - 1$ (for the proof, see either [12] or [14]). It is clear that the set $B[q,x]$ of permutation polynomials of GF(q) forms a group under the operation of composition and reduction modulo $x^q - x$. This
is known as the Betti–Mathieu group. The group has the following property proven by Carlitz [12] and Dickson [14]:

\[ B[q, x] \cong GL(n, p), \]

where \( GL(n, p) \) is the general linear group of non-singular \( n \times n \) matrices over \( GF(p) \) under matrix multiplication. It follows from (8) that

\[ |B[q, x]| = p^\sigma \cdot \prod_{i=1}^{n} (p^i - 1) \]

for \( \sigma = n(n - 1)/2 \).

Let \( Tr = Tr_{K/F} \) be the absolute trace function defined in chapter I where \( K = GF(q) \) and \( F = GF(p) \). Denote \( L_\alpha(z) = Tr(\alpha z) \) for \( \alpha \in GF(q) \). Let \( G \) be a finite abelian group with identity element \( 1_G \) and \( \mathbb{C}_* \) the multiplicative group of complex numbers with absolute value 1. The character \( \chi \) of \( G \) is a homomorphism from \( G \) into \( \mathbb{C}_* \), i.e., we define the character \( \chi \) of \( G \) by setting, for all \( \alpha_1, \alpha_2 \in G \),

\[ \chi(\alpha_1 \alpha_2) = \chi(\alpha_1) \cdot \chi(\alpha_2). \]

It is known that the number of characters of a finite abelian group \( G \) is equal to \( |G| \). A character \( \chi \) of \( G \) is called the additive character of \( G \) if and only if \( \chi(\alpha_1 + \alpha_2) = \chi(\alpha_2) + \chi(\alpha_2) \) for all \( \alpha_1, \alpha_2 \in G \).

Let \( p \) be the characteristic of \( GF(q) \). Consider the additive group \( < GF(q), +> \). Then, for all \( \alpha \in GF(q) \), the function \( \chi_1 \) defined by

\[ \chi_1(\alpha) = \exp\left[2\pi i \cdot Tr(\alpha)/p\right] \]

is called a character of \( <GF(q), +> \). Since the absolute
trace function $\text{Tr}_{K/F}$ is a linear transformation from $K$ onto $F$, $\chi_1(\alpha_1 + \alpha_2) = \chi_1(\alpha_1) + \chi_1(\alpha_2)$ for $\alpha_1, \alpha_2 \in \text{GF}(q)$. So $\chi_1$ is an additive character of $\text{GF}(q)$. We refer to $\chi_1$ as the canonical additive character of $\text{GF}(q)$.

Let $\beta \in \text{GF}(q)$. We define a function $\chi_\beta$ by $\chi_\beta(a) = \chi_1(\beta a)$ for all $a \in \text{GF}(q)$. Then we can show that $\chi_\beta$ is an additive character of $\text{GF}(q)$ by using the definition of $\chi_1$. Thus all additive characters of $\text{GF}(q)$ can be represented by $\chi_1$, and $\text{GF}(q)$ has exactly $q$ additive characters since the number of characters of $\text{GF}(q)$ is $|\text{GF}(q)|$. In particular, if $\beta = 0$ then we have the trivial character $\chi_0$ of $\text{GF}(q)$ such that $\chi_0(a) = 1$ for all $a \in \text{GF}(q)$.

For any two elements $a, b \in \text{GF}(q)$, consider a polynomial

$$g(x) = x + a \cdot \sum_{s=0}^{n-1} (bx)^p^s = x + a \cdot L_b(x).$$

Mathieu [25, pp. 294–300] proved the following Theorem 4 which may be useful to characterize the cycle structure of the Betti–Mathieu group. We state the theorem without proof.

**Theorem 4.** All polynomials of the Betti–Mathieu group can be derived from the permutation polynomials $g(x)$ in (11).

Next we will investigate the cycle structure of the
polynomials in (11) by considering the absolute trace function and the additive character of GF(q). First we need to find a necessary and sufficient condition for (11) to be a permutation polynomial of GF(q).

Let GF(q) = GF(q)\{0\}. Then

**THEOREM 5.** Let \( a \) and \( b \) be any two elements of GF(q)*. Consider a polynomial \( g(x) = x + a \cdot L_b(x) \). Then \( g(x) \) represents a permutation on GF(q) if and only if \( a \) and \( b \) satisfies

\[
(12) \quad b \cdot L_{\beta}(a) + \beta \neq 0 \quad \text{for all } \beta \in GF(q)^*.
\]

**Proof.** Suppose that the given polynomial \( g(x) \) is a permutation polynomial of GF(q) with \( a \neq 0 \neq b \). In [23, pp. 350], it is proven that the polynomial \( f(x) \in GF[q,x] \) is a permutation polynomial of GF(q) if and only if

\[
(13) \quad \sum_{c \in GF(q)} \chi_{\beta}(f(c)) = 0
\]

for all nontrivial additive characters \( \chi_{\beta} \) of GF(q). Let GF(q) = \( F \). From [23, pp. 218], for all \( \beta \in GF(q)^* \)

\[
(14) \quad \sum_{c \in F} \chi_{\beta}(g(c))
\]

\[
= \begin{cases} 
q, & \text{if } \beta ab^{n-1} + \beta a^p b^{np^{n-1}} + \ldots + \beta^{p^{n-1}}(1+ab) b^{np^{n-1}} = 0 \\
0, & \text{otherwise}
\end{cases}
\]

Since Tr(\( \beta a \)) \( \in GF(p) \),
\[
\beta a \beta^{n-1} + \beta a \beta^{n-1} + \ldots + \beta a \beta^{n-1} + \beta a \beta^{n-1} \beta a \beta^{n-1} \\
= \text{Tr}(\beta a) \cdot \beta a^{n-1} + \beta a^{n-1} \\
= [b \cdot L_{\beta}(a) + \beta] \beta^{n-1} \\
\neq 0.
\]

Thus, \( b \cdot L_{\beta}(a) + \beta \neq 0 \) for all \( \beta \in \text{GF}(q) \).

On the other hand, if \( g(x) \) satisfies the condition (12), then (14) implies that \( \sum_{c \in F} \chi_{\beta}(c) = 0 \) for all nonzero elements \( \beta \in \text{GF}(q) \). Thus \( g(x) \) is a permutation polynomial of \( \text{GF}(q) \) by (13). \( \square \)

In the next lemma, we will find the cycle structure of permutation polynomials \( g(x) \) in (11).

**Lemma 6.** Let \( a \) and \( b \) be any two elements of \( \text{GF}(q)^* \) and \( g(x) = x + a \cdot L_b(x) \in B[q, z] \). Then

(a) if \( L_b(a) = 0 \), then \( g(x) \) represents a regular permutation on \( p^n - p^{n-1} \) elements of \( \text{GF}(q) \) with the order \( p \), and

(b) if \( L_b(a) \neq 0 \) for some positive integer, then \( g(x) \) represents a regular permutation on \( p^n - p^{n-1} \) elements of \( \text{GF}(q) \) with the order \( k \) where \( k \) is the least positive integer such that \( \{1 + L_b(x)\}^k \neq 1 \).

**Proof.** First we denote \( t \) compositions of \( g(x) \) by \( g^{(t)}(x) \) for any nonnegative integer \( t \). Also we define
\(g^{(0)}(x) = x\). Then, we can show inductively that

\[(15)\]  
\[
g^{(t)}(x) = x + a \cdot A_t \cdot L_b(x),
\]

where

\[
A_t = \sum_{j=0}^{t-1} \binom{t}{j} \cdot \{L_b(a)^{t-j} - 1\}.
\]

Note that the permutation polynomial \(g(x)\) fixes \(p^{n-1}\) elements satisfying \(L_b(x) = 0\) since \(|\text{Ker}(L_b)| = |\text{Ker}(\text{Tr})| = p^{n-1}\).

If \(L_b(a) = 0\), then (15) implies that

\[
g^{(t)}(x) = x + a \cdot t \cdot L_b(x).
\]

Thus the order of \(g(x)\) is \(p\), and so \(g(x)\) represents a regular permutation on \(p^n - p^{n-1}\) elements in \(\text{GF}(q)\) with order \(p\). This proved (a).

Suppose that \(L_b(x) \neq 0\). Because \(g(x)\) is a permutation polynomial of \(\text{GF}(q)\), \(b \cdot L_b(a) + \beta \neq 0\) for all \(\beta \in \text{GF}(q)^{*}\) from Theorem 5. Since \(\beta\) was an arbitrary nonzero element of \(\text{GF}(q)\), \(b\{L_b(a) + 1\} \neq 0\) when \(\beta = b\). So \(L_b(a) \neq -1\). From (15), if \(L_b(a) \neq 0\), then

\[
A_t = [L_b(a)]^{-1} \sum_{j=0}^{t} \binom{t}{j} \cdot L_b(a)^{t-j} - 1
\]

\[
= [L_b(a)]^{-1} \{1 + L_b(a)^t - 1\}.
\]

Let \(k\) be the least positive integer so that

\[\{1 + L_b(a)\}^k = 1.\]

Then \(A_k = 0\) and the order of \(g(x)\) is \(k\). Thus \(g(x)\) represents a regular permutation on \(p^n - p^{n-1}\)
elements with the order $k$ such that $(1 + L_b(a))^k \neq 1.$

Next, we will construct an interesting group consisting of permutation polynomials $g(z)$ in $B[q,z]$.

Consider a polynomial $g(z)$ in (11) when $a = 1$ and $b \in \text{Ker}(\text{Tr})$. Then $b\text{Tr}(\beta) + \beta \neq 0$ for all $\beta \in GF(q)^*$. If not, there exists at least one nonzero element $c \in GF(q)$ such that $b\text{Tr}(c) + c = 0$. This implies that $\text{Tr}(c)\cdot\text{Tr}(b) + \text{Tr}(c) = \text{Tr}(c) = 0$. So $c \in \text{Ker}(\text{Tr})$. By the condition on $c$, $c = 0$ contradicts $c \in GF(q)^*$. Thus a polynomial of the form

$$g(z) = z + L_b(z) \quad (b \in \text{Ker}(\text{Tr}))$$

is a permutation polynomial of $GF(q)$ and an element of $B[q,z]$.

Let $K$ be the set of all permutation polynomials $g(z)$ in (16). Then it is clear that $K$ is a subgroup of $B[q,z]$. And, from (15), we can see that the order of each nontrivial polynomial in $K$ is $p$ and $|K| = |\text{Ker}(\text{Tr})| = p^{n-1}$.

By Lemma 6, each $\varphi(x) \in K$ represents a regular permutation on $p^n - p^{n-1}$ elements of $GF(q)$ with order $p$. Clearly $g(c) = c$ for all $c \in \text{Ker}(L_b)$. Thus we obtain the following Lemma 7.

**Lemma 7.** Let $K = \{g(z) = z + L_b(z) \mid b \in \text{Ker}(\text{Tr})\}$.

Then,

(a) $K$ is a $p$–subgroup of the Betti–Mathieu group and
\[ |K| = p^{n-1}. \]

(b) Every nontrivial polynomial \( g(x) \) in \( K \) represents a regular permutation on \( \text{GF}(q) \setminus \text{Ker}(L_b) \) with order \( p \).
CHAPTER III

COMPOSITION WITH AFFINE LINEAR POLYNOMIALS
OVER A FINITE FIELD

1. Introduction. Let \( q = p^n \) for some prime \( p \) and some positive integer \( n \). In [33] Wells characterized all polynomials over a finite field which commute with translations. Mullen [26] generalized the characterization to linear polynomials over \( \text{GF}(q) \), i.e., he characterized all polynomials \( f(x) \in \text{GF}[q,x] \) for which \( \deg(f) < q \) and \( f(bx + a) = bf(x) + a \) for fixed elements \( a \) and \( b \) of \( \text{GF}(q) \) with \( a \neq 0 \).

In this chapter we will study the polynomials \( f(x) \in \text{GF}[q,z] \) for which \( \deg(f) < q \) and

\[
(1) \quad f(bx + a) = bf(x) + c
\]

for fixed elements \( a, b, \) and \( c \) of \( \text{GF}(q) \) with \( a \neq 0 \neq c \).

Consider an arbitrary function \( \xi: \text{GF}(q) \rightarrow \text{GF}(q) \) from \( \text{GF}(q) \) into \( \text{GF}(q) \). By using the Lagrange's Interpolation Formula for the given function \( \xi \), \( \xi \) can be represented by a polynomial \( g(z) \) of \( \text{GF}(q) \) which is congruent \( \text{(mod} x^q - x) \) to a unique polynomial of \( \text{GF}(q) \) with the degree < \( q \). This
will be used to characterize all polynomials of GF(q) satisfying (1). The characterization will be obtained by equating coefficients in (1) and using a result from the generalized symmetric group (ref. [29] and [30]).

2. Elementary results from \( f(bx + a) = b \cdot f(x) + c \).

Let \( f(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{q-1}x^{q-1} \in \text{GF}[q,x] \). For an obvious case \( b = 0 \), \( f(x) \) satisfies (1) if and only if

\[
b_0 + ab_1 + a^2b_2 + \cdots + a^{q-1}b_{q-1} - c = 0.
\]

It is easy to see, using Lemma 1 below, that the number of polynomials of GF(q) satisfying (1) is exactly \( q^{q-1} \) for \( b = 0 \).

LEMMA 1. Consider a polynomial \( g(x_1, \ldots, x_m) \in \text{GF}[x_1, \ldots, x_m] \) with \( \deg(g) = 1 \). Then the equation \( g(x_1, \ldots, x_m) = 0 \) has \( q^{m-1} \) solutions in \([\text{GF}(q)]^m\).

Proof. Let \( g(x_1, \ldots, x_m) = a_1x_1 + \ldots + a_mx_m + d = 0 \). Since \( \deg(g) = 1 \), there is at least one \( a_k \neq 0 \) for \( 1 \leq k \leq m \). If the values of \( x_i \)'s \((1 \leq i \leq m, i \neq k)\) are given arbitrarily from GF(q), then \( x_k \) is uniquely determined only once. This implies that the above equation has \( q^{m-1} \) solutions over the finite field. \( \square \)

PROPOSITION 2. Suppose that \( b = 1 \) in (1). Then
every polynomial \( f(x) \in \text{GF}[q, x] \) satisfying (1) has either \( \text{deg}(f) = 1 \) or \( \text{deg}(f) \equiv 0 \mod p \).

Proof. Suppose that a polynomial \( f(x) \in \text{GF}[q, x] \) satisfies (1) with degree \( d \) and \( 0 < d < q \). Let \( f(x) = \sum_{s=0}^{d} b_s x^s \) where each coefficient \( b_s \in \text{GF}(q) \). Let \( d_s \) denote the coefficient of \( x^s \) in the polynomial \( f(bx + a) \). Then

\[
 d_s = \sum_{t=s}^{d} \binom{t}{s} b_t a^{t-s}.
\]

By (1) and (2), if \( 1 < d < q \) and \( s = d - 1 \), then \( b_{d-1} = b_{d-1} + db_d a \). Since \( b_d a \neq 0 \), \( d \equiv 0 \mod p \). Otherwise, \( d = 1 \) implies that there are \( q \) polynomials of the type \( a^{-1}cx + a \) for \( c \in \text{GF}(q) \) satisfying (1) for \( b = 1 \).

**THEOREM 3.** Let \( f(x) = \sum_{s=0}^{d} b_s x^s \in \text{GF}[q, x] \) with \( 0 < d < q \).

Then the polynomial \( f(x) \) satisfies condition (1) with \( b = 1 \) if and only if

(a) either \( d = 1 \) or \( d \equiv 0 \mod p \),

(b) \( b_0 = -c + f(a) \), and

\[
 s b_s = \sum_{t=s+1}^{d} \binom{t}{s} b_t a^{t-s},
\]

where \( 0 < s \leq d \) and \( s \) is not divisible by \( p \).

Proof. By Proposition 2 and (2), we can show that (a) and (b) are both necessary if a polynomial of \( \text{GF}(q) \) satisfies the condition (1') which is (1) with
\[ b = 1. \]

On the other hand, suppose that there is a polynomial \( f(x) \) of \( \text{GF}(q) \) satisfying (a) and (b). It can be easily shown that the polynomial \( f(x) \) satisfies (1'). If \( d = \deg(f) < q \), then \( d = 1 \) or \( d = rp \) for some \( r \) with \( 0 < r < p^{n-1} \). If \( d = 1 \), then the number of such polynomials over the finite field is \( q \). Assume that \( d \neq 1 \). If each \( b_s \) is chosen arbitrarily from \( \text{GF}(q) \) for \( s = 0, p, 2p, \ldots, rp \), then the other coefficients can be uniquely determined by (b). Thus the number of such polynomials in (1') is \((q - 1)q^r\) for each fixed \( r \) with \( 1 < r < p \). Since
\[
q + \sum_{r=1}^{p^{n-1}-1} (q - 1)q^r = q^{p^n-1}
\]
and such polynomials exist uniquely, \((q - 1)q^r\) polynomials over \( \text{GF}(q) \) given in (a) and (b) satisfy the condition (1').

The next theorem is a slight generalization of Mullen’s Theorem [26]. The proof Theorem 4 is straightforward from his proof.

**Theorem 4.** The polynomial \( f(x) = \sum_{s=0}^{q-1} b_s x^s \in \text{GF}[q, x] \) satisfies (1) with \( b \neq 0 \) if and only if
\[
(3) \quad b_0 b = -c + f(a),
\[
\]
\[
(b_s (1 - b^{s-1}) = b^{s-1} \sum_{t = s+1}^{q-1} \left( \begin{array}{c} t \\ s \end{array} \right)b_t a^{t-s} \quad (0 < s < q). \]
We will denote by $N(f)$ the number of polynomials $f(x)$ over \( GF(q) \) satisfying condition (1) and by $NP(f)$ the number of permutation polynomials over the finite field satisfying (1) with $\deg(f) < q$.

In the next section, we will calculate $N(f)$ and $NP(f)$ by considering a result from Polya's theory of counting and the concept of wreath product.

3. Computation of $N(f)$ over a finite field. Let $G$ be the permutation group on a finite set $D$ and $H$ the permutation group on a finite set $R$. Let $g$ and $h$ be the fixed elements of $G$ and $H$ where the cycle types of $g$ and $h$ are $(u_1, u_2, \ldots)$ and $(v_1, v_2, \ldots)$. Following deBruijn [13] we define the weight $W(f)$ of any mapping $f$ from $D$ to $R$ by

$$W(f) = \begin{cases} 1, & \text{if } f \text{ is a 1:1 mapping,} \\ 0, & \text{otherwise.} \end{cases}$$

Then it is shown in [13, pp. 171-172] that the number of mappings $f$ so that $fg = hf$ is equal to the sum of $W(f)$ extended over all $f$ that satisfies $fg = hf$; that is,

$$\sum_{f \in \mathcal{N}} W(f) = \prod_{i} \left( \sum_{j} u_{i}^{j} \right)^{v_{i}},$$

where $\mathcal{N}$ is a set of all mappings $f: D \to R$ satisfying $fg = hf$. Let $D = R = GF(q)$ and $g(x) = bx + a$ and $h(x) = bx + c$ where $b \neq 0$. If $b = 1$, then it can be easily shown that $g(x)$ and $h(x)$ represent regular permutations of $GF(q)$ which are both composed of $p^{n-1}$ cycles of length $p$. Thus
(4) implies $N(f) = (pv_b)^{v_p} = q^{p^{n-1}}$.

Suppose now that $b \neq 1$. If $m$ is the multiplicative order of $b$, then $g(x)$ and $h(x)$ represent regular permutations of $\text{Sym}(q)$ which are composed of $(q - 1)/m$ cycles of length $m$, and one fixed point $a/(1 - b)$ for $g(x)$ and $c/(1 - b)$ for $h(x)$. Thus, by (4), $N(f) = (v_1 + mv_m) = q^{um}$ where $v_m = v_m = (q - 1)/m$. This proved

LEMMA 5. Suppose $b = 1$ in (1). Then $N(f) = q^{p^{n-1}}$.

LEMMA 6. Let $m$ be the multiplicative order of $b \neq 1$ in (1). Then $N(f) = q^\kappa$ for $\kappa = (q - 1)/m$.

4. Computation of $NP(f)$ over a finite field. In this section we will compute $NP(f)$ over a finite field by using a result from the wreath product of a finite group by a permutation group $\leq \text{Sym}(q)$. The following definitions and elementary results from wreath products may be found in [19] and [20]. Let $G$ be a permutation group on a set $\Omega$ and $G'$ a permutation group on $\Omega'$. Two permutation groups $G$ and $G'$ are said to be similar if and only if there exists a bijection $\psi: \Omega \to \Omega'$ and an isomorphism $\phi: G \to G'$ satisfying

$$\phi(\pi)(\psi(\omega)) = \psi(\pi(\omega))$$

for all $\pi \in G$ and $\omega \in \Omega$. 
If (5) is to hold, then we will write \( G \cong G' \).

Suppose that \( \Omega \cap \Omega' = \emptyset \). By the direct sum \( G \oplus G' \), we mean the following group action on \( \Omega \cup \Omega' \) defined by
\[
(\pi, \pi')(\omega) = \begin{cases} 
\pi(\omega) & \text{for } \omega \in \Omega \\
\pi'(\omega) & \text{for } \omega \in \Omega'
\end{cases}
\]
for all \((\pi, \pi') \in G \times G'\), the cartesian product of \( G \) and \( G' \). Let \(|\Omega| = k\). A homomorphism \( \varphi \) of a group \( G \) into the symmetric group \( S_k \) is called a permutation representation of \( G \). We also say that \( \varphi \) is a faithful permutation representation of \( G \) if \( \varphi \) is one-to-one, so that \( G \) is mapped isomorphically into \( S_k \) and the Kernel of \( \varphi \) is an identity in \( G \). Let \( \pi \) be an arbitrary element of \( S_k \) and \( C_{S_k}(\pi) \) the centralizer of \( \pi \) in \( S_k \).

Let \( \Delta_i = \{1, \ldots, i\} \subset \Omega \) for \( 1 \leq i \leq k \). In [19, pp. 135], it is shown that
\[
(6) \quad C_{S_k}(\pi) \cong \varphi[C_i \wr S_{a_i}(\pi)]
\]
where \( \varphi \) is a faithful permutation representation of the wreath product of \( C_i = \langle (1, \ldots, i) \rangle \leq S_i \) by \( S_{a_i}(\pi) \), and \( a_i(\pi) \) is the number of \( i \)-cycles in the cycle decomposition of \( \pi \).

Next, consider the permutation polynomials \( f(x) \) of \( \text{GF}(q) \) satisfying condition (1) with \( b \neq 0 \) and \( \deg(f) < q \); that is \( f(bx + a) = bf(x) + c \) for fixed \( a, b, \) and \( c \in \text{GF}(q) \) with \( b \neq 0 \). Let \( g(x) = bx + a \) and \( h(x) = bx + c \).

Then (1) is to hold if and only if \( f^1g(x) = h(x) \).

For a nonzero element \( \beta \in \text{GF}(q) \), we define a mapping
\( \psi_\beta: \text{GF}(q) \to \text{GF}(q) \) by \( \psi_\beta(x) = \beta x \) for all \( x \in \text{GF}(q) \). Then for \( \beta = a^{-1}c \),

\[
(7) \quad (f\psi_\beta)^{-1}g(f\psi_\beta)(x) = \psi_\beta^{-1}h\psi_\beta(x) = g(x)
\]

By \( (7) \), \( f\psi_\beta(x) \in C_Z(g(x)) \) if and only if \( f(x) \in C_Z(g(x)) \circ \psi_{\beta^{-1}} \) where \( Z = S[q,x] \), the set of all permutation polynomials of \( \text{GF}(q) \) which is isomorphic to \( \text{Sym}(q) \). Note that \( a_1(g) = 1, a_m(g) = (q - 1)/m \) and \( a_i(g) = 0 \) for \( i \neq 1 \) or \( m \). Since \( \beta \) was a fixed nonzero element of \( \text{GF}(q) \),

\[
(8) \quad \text{NP}(f) = |C_Z(g(x)) \circ \psi_{\beta^{-1}}| = |C_Z(g(x))| = |C_i| a_i(g) \cdot |S_{a_i(g)}| = m^{\kappa} \cdot (\kappa!)
\]

where \( \kappa = (q - 1)/m \) and \( m \) is the multiplicative order of \( b \) in \( (1) \). By \( (8) \) it is easy to show that if \( b = 1 \) then \( \text{NP}(f) = p^{n-1}(p^{n-1}) \). Since each function from \( \text{GF}(q) \) to itself can be written by a unique polynomial of \( \text{GF}(q) \) with the degree \( < q \), there are exactly \( m^{\kappa} \cdot (\kappa)! \) permutation polynomials of \( \text{GF}(q) \) satisfying \( (1) \).

We have therefore

**Theorem 7.** \( \text{NP}(f) = m^{\kappa} \cdot (\kappa!) \) where \( m = |b| \) and \( \kappa = (q - 1)/m \).
Remark. We can also compute $NP(f)$ over the finite field by using a result from either Polya's Theory of enumeration ([13, pp. 171—172]) or Burnside [10, pp. 224—226] for $b = 1$ and $a = c$.

5. The case $b = 1$ and $\deg(f) < p^2$. Consider a finite field $GF(q)$ where $q = p^n$. Here we will find the exact form of all polynomials $f(x)$ of $GF(q)$ for which $\deg(f) < p^2$ and

\[ f(x + a) = f(x) + c \]

for the fixed nonzero elements $a$ and $c$ in $GF(p^n)$.

We will use the standard convention for binomial coefficients, i.e., $\binom{s}{t} = 0$ if $s < t$. We will require the following known property of binomial coefficients (E. Lucas 1887).

If $s = \sum_{i=0}^{k} s_i p^i$ and $t = \sum_{i=0}^{k} t_i p^i$ $(0 \leq s_i, t_i \leq p - 1)$ are the base $p$ representations for $s$ and $t$, then

\[ \binom{s}{t} \equiv \binom{s_1}{t_1} \binom{s_2}{t_2} \cdots \binom{s_k}{t_k} \pmod{p}, \]

where $p$ is a prime. It is well known that

\[ \binom{s}{t} = \binom{s-1}{t} + \binom{s-1}{t-1}. \]

Let $E_p(m)$ denote the largest exponent $k$ such that $p^k$ divides $m \in \mathbb{N}$, and $d_s$ the sum of the digits in the representation of $s$ written in base $p$.

Let $s = a_0 + a_1 p + \ldots + a_e p^e$ for some $e \in \mathbb{N}$. Then
it is not hard to show that $s - d_s = \sum_{j=0}^{\delta} a_j (p^j - 1)$, and so $(s - d_s)/(p-1) = \sum_{j=1}^{\delta} [s/p^j] = E_p(s!)$ (see [18, pp. 15]). Thus,

\begin{align*}
E_p\left(\frac{s}{t}\right) &= E_p(s!) - E_p((s-t)! - E_p(t!)
\end{align*}

\begin{align*}
&= (d_t + d_{s-t} - d_s)/(p-1). \tag{12}
\end{align*}

If deg$(f) = 1$, then $f(x) \in GF[q,z]$ satisfies (9) if and only if $f(x) = a'cx + u$ for $u \in GF(q)$. So we assume now that deg$(f) \neq 1$.

**THEOREM 8.** Let $f(x) = \sum_{i=0}^{d} b_i x^i \in GF[p^n, x]$ with $d < p^2$.

Then $f(x)$ satisfies (9) if and only if the following conditions holds:

(a) $d = rp$ for $0 < r < p$, and for each fixed $m$ and $k$ with $0 < k < m \leq r$,

\begin{align*}
(m - k)b_{\delta_m}a^p + (k + 1)b_{\delta_m}a &= \begin{cases} c & \text{if } m = 1 \\
0 & \text{otherwise}
\end{cases}
\end{align*}

where $\delta_{mk} = mp - k(p - 1)$.

(b) The other coefficients which do not occur in (a) are all zero.

Proof of Theorem 8. Let $A_i$ denote the coefficient of $x^i$ in the polynomial $f(x + b)$ in (9). Then

\begin{align*}
A_{d-1} = \sum_{j=0}^{\delta} \left(\frac{d-j}{i-j}\right) b_{d-j} a^{i-j}. \tag{13}
\end{align*}

\begin{align*}
(0 \leq i < d)
\end{align*}
Suppose that the polynomial $f(x)$ satisfies the condition (9). From Proposition 2, clearly $d = rp$ for $0 < r < p - 1$. First, we will show part (b) in the theorem.

To do this, we need to find all zero coefficients in $f(x)$ with (9). By using (10) and induction on $i$ with $1 < r < p$,

$$A_{d-2} = \binom{d}{2} b_d a^2 + \binom{d-1}{1} b_{d-1} a + \binom{d-2}{0} b_{d-2}$$

$$= (d - 1) b_{d-1} a + b_{d-2}$$

$$= - b_{d-1} a + b_{d-2}.$$ 

Since $b \neq 0$, (9) implies $b_{d-1} = 0$. Assuming $b_{d-i} = 0$ for $1 < i < p-2$, we can see easily that

$$A_{d-p+1} = \binom{d}{p-1} b_d a^{p-1} + \binom{d-p+2}{1} b_{d} a^{p+2} a + b_{d-p+1}$$

$$= 2 b_{d-p+2} a + b_{d-p+1}.$$ 

So $b_{d-p+2} = 0$. Thus $b_{d-i} = 0$ for all $i = 1, \ldots, p - 2$.

In general we will prove that $b_{d-sp-t} = 0$ for each fixed $s$ and $t$ with $0 < s < r$ and $0 < t < p - s - 1$. Fix $s$ and $t$. Assume that $b_{d-up-v} = 0$ for all $u$ and $v$ satisfying either

(i) $0 \leq u < s < r - 1$ and $0 < v < p - u - 1$, or

(ii) $0 < v < t < p - s - 1$ if $u = s$.

With this assumption we will compute $A_{d-sp-t-1}$. 

Let $z = z(s, t) = sp + t + 1$ for each fixed $s$ and $t$.

Then, by (13) and the inductive hypothesis,

$$A_{d-z} = \sum_{j=0}^{s} \left( \frac{d-j}{z-j} \right) b_{d-j} z^{-j}$$

$$= -ta b_{rp-sp-t} + b_{rp-z} + \sum_{i=0}^{s} \sum_{j=0}^{t} \Delta_z(i,j) \cdot b_{i} d^{-j}$$

where $\Delta_z(i,j) = \left( \begin{array}{c} c \\ y \end{array} \right) = \left( \begin{array}{c} (r-i) + i - j \\ (s-i) + i - j + t + 1 \end{array} \right) = \left( \begin{array}{c} rp - i (p - 1) - j \\ z - i (p - 1) - j \end{array} \right)$.  

So, if $0 < r - i < p$ and $0 \leq s - i < p$ then $d_y + d_{(r - y)} - d_e = p - 1$ implies $E_p[\Delta_z(i,j)] = 1$ by (13).  This says $\Delta_z(i,j) \equiv 0 \pmod{p}$ for the fixed $z$ and each given $i$ and $j$.  Hence, $A_{d-z} = -ta b_{d-z} + b_{d-z}$.  From (9) and the inductive hypothesis, $b_{d-z} = 0$ for every $s$ and $t$ such that $0 \leq s \leq r - 1$ and $0 < t < p - s - 1$.  It is not hard to check that those coefficients run through all coefficients in $j(z)$ except the ones occurring in (a).  This completes the proof of (b) in theorem 8.

To obtain the first part, we first denote by $R_{mk}$ the condition given in part (a) for each $m$ and all $k$'s such that $0 < k < m \leq r$; that is,

$$R_{10} : b_0 a^p + b_1 a = c,$$

$$R_{mk} : (m - k) b_{\delta_{mk}} a^p + (k + 1) b_{\delta_{m,k+1}} a = 0$$
for \( m \neq 1 \).

For each fixed \( m \) and all \( k \)'s with \( 0 < k < m \leq r \), the condition \( \mathcal{R}_{mk} \) will be obtained recursively by using \((11-13)\) and finding a certain pattern of the binomial coefficients given by \( f(x + a) \) in \((9)\). We will see that each condition \( \mathcal{R}_{mk} \) can be derived recursively by computing \( A_{mp-kp-p+k} \) for each fixed \( m \) and all \( k \)'s such that \( 0 < k < m \leq r \).

Suppose that \( m = r \). If \( k = 0 \), then

\[
A_{d-p} = \left(\delta_{rk} \right) b_{\delta_{rk}} a^p + \left(\delta_{r,k+1} \right) \ b_{\delta_{r,k+1},k+1} a + b_{\delta_{r-1,k}}
\]

\[
= r b_{\delta_{r,0}} a^p + b_{\delta_1} a + b_{d-p}.
\]

So the condition \( \mathcal{R}_{r,0} \) is obtained from \((9)\).

In general, let \( z = z(k) = kp + (p - k) \) and

\[
\bar{\Delta}_k(i,j) = \Delta_k(i,j) \cdot b_e a^y = \left(\frac{d-i(p-1)-j}{z-i(p-1)-j} \right) b_e a^y,
\]

where \( e = d-i(p-1)-j \) and \( y = z-i(p-1)-j \) for each fixed \( k = 0, 1, \ldots, r-1 \) and some integers \( i, j \geq 0 \). Then one can see

\[
(17) \quad A_{\delta_{r-1,k}} = \bar{\Delta}_k(k,p-1) + \bar{\Delta}_k(k,p) + \sum_{i=0}^{k} \sum_{j=0}^{i} \bar{\Delta}_k(i,j).
\]

\[
= \bar{\Delta}_k(k,0) + \bar{\Delta}_k(k,p-1) + \bar{\Delta}_k(k,p)
\]

\[
+ \sum_{0 \leq j \leq i \leq k-1} \bar{\Delta}_k(i,j) + \sum_{i=1}^{k} \bar{\Delta}_k(k,j).
\]

Note that \( i-j-k \) is not divisible by \( p \). Since \( -k \leq i-j-k < 0 \) and \( k < p, 0 < p+i-j-k < p \) implies that
$E_p[\Delta_k(i,j)] = \{(k+p-j-k)+(r-1)-(r-j)\}/(p-1)$

Therefore $\Delta_k(i,j) \equiv 0 \pmod{p}$ for each $i, j < k$. By the same way, we can see $\Delta_k(k,j) \equiv 0 \pmod{p}$ for $j = 1, 2, \ldots, k$. Hence

(18) $A_{\delta_{r-1,k}} = (r-k)b_{\delta_{r,k}}^p + (k+1)b_{\delta_{r,k+1}} + b_{\delta_{r-1,k}}$

for each $k = 1, 2, \ldots, r-1$. By equating the coefficients in (9), we get the conditions $\mathcal{R}_{r,k}$ for $0 \leq k < r$.

To obtain the conditions $\mathcal{R}_{uk}$ for $0 \leq k < m < r$, fix $m$ and $k$. Suppose that $\mathcal{R}_{uk}$ is true for each $u$ such that $m < u < r$. Then consider the coefficient of $x^u$ in $f(x + b)$ where $\sigma = \delta_{m-1,k}$. If $m-1 \leq u < r$ and $0 \leq v \leq r-1$ then the binomial coefficient in front of $b_{\delta_{uv}}$ in $A_{\delta_{m-1,k}}$ can be written by

(18') $\Delta_{mk}(u,v) = \left(\binom{u-v}{p} + v\binom{u-v+k-m}{p} + \binom{p-k+v}{p}\right)$.

Let $u' = u - v + k - m$. Since $m - k \leq u - v < r$ and $0 \leq k < m < r$, $0 \leq u' \leq r - (m - k) < p$ for the fixed $m$ and $k$. Thus $\Delta_{uv} \equiv 0 \pmod{p}$ by (12). Also, by (12), if $m - 1 < u \leq m - k$ and $k \leq v \leq k + u - m + 1$, then $E_p[\Delta_{uv}(u,v)] = 1$ implies $\Delta_{uv}(u,v) \equiv 0 \pmod{p}$.

Next choose $u$ and $v$ so that $m + 1 \leq u \leq r$ and $k \leq v \leq u-m+k+1$. Then we denote
Note that each binomial coefficient in (19) is not a zero modulo $p$. Let $B_{u0} = \binom{u-k}{u-m+1}/(u-k)$. Then, by using the induction on $i = 0, 1, \ldots, m' - m$, it is not hard to show that there exists a nonzero number $B_{ui} \in GF(p)$ such that

$$S_{ui} = \sum_{i=0}^{u-m-1} B_{ui} \cdot \left( (u-k-i) \cdot b_{\delta_{u}, k+i} \cdot a^p \right. \left. + (k+i+1) \cdot b_{\delta_{u}, k+i+1} \cdot a \right) \cdot b_{\delta_{u-m}, i}^p$$

where $B_{ui} = \{(u-m-i+1)(k+1)/i(u-k-i)\}B_{ui}$ for $i = 1, \ldots, u - m$.

We denote $R_{mk} = (m-k)b_{\delta_{mk}} \cdot b^p + (k+1)b_{\delta_{m, k+1}} \cdot b$.

By our assumption, each summation $S_{ui} \equiv 0 \pmod{p}$ since

$$S_{ui} = \sum_{i=0}^{u-m} B_{ui} \cdot R_{u, k+i}$$

for each given $u$ and $i$. From (b) in theorem 8,

$$A_{\delta_{m-1}, k} = \left( \frac{\delta_{mk}}{p} \right) b_{\delta_{mk}} \cdot a^p + \left( \frac{\delta_{l} + 1}{i} \right) b_{\delta_{m, k+i}} \cdot a + b_{\delta_{m-1}, k}$$

$$= (m-k)b_{\delta_{mk}} \cdot a^p + (k+1)b_{\delta_{m, k+1}} \cdot a + b_{\delta_{m-1}, k}$$

$$+ \sum_{u=m+1}^{r} \sum_{i=0}^{u-m} S_{ui}.$$
Equating the above coefficients for each fixed \( m \) and all \( k \) with \( 0 \leq k < m < r \) in (9), the conditions \( \mathcal{R}_{mk} \) in (a) of theorem 8 can now be derived. Therefore (a) and (b) in the theorem are both necessary if (9) is to hold.

Suppose that \( f(x) \) is a polynomial satisfying (a) and (b) and \( u = (m-1)p - k(p-1) \). By (22) and (a) in Theorem 8, \( A_u = \mathcal{R}_{mk} + b_u = b_u \) for \( 0 \leq k < m < r \) and \( m \neq 1 \). And if \( m = 1 \), then \( A_0 = b_p + b_0 + b_0 = c + b_0 \). Thus the polynomials given by (a) and (b) in Theorem 8 satisfy (9) and the number of such polynomials is exactly \( p^{np} \).

It follows from (18') and (12) that the proof of the following Corollary 9 is clear.

**COROLLARY 9.** Suppose that a polynomial \( f(x) \in \text{GF}[q,x] \) satisfies (9) with \( \deg(f) < p^2 \). If \( A_{mp-kp+k} \) is a coefficient of \( x^{mp-kp+k} \)-term in \( f(x + a) \) for \( 0 \leq k \leq m \leq r \), then

\[
A_{mp-kp+k} = \begin{cases} 
  b_{mp-kp+k} & \text{if } m = r \\
  (m-k+1)b_u a^p + (k+1)b_v a + b_{mp-kp+k} & \text{otherwise}
\end{cases}
\]

where \( u = (m+1)p - k(p-1) \) and \( v = (m+1)p - (k+1)(p-1) \).

**COROLLARY 10.** In Theorem 8, \( N(f) = 1 + \sum_{k=0}^{p-1} (q - 1)q^k \) = \( p^{np} \) if \( \deg(f) < p^2 \).
Proof. It is clear from Theorem 4 and Theorem 8.

Let $T = \{ t_\alpha : \text{GF}(q) \to \text{GF}(q) \mid t_\alpha(x) = x + \alpha \text{ for } \alpha \in \text{GF}(q) \}$.

**Corollary 11.** The normalizer of $T$ in $S[p^2,x]$ is $\mathcal{N}$ where $S[p^2,x]$ is the set of all permutation polynomials of $\text{GF}(p^2)$ and $\mathcal{N}$ is the group of all affine permutation polynomials of $\text{GF}(p^2)$.

Proof. Let $N(T)$ be the normalizer of $T$ in $S[p^2,x]$. Let $g(x) \in N(T)$. Then, for every $\alpha \in \text{GF}(p^2)$, there is a unique $\beta \in \text{GF}(p^2)$ such that $g(x + \alpha) = g(x) + \beta$. Let $g(x) = a_0 + a_1x + \ldots + a_{q-1}x^{q-1}$ where $q = p^2$. If $\alpha \in \text{GF}(p)$, then $\alpha^p = \alpha$ and (a) in Theorem 8 implies that $(k+1)a_{\sigma_{m,k+1}^\delta} = -(m-k)a_{\sigma_{m,k}^\delta}$ for fixed $m$ and $k$ with $m \neq 1$.

Since $\alpha$ runs through all elements of $\text{GF}(q)$ and $g(x) \in N(T)$, we can choose some $c$ and $d \in \text{GF}(q)$ so that $c^p - c \neq 0$ and $g(x + c) = g(x) + d$ for some $d \in \text{GF}(q)$. By (a), $a_{\sigma_{m,k}^\delta}(c^p - c) = 0$. Thus $a_{\sigma_{m,k}^\delta} = 0$ for $0 \leq k < m \leq r$ with $r \neq 1$. Hence $g(x) = a_0 + a_1x + a_px^p$ and $a_pa^p + a_1\alpha + a_0 = g(\alpha) = \beta$ for all $\alpha \in \text{GF}(p^2)$. Since $g(x)$ is a permutation polynomial of $\text{GF}(p^2)$ and $\beta$ is uniquely determined by $\alpha$ in the finite field, $a_1x + a_px^p \in B[p^2,x]$ and $g(x) \in \mathcal{N}$.

To show $\mathcal{N} \subset N(T)$, let $f(x) = a + bx + cx^p \in \mathcal{N}$. Then
it is sufficient to show that $f^t \alpha f(x) \in N(T)$ for all $\alpha \in GF(q)$. If $f^t(x) = c + dx + ex^p$, then $dc + eb^p = 0$ and $db + ec^p = 1$. From this $f^t \alpha f(x) = x + e\alpha^p \in T$ for all $\alpha \in GF(p^2)$. \(\square\)
CHAPTER IV

POLYNOMIAL ISOMORPHISMS OF CAYLEY OBJECTS
OVER A FINITE FIELD

1. Introduction. Let \( q = p^n \) where \( p > 2 \) is the characteristic of the finite field \( \text{GF}(q) \). Here we prove our main results Theorem 1 and Theorem 2 which generalize previous results of S. Bays [4] and P. Lambossy [21] as stated in chapter I.

Our method is different from the methods of the above mentioned authors. First we explore the fact that there might exist a certain (possibly small) class of automorphisms on \( \text{GF}(q) \) so that any two Cayley objects of \( \text{GF}(q) \) are isomorphic by an element in the class (see Lemma 5). Second we will find the polynomial representation of the isomorphisms by reformulating and characterizing the above fact in terms of permutation polynomials over the finite field by means of the results from chapters II and Chapter III.

2. Definition, terminology, and main Theorems. By an affine \( p \)-polynomial \( w(x) \) over \( \text{GF}(q) \), we mean \( w(x) = f(x) + \)
where \( f(x) \) is a \( p \)-polynomial of \( \text{GF}(q) \) and \( \alpha \in \text{GF}(q) \).

Let \( \mathcal{A} \) denote the set of affine permutation \( p \)-polynomials over \( \text{GF}(q) \); that is, \( \mathcal{A} = T \circ B[q,z] \) is the polynomial representation of \( A \), the group of all invertible affine linear transformations of \( \text{GF}(q) \) over \( \text{GF}(p) \).

Let \( W \) be the group of \( w(x) = \beta + x + L_\gamma(x) \) for \( \beta \in \text{GF}(q) \), \( \gamma \in \text{Ker}(\text{Tr}) \) where \( L_\gamma(x) \) denotes \( \text{Tr}(\gamma x) \).

**DEFINITION.** Let \( \Psi \) be a permutation group in \( \text{Sym}(q) \). A combinatorial object \( \mathcal{C} = [\text{GF}(q), S] \) is called a Cayley \( \Psi \)-object over \( \text{GF}(q) \) if there exists a Sylow \( p \)-subgroup \( P \) of \( \text{Aut}(\mathcal{C}) \) such that \( T \subseteq P \subseteq \Psi \).

Consider a polynomial \( f(x) \in \text{GF}[q,z] \). We denote by \( f_e(x) \) the sum of all even degree terms in \( f(x) \), and by \( f_o(x) \) the sum of all odd degree terms in \( f(x) \). We define a linear operator \( \phi: \text{GF}(q) \to \text{Ker}(\text{Tr}) \) by \( \phi(x) = x^p - x \) for all \( x \in \text{GF}(q) \).

We will denote by \( \mathcal{C} \subseteq \text{GF}[q,z] \) the set of all polynomials \( f(x) \in \text{GF}[q,z] \) determined by the following condition:

For each \( \alpha \in \text{GF}(q) \), there exists an element \( c \in \text{GF}(p) \) such that \( 2 \cdot f_e(\alpha) = -f_o(c) \).

**THEOREM 1.** Let \( \mathcal{C} \) and \( \mathcal{D} \) be any two Cayley objects over \( \text{GF}(p^2) \). Suppose that there is a Sylow \( p \)-subgroup \( P \) of \( \text{Aut}(\mathcal{C}) \) with \( T \subseteq P \subseteq A \). Then \( \mathcal{C} \) and \( \mathcal{D} \) are isomorphic if
and only if they are isomorphic by a permutation polynomial \( f(x) \) over \( \text{GF}(p^2) \) of the form

\[
f(x) = a[\phi(\lambda x)]^2 + w(x)
\]

for some elements \( a \) and \( \lambda \) in \( \text{GF}(p^2) \), and an affine \( p \)-polynomial \( w(x) \) in \( \mathcal{A} \).

As mentioned in chapter I, we will solve the isomorphism problem in the case that \( \mathcal{O} \) is a Cayley \( \mathcal{W} \)-object over \( \text{GF}(q) \).

**Theorem 2.** Let \( \mathcal{O} \) and \( \mathcal{O'} \) be any two isomorphic Cayley objects over \( \text{GF}(q) \). Suppose that \( \mathcal{O} \) is a Cayley \( \mathcal{W} \)-object over \( \text{GF}(q) \). Then an isomorphism from \( \mathcal{O} \) to \( \mathcal{O'} \) can be represented by a permutation polynomial \( f(x) \) in \( \text{To} \mathcal{F} \subset \text{GF}[q, z] \).

3. Preliminaries. By \( \phi(f) \), we mean the cycle type of a permutation polynomial \( f(x) \) of \( \text{GF}(q) \). For a polynomial \( f(x) \in \text{GF}[q, z] \), \( f^{(m)}(x) \) denotes \( m \) compositions of \( f(x) \); that is,

\[
f^{(m)}(x) = \underbrace{f \circ f \circ \cdots \circ f}_m(x) = f(f(\cdots f(x)\cdots)).
\]

And the order \( |f| \) of \( f(x) \) is the least positive integer \( m \) such that \( f^{(m)}(x) \equiv x \pmod{x^q - x} \).

**Lemma 3.** Let \( \beta \in \text{GF}(q) \). Consider an affine \( p \)-polynomial \( w(x) = \beta + x + L_\gamma(x) \) of \( \text{GF}(q) \). Then,

(a) \( w(x) \in \mathcal{A} \) if and only if, for every \( c \in \text{GF}(q)^\star \), \( \gamma \cdot L_\gamma(c) \)
+ c \neq 0.

(b) If \( w(x) \in \mathcal{A} \setminus \{x\} \), then \(|w| = p\). (c) \( W = \{w(x) = \beta + x + L_{\gamma}(x) \in \mathcal{A} \mid \beta \in \text{GF}(q) \text{ and } \gamma \in \text{Ker}(Tr)\} \) is a \( p \)-subgroup of \( \mathcal{A} \).

Proof. (a) Let \( h(x) = x + L_{\gamma}(x) \). Since \( w(x) = t^{\beta}h(x) \) and \( t^{\beta}(x) \) represents a permutation over \( \text{GF}(q) \), it is clear that \( w(x) \) is a permutation polynomial of \( \text{GF}(q) \) if and only if \( h(x) \) is a permutation polynomial. So the necessary and sufficient condition in (a) follows from Theorem 5, chapter II.

(b) Let \( w(x) = \beta + x + L_{\gamma}(x) \in W \). Then

\[
\begin{align*}
 w^{(m)}(x) &= x + m \cdot L_{\gamma}(x) + \sum_{j=0}^{m-1} \{\beta + j \cdot L_{\gamma}(\beta)\} \\
&= m\beta + \{m(m - 1)/2\} \cdot L_{\gamma}(\beta) + x + m \cdot L_{\gamma}(x).
\end{align*}
\]

Since \( m = p > 2 \) is the least number so that \( w^{(m)}(x) = x \), \(|w| = p\).

(c) To see \( W \leq \mathcal{A} \), it is sufficient to show that, for any two element \( w_1(x) = \beta_1 + x + L_{\gamma_1}(x) \) and \( w_2(x) = \beta_2 + x + L_{\gamma_2}(x) \) in \( W \), \( w_1(w_2(x)) \in W \). Since \( w_1(w_2(x)) = c + x + L_{\eta}(x) \) for \( c = \beta_1 + \beta_2 + L_{\gamma_1}(\beta_2) \in \text{GF}(q) \) and \( \eta = \gamma_1 + \gamma_2 \in \text{Ker}(Tr) \), \( W \leq \mathcal{A} \). Since the order of any \( w \in W \setminus \{x\} \) is a power of \( p \) by (b), it follows from the Cauchy's theorem in group theory that \( W \) is a \( p \)-group in \( \mathcal{A} \).

Lemma 4. Let \( w(x) = \beta + x + L_{\gamma}(x) \in W \setminus \{x\} \) where \( W \)
is the group defined in Lemma 3, (b). Then,

(a) $\beta \in \text{GF}(p)$ and $\gamma \neq 0$ if and only if $w(x)$ is composed of $p^{n-1} - p^{n-2}$ disjoint cycles of length $p$.

(b) Either $\beta \in \text{GF}(q)$ and $\gamma = 0$, or $\beta \notin \text{GF}(p)$ and $\gamma \neq 0$ if and only if $w(x)$ is composed of $p^{n-1}$ disjoint cycles of length $p$.

Proof. (a) Suppose that $\beta \in \text{GF}(p)$ and $\gamma \in \text{Ker}(\text{Tr}) \setminus \{0\}$. Consider a polynomial $w(x) = \beta + x + L_\gamma(x) \in W \setminus \{x\}$. If $w(\alpha) = \alpha$ for an element $\alpha \in \text{GF}(q)$, then $\beta + L_\gamma(\alpha) = 0$. Since $L_\gamma$ is a linear transformation of $\text{GF}(q)$ over $\text{GF}(p)$, we can choose an element $c$ such that $L_\gamma(c) = \beta$. So, $L_\gamma(c + \alpha) = 0$. Then $\gamma(c + \alpha) \in \text{Ker}(\text{Tr})$ if and only if $\alpha = \gamma^{-1}\eta - c$ for each $\eta \in \text{Ker}(\text{Tr})$. So $w(x)$ fixes $p^{n-1}$ elements of $\text{GF}(q)$ and it is composed of $p^{n-1} - p^{n-2}$ cycles of length $p$ since $|w| = p$.

Conversely, if $w(x)$ is composed of $p^{n-1} - p^{n-2}$ disjoint cycles of length $p$, then $\gamma \neq 0$ and there is an element $\alpha \in \text{GF}(q)$ such that $w(\alpha) = \alpha$. This implies $\beta = -L_\gamma(\alpha) \in \text{GF}(p)$.

(b) It is noted that either $\beta \in \text{GF}(q)$ and $\gamma = 0$, or $\beta \notin \text{GF}(p)$ and $\gamma \neq 0$ if and only if there is no fixed element under $w(x)$. Since $|w| = p$ by (b) in Lemma 3, the above sufficient condition is true if and only if $w(x)$ is composed of $p^{n-1}$ disjoint cycles of length $p$; that is,
\[ a(w) = a(x + \beta). \]

4. Key Lemmas. We will usually write our operators on the left. Let \( Y \) be a subset of a group \( G \) and \( y \in Y, g \in G \). Then we will use the exponential notation \( Y^g \) for \( g^{-1}Yg \), and \( y^g \) for \( g^{-1}yg \).

Let \( G_1 \) and \( G_2 \) be permutation groups contained in the symmetric group \( S_V \) on a set \( V \). We denote a set \( H_{G_1}(G_2) = \{ x \in S_V \mid G_1^x < G_2 \} \). From the following Lemma 5, we will see the existence of isomorphisms between two combinatorial objects over \( GF(q) \). The proof is based on N. Brand [6].

**Lemma 5.** Suppose that \( \mathcal{G} \) and \( \mathcal{H} \) are isomorphic combinatorial objects of a vertex set \( V \). Let \( P \) be any Sylow p–subgroup of \( Aut(\mathcal{G}) \) and \( Q \) a p–group in \( Aut(\mathcal{H}) \). Then \( \mathcal{G} \) and \( \mathcal{H} \) are isomorphic by an element in \( H_Q(P) \).

**Proof.** Let a mapping \( \xi : V \to V \) be an isomorphism from \( \mathcal{G} \) onto \( \mathcal{H} \). \( P^{\xi^{-1}} \) is a Sylow p–subgroup of \( Aut(\mathcal{H}) \). Let \( Q' \) be any Sylow p–subgroup of \( Aut(\mathcal{H}) \) with \( Q < Q' \). By the Sylow theorem, there exists an automorphism \( \varphi \in Aut(\mathcal{H}) \) such that \( Q' \varphi^{-1} = P^{\xi^{-1}} \). Thus \( Q' \varphi^{-1} \subseteq P^{\xi^{-1}} \) if and only if \( Q' \varphi^{-1} \subseteq P \). Hence \( \varphi^{-1} \xi \in H_Q(P) \) and it is an isomorphism from \( \mathcal{G} \) onto \( \mathcal{H} \) since \( f \) is an isomorphism from \( \mathcal{G} \) onto \( \mathcal{H} \).
onto \( \mathcal{S} \) and \( \varphi^{-1} \in \Aut(\mathcal{S}). \)

Next we will reformulate Lemma 5 in terms of permutation polynomials of \( \GF(q) \). Let \( V = \GF(q) \) and \( S[q,z] \) the group of permutation polynomials of \( \GF(q) \). If two combinatorial objects over \( \GF(q) \) are isomorphic, then the above lemma says that they are isomorphic by a function in \( H_Q(P) \). By Lagrange's Interpolation Formula, the function can be represented by a unique permutation polynomial \( f(z) \) over \( \GF(q) \) with \( \deg(f) < q - 1 \) and

\[
f(z) \in H_{\mathcal{S}}(\mathcal{P}) = \{h(z) \in S[q,z] | \mathcal{L}^h < \mathcal{P}\}
\]

where \( \mathcal{P} \) and \( \mathcal{L} \) are the polynomial representations over \( \GF(q) \) of \( P \) and \( Q \).

This is quite natural because \( \Aut(\mathcal{S}) \triangleq \Sym(q) \triangleq S[q,z] \).

Consider the group \( W = \{w(x) = \beta + x + L_\gamma(x) \in \mathcal{M} | \beta \in \GF(q), \gamma \in \Ker(Tr)\} \) and \( T = \{t_\alpha : \GF(q) \rightarrow \GF(q) | t_\alpha(x) = x + \alpha \text{ for } \alpha \in \GF(q)\} \).

**Lemma 6.** If \( f(x) \in H_T(W) \), then \( f(x + c) = f(x) + f(c) - f(0) \) for every \( c \in \GF(p) \).

**Proof.** Suppose that \( f(x) \in H_T(W) \). Then, for each \( \alpha \in \GF(q) \), we can choose a unique \( w(x) = \beta + x + L_\gamma(x) \in W \) such that \( \alpha(t_\alpha) = \alpha(w) \) and

\[
(1) \quad f(x) + \alpha = f(\beta + x + L_\gamma(x)).
\]
If \(c\) is an element of \(\text{GF}(p)\), then there is an element \(b \in \text{GF}(q)\) with \(L_\gamma(b) = c\) since \(L_\gamma\) is a linear transformation from \(\text{GF}(q)\) onto \(\text{GF}(p)\). It follows from (1) that
\[
f(c) + a = f(\beta + c + L_\gamma(L_\gamma(d))) = f(\beta + c).
\]

Also (1) implies \(a = f(\beta) - f(0)\) when \(x = 0\). So \(f(c) + f(\beta) - f(0) = f(\beta + c)\) for \(c \in \text{GF}(p)\). Since \(\beta\) is uniquely determined by \(\alpha\) and runs through all elements of \(\text{GF}(q)\), \(f(x) + f(c) - f(0) = f(x + c)\) for every \(c \in \text{GF}(p)\).

5. Proof of Theorem 1. For \(q = p^2\), let \(\mathcal{C}\) and \(\mathcal{S}\) be two isomorphic Cayley objects over \(\text{GF}(q)\). Suppose that \(P\) is a Sylow \(p\)-subgroup of \(\text{Aut}(\mathcal{S})\) such that \(T < P < \mathcal{A}\). Let \(\mathcal{P}\) denote the polynomial representation over \(\text{GF}(q)\) of \(P\).

By Lemma 5, an isomorphism of \(\mathcal{C}\) and \(\mathcal{S}\) can be expressed by a permutation polynomial \(f(x)\) in \(\mathcal{H}_T(\mathcal{P})\) with \(\deg(f) < p^2 - 1\) since \(\mathcal{S}\) is a Cayley object over \(\text{GF}(p^2)\).

Consider the permutation polynomial group \(W\) defined in Lemma 3 for \(n = 2\). Since \(|W| = p^3\) and \(|\mathcal{A}| =

\[|T|B[p^2,x]| = p^3 \prod_{i=1}^{2}(p^i - 1), \quad W \leq \mathcal{A}\]
implies that \(W\) is a Sylow \(p\)-subgroup of \(\mathcal{A}\). Since \(\mathcal{P}\) is a \(p\)-subgroup of \(\mathcal{A}\), there exists a Sylow \(p\)-subgroup \(\mathcal{H}\) of \(\mathcal{A}\) such that \(T < \mathcal{P} < \mathcal{H}\). By the Sylow theorem we can choose a polynomial \(\psi(x) \in \mathcal{A}\) so that \(T^{\psi^{-1}} < \mathcal{H}^{\psi^{-1}} < \mathcal{H}^{\psi^{-1}} = W\). Since \(\psi(x) = \ell(x) + c\) for some \(c \in \text{GF}(p^2)\) and some permutation \(p\)-polynomial \(\ell(x)\)
\[ \in B[p^2,x], \ T^f < W^\psi = [W^{\psi^t}]^t = W^t \text{ if and only if } T^R^{-1} < W. \]

Thus \( f(x) \) can be written by a polynomial of the form \( g(x) \) for \( g(x) \in H_T(W) \).

Next we will characterize the set \( H_T(W) \).

Let \( g(x) \in H_T(W) \). If \( h(x) = g(x) - g(0) \), then \( h(x) = T^{-1} c g(x) \) for \( c = g(0) \) and \( T^h = [T^{-1} c] g = T^g < W \) since \( T \) is commutative. Thus it is sufficient to find all polynomials \( h(x) \) of \( GF(p^2) \) for which \( h(0) = 0 \) and

\[
T^h < W.
\]

If \( W_0 = \{ w(x) = \beta + z + L_\gamma(x) \in W \mid \beta \in GF(p) \text{ and } \gamma \in \text{Ker}(T^e) \setminus \{0\} \} \), then \( T^h \in \{ W \setminus W_0 \} = W_* \) by Lemma 4. So \( H_T(W) = H_T(W_*) \). Then, for each \( \alpha \in GF(p^2) \), there exists a unique polynomial \( w(x) = \beta + z + L_\gamma(x) \in W_* \) such that \( t^h_\alpha(x) = w(x) \).

For each \( \alpha \in GF(p^2) \), we have an element \( z \in GF(p^2) \) such that \( t^h_\alpha(z) = 0 = h^{-1}(\alpha) + z + L_\gamma(z) \), since \( h(x) \) is a permutation polynomial over \( GF(p^2) \) with \( h(0) = 0 \). Then \( t^h_\alpha(z) = 0 \) if and only if \( z = h^{-1}(-\alpha) \), and so

\[
(3) \quad h^{-1}(\alpha) + h^{-1}(-\alpha) = -L_\gamma(z) = -(\gamma z + \gamma^p z^p) = (z^p - z) \gamma
\]

for each \( \alpha \in GF(p^2) \) and the corresponding \( \gamma \in \text{Ker}(T^e) \).

Let \( \Gamma \) be a set of elements \( \gamma \in \text{Ker}(T^e) \) satisfying
(3) for each \( \alpha \in \text{GF}(p^2) \). Then we define a mapping

\[ \zeta: \text{GF}(p^2) \rightarrow \text{GF}(p^2) \times \Gamma \]

by

\[
(4) \quad \zeta(\alpha) = (\beta, \gamma)
\]

\[
= \begin{cases} 
(h^{-1}(\alpha),0) & \text{if } \alpha \in h(\text{GF}(p)) \\
(h^{-1}(\alpha),[h^{-1}(\alpha)+z]/[z^p-z]) & \text{otherwise}
\end{cases}
\]

where \( z = h^{-1}(-\alpha) \).

Clearly the mapping \( \zeta \) is well-defined, and injective since there is only one element \( \beta \in \text{GF}(p^2) \) for every \( \alpha \in \text{GF}(p^2) \). So we have a unique element \( \zeta(\alpha) = (h^{-1}(\alpha), \gamma) \in \text{GF}(p^2) \times \Gamma \) for each \( \alpha \in \text{GF}(p^2) \).

Thus \( h(x) \) satisfies (2) if and only if there exists a unique \( \zeta(\alpha) = (h^{-1}(\alpha), \gamma) \in \text{GF}(p^2) \times \Gamma \) such that, for all \( \alpha \in \text{GF}(p^2) \),

\[
(5) \quad h(h^{-1}(\alpha) + x + L_\gamma(z)) = h(x) + \alpha.
\]

Since \( L_\gamma(c) = 0 \) for \( c \in \text{GF}(p) \), Lemma 6 and (5) imply that \( h(x) \in H_{L_\gamma}(W) \) also satisfies, for \( c \in \text{GF}(p) \),

\[
(6) \quad h(x + c) = h(x) + h(c).
\]

Let \( h(x) \sum_{s=1}^{d} b_s x^s \in \text{GF}[p^2,z] \) with \( d < p^2 \). If \( d = 1 \), then \( h(x) \) represents a multiplier mapping on \( \text{GF}(p^2) \). So we assume that \( d \neq 1 \). By Theorem 8 in chapter III and (6), \( d = rp \) for some \( r \) with \( 0 < r < p \) and

\[
(7) \quad (m-k)b_{mp-kp+k} + (k+1)b_{mp-kp+k+1} = 0
\]

for \( 2 \leq m \leq r \) and \( 0 \leq k \leq m-1 \). Again, by (b) of Theorem 8 in chapter III,

\[
(8) \quad h(x) = \sum_{s=1}^{d} b_s x^s
\]
\[ h(L_\gamma(x)) = \sum_{i=1}^{r} \sum_{k=0}^{i} b_{ip-kp-k} \cdot x^{ip-kp-k}. \]

So,

\[ h(L_\gamma(x)) = \sum_{i=1}^{r} \sum_{k=0}^{i} b_{ip-kp-k} \cdot (\gamma z + \gamma^p z^p)^{ip-kp-k} \]

\[ = \sum_{i=1}^{r} \sum_{k=0}^{i} b_{ip-kp-k} \cdot (\gamma z + \gamma^p z^p)^{i} \]

\[ = \sum_{i=1}^{r} (\gamma z + \gamma^p z^p)^{i} \cdot \sum_{k=0}^{i} b_{ip-kp-k} \]

\[ = \sum_{i=1}^{r} \sum_{j=0}^{i} \binom{i}{j} (\gamma z)^{ip-j} \cdot \sum_{k=0}^{j} b_{ip-kp-k} \]

\[ = \sum_{i=1}^{r} \sum_{j=0}^{i} \binom{i}{j} A_i(\gamma z)^{ip-j}, \]

where \( A_i = b_{iP} + b_{iP-p+1} + b_{iP-2p+2} + \ldots + b_1 \).

From (7), if \( 2 \leq k < i \leq r \), then

\[ \sum_{k=0}^{i} \{ (i - k)b_{ip-kp-k} + (k + 1)b_{ip-kp-p+k+1} \} \]

\[ = \sum_{k=0}^{i} \{ b_{ip-kp-k} + b_{iP-kP-p+k+1} \} \]

\[ = i \cdot A_i = 0 \]

for every \( i = 2, 3, \ldots, r \). Since \( 1 < i < p \), \( A_i = 0 \) and

\[ h(L_\gamma(x)) = \sum_{i=0}^{1} \binom{1}{j} A_i(\gamma z)^{ip-j} \]

\[ = A_i(\gamma z + \gamma^p z^p) \]

\[ = (b_1 + b_p) \cdot L_\gamma(x). \]

By using (10) and Corollary 9 in chapter III, for all \( \alpha \in GF(p^2) \) with \( \beta = h^{-1}(\alpha) \),

\[ h(\beta + x) + h(L_\gamma(x)) = h(x) + \alpha \]

implies that every term in (11) will vanish except \( x^p \), \( x \), and constant terms. Also, by equating those three terms in (11), we can obtain the following three conditions for \( h(z) \in \mathbb{H}_T(W_*) \):

\[ \beta = h^{-1}(\alpha), \]

\[ h(\beta + x) \]

\[ h(L_\gamma(x)) = h(x) \]

\[ + \alpha \]
(i) \(2b_2\beta^p + b_{p+1}\beta + b_p + (b_1 + b_p)\gamma^p = b_p\).

(ii) \(b_{p+1}\beta^p + 2b_2\beta + b_1 + (b_1 + b_p)\gamma = b_1\).

(iii) \(b_p\beta^p + b_1\beta = \alpha\).

By (7) we can rewrite these as follows: For all \(\alpha \in GF(q)\) with \(\zeta(\alpha) = (\beta, \gamma) \in GF(p^2) \times \Gamma\),

(I) \(2b_2(\beta^p - \beta) = (b_1 + b_p)\gamma\),

(II) \(b_p\beta^p + b_1\beta = \alpha\)

Since \(\beta = h^{-1}(a)\) runs through all elements of \(GF(p^2)\), \(b_1 + b_p \neq 0\) from (II).

Hence, (I) and (II) implies that if \(h(x) \in H_T(W)\) with \(h(0) = 0\) then the polynomial is of the form

\[h(x) = a(x^p - x)^2 + bx^p + cx\]

for some \(a, b,\) and \(c \in GF(p^2)\). Furthermore, \(bx^p + cx \in B[p^2, x]\) and \(a(\beta^p - \beta) = (b + c)\gamma\) for \((\beta, \gamma) = \zeta(\alpha) = (h^{-1}(\alpha), \gamma) \in GF(p^2) \times \Gamma\).

On the other hand, suppose that a polynomial \(h(x) = a(x^p - x)^2 + bx^p + cx \in GF[p^2, x]\) satisfying the conditions (I) and (II). From (5), \(h(\beta + x + L_\gamma(x)) = h(x) + \alpha\) where \(\beta = h^{-1}(\alpha)\) and \(\zeta(\alpha) = (\beta, \gamma) \in GF(p^2) \times \Gamma\) for each \(\alpha \in GF(p^2)\).

Let \(k(x) = bx^p + cx\). Since \(2a(\beta^p - \beta) = k(1) \cdot \gamma\) and the absolute trace function Tr is a linear transformation of \(GF(p^2)\) over the prime subfield, for every \(\alpha\) in the
finite field,
\[ h(\beta + x + L_\gamma(z)) = a\{(x^p - x) + (\beta^p - \beta)\}^2 \]
\[ + b(x^p + \beta^p) + c(x + \beta) + k(1) \cdot L_\gamma(z) \]
\[ = h(x) + h(\beta) \]
\[ + \{2a(\beta^p - \beta) + k(1) \cdot \gamma\}(x^p - x) \]
\[ = h(x) + h(\beta) \]
\[ = h(x) + a \]

Thus the given polynomial \( h(x) \in H_T(W) \).

According to the above results, we proved that a polynomial \( h(x) \in H_T(W) \) with \( T < P < A \) and \( h(0) = 0 \) if and only if \( h(x) = a(x^p - x)^2 + k(x) \) for \( k(x) \in B[p^2, x] \) such that \( 2a(\beta^p - \beta) = k(1) \cdot \gamma \) for \((\beta, \gamma) = \zeta(\alpha) = GF(p^2) \times \Gamma\).

Thus, if \( \phi \) is a linear operator on \( GF(p^2) \) defined by \( \phi(x) = x^p - x \) for all \( x \in GF(p^2) \) and \( \ell(x) = a_i x^p + a_0 x \in B[p^2, x] \), then
\[ f(x) = g(\ell(x)) = h(\ell(x)) + g(0) \]
\[ = a\{(\lambda x)^p - \lambda x\}^2 \]
\[ + (b_a x^p + c_a x^p + (b_{a_1} + c_{a_1})x + g(0) \]
\[ = a[\phi(\lambda x)]^2 + \omega(x) \]
for \( \lambda = a_i - a_2 \) and \( \omega(x) = (b_{a_2} + c_{a_1})x^p + (b_{a_2} + c_{a_1})x + g(0) \in A \).

Therefore, two Cayley objects of \( GF(p^2) \) with \( T \subseteq P \subseteq A \) are isomorphic if and only if they are isomorphic by a
function in $H_T(W)$ and the function on $GF(p^2)$ can be represented by a permutation polynomial $f(x)$ over $GF(p^2)$ of the form $a[\phi(\lambda x)]^2 + \omega(x)$ where $\lambda$ is some element of $GF(p^2)$ and $\omega$ is an affine $p$–polynomial of $\mathbb{F}_p$.

6. Proof of Theorem 2. Let $q = p^n$ for an arbitrary positive integer $n$. Let $\mathcal{C}$ and $\mathcal{D}$ be any two Cayley objects over $GF(q)$. Suppose that $\mathcal{D}$ is a Cayley $W$–object of $GF(q)$.

From Lemma 5 and the definition of a Cayley $W$–objects, an isomorphism from $\mathcal{C}$ to $\mathcal{D}$ can be represented by a polynomial $f(x)$ over $GF(q)$ in $H_T(\mathcal{P})$ where $\mathcal{P}$ is the polynomial representation over $GF(q)$ of $P \in Sym(q)$ such that $P \subseteq \mathcal{P}$. Since $T^f < \mathcal{P} < W$, $T^f < W$ implies that $f(x) \in H_T(W)$ where $W$ is the group of permutation polynomials over $GF(q)$ of the form

$$w(x) = \beta + x + L_\gamma(x)$$

for $\beta \in GF(q)$ and $\gamma \in Ker(Tr)$. It is sufficient to characterize all polynomials $g(x) \in H_T(W)$ by setting $g(x) = f(x) - f(0)$.

Suppose that a polynomial $g(x) \in H_T(W)$. From the definition of $H_T(W)$, for each $\alpha \in GF(q)$, there is a unique $w(x) = \beta + x + L_\gamma(x) \in W$ such that

$$(12) \quad g(z) + \alpha = g(z) + g(\beta) = g(\beta + x + L_\gamma(x)).$$
Fix $\beta$ in (12) and consider a permutation polynomial $k(x) = x + L_\gamma(z)$. Then there exists an element $z \in \operatorname{GF}(q)$ such that $k(z) = z + L_\gamma(z) = -\beta$. Since $k^{-1}(x) = x - L_\gamma(x)$ and $p$ is an odd prime number, $z = k^{-1}(-\beta) = -\beta - L_\gamma(-\beta) = -\beta + L_\gamma(\beta)$. Since $g(\beta) + g(z) = g(\beta + z + L_\gamma(z)) = g(0) = 0$ by (12),
$$g(\beta) + g(-\beta) + g(L_\gamma(\beta)) = 0.$$ Thus

(13) \hspace{1cm} g(\beta) + g(-\beta) = -g(0).$$

By (13), $2 \cdot g_\epsilon(x) = g(x) + g(-x)$ implies that

(14) \hspace{1cm} 2 \cdot g_\epsilon(\beta) = -g(\beta).

Since $\beta$ runs through all elements of $\operatorname{GF}(q)$, $g(x)$ satisfies also $2 \cdot g_\epsilon(x) = -g_\epsilon L_\gamma(\beta)$ for some $\gamma_x \in \operatorname{Ker}(\operatorname{Tr})$ depending on each $x \in \operatorname{GF}(q)$. Thus, for every $\alpha \in \operatorname{GF}(q)$,

$2 \cdot g_\epsilon(\alpha) = -g_\epsilon L_\gamma(\alpha)$ and there is an element $c \in \operatorname{GF}(p)$ such that

(15) \hspace{1cm} 2 \cdot g_\epsilon(\alpha) = -g_\epsilon(c)$

because $L_\gamma : \operatorname{GF}(q) \to \operatorname{GF}(q)$ is a linear transformation of $\operatorname{GF}(q)$ over $\operatorname{GF}(p)$, both considered as vector spaces over $\operatorname{GF}(p)$. Therefore $g(x) \in \mathcal{F}$, and so $f(x) = t g(0) g(x) \in \mathcal{F}$. 

Remark. In (15), $g_\epsilon(c) = 0$ for every $c \in \text{GF}(p)$. 
BIBLIOGRAPHY


6. N. Brand, Quadratic Isomorphisms of \( \mathbb{F}_p \oplus \mathbb{F}_p \) objects Congressus Numerantium 58 (1987), 157–163.
7. N. Brand, Design Isomorphisms and Group Isomorphisms
9. J. V. Brawley, L. Carlitz, and T. Vaughan, Linear
   Polynomials with Coefficients in a Subfield, Acta
   Arith. XXIV (1973), 193–199.
    Amer. Math. Soc. 4 (1953), 538.
12. L. Carlitz, A Note on the Betti–Mathieu Group
13. N. G. de Bruijn, Polya’s Theory of Counting, Applied
    Combinatorial Mathematics, (Ed., E. F. Beckenbach)
14. L. E. Dickson, The Analytic Representation of
    Substitutions on a Power of a Prime Number of Letters
    with a Discussion of the Linear Group, Ann. of Math.
    11 (1897), 66–120.
15. L. E. Dickson, Linear Groups with an Exposition of the
    Galois Field Theory, Dover, New York, 1958.
16. B. Elspas and J. Turner, Graphs with Circulant
    297–307.
17. C. D. Godsil, On Cayley Graph Isomorphisms, Ars


25. É. Mathieu, *Memoire sur l'étude des fonctions de plusieurs quantités, sur la manièrè de les former et sur les substitutions qui les laissent invariables*, Journal de Mathématiques Pure et Appliquées, 2nd series, 6 (1861), 241–323.


28. Ö. Ore, Contributions to the Theory of Polynomials
Amer. Math. Soc. Trans. 36 (1934), 243–274.

29. M. Oshima, Some Remarks on the Characters of the


31. P. P. Palfy, Isomorphism Problem for Relational
Structures with a Cyclic Automorphism, European J.
Combin. 8 (1987), 35–43.

32. K. T. Phelps, Isomorphism Problem for Cyclic Block
Designs, preprint.

33. C. Wells, Polynomials over Finite Fields which
commute with Translations, Proc. Amer. Math. Soc. 46

RELATED BOOKS

34. D. Gorenstein, Finite Groups, New York: Harper and

35. B. Huppert, Endliche Gruppen, I, Springer–Verlag
Berlin 1967.