Group Actions on Minimal Functions Over Finite Fields.

Francisco Rivero

Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_disstheses

Recommended Citation
https://digitalcommons.lsu.edu/gradschool_disstheses/4473

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.
INFORMATION TO USERS

The most advanced technology has been used to photograph and reproduce this manuscript from the microfilm master. UMI films the original text directly from the copy submitted. Thus, some dissertation copies are in typewriter face, while others may be from a computer printer.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyrighted material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each oversize page is available as one exposure on a standard 35 mm slide or as a 17” × 23” black and white photographic print for an additional charge.

Photographs included in the original manuscript have been reproduced xerographically in this copy. 35 mm slides or 6” × 9” black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.
Group actions on minimal functions over finite fields

Rivero, Francisco, Ph.D.
The Louisiana State University and Agricultural and Mechanical Col., 1987
PLEASE NOTE:

In all cases this material has been filmed in the best possible way from the available copy. Problems encountered with this document have been identified here with a check mark __ __.

1. Glossy photographs or pages ______
2. Colored illustrations, paper or print ______
3. Photographs with dark background ______
4. Illustrations are poor copy ______
5. Pages with black marks, not original copy ______
6. Print shows through as there is text on both sides of page ______
7. Indistinct, broken or small print on several pages __ 
8. Print exceeds margin requirements ______
9. Tightly bound copy with print lost in spine ______
10. Computer printout pages with indistinct print ______
11. Page(s) _______ lacking when material received, and not available from school or author.
12. Page(s) ________ seem to be missing in numbering only as text follows.
13. Two pages numbered ______. Text follows.
14. Curling and wrinkled pages ______
15. Dissertation contains pages with print at a slant, filmed as received ______
16. Other ____________________________________________________

__________________________

__________________________

UMI
GROUP ACTIONS ON MINIMAL FUNCTIONS
OVER FINITE FIELDS

A dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor in Philosophy

in

The Department of Mathematics

by

Francisco Rivero
B.S., Universidad de Los Andes , 1976
M.S., Louisiana State University , 1984
December , 1987
ACKNOWLEDGEMENTS

I want to express my gratitude to Dr. Robert Perlis for his guidance and assistance throughout this dissertation. I also want to thank Dr. Jorge Morales and Dr. Ying Cheng for their assistance on group rings.

Finally, I express my gratitude to my wife Nancy and to my children Francisco and Paola.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>ii</td>
</tr>
<tr>
<td>Table of contents</td>
<td>iii</td>
</tr>
<tr>
<td>Abstract</td>
<td>iv</td>
</tr>
<tr>
<td>Introduction</td>
<td>v</td>
</tr>
<tr>
<td>Chapter 1. Minimal functions over finite fields</td>
<td></td>
</tr>
<tr>
<td>Fourier analysis</td>
<td>1</td>
</tr>
<tr>
<td>McGehee's Problem</td>
<td>5</td>
</tr>
<tr>
<td>Chapter 2. The group ring</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>17</td>
</tr>
<tr>
<td>The group ring FG</td>
<td>17</td>
</tr>
<tr>
<td>The isomorphism theorem for the rational group ring Q G</td>
<td>20</td>
</tr>
<tr>
<td>Group action on Q G</td>
<td>32</td>
</tr>
<tr>
<td>Some conditions for minimality</td>
<td>35</td>
</tr>
<tr>
<td>CHAPTER 3. Groups acting on the set of minimal functions</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>45</td>
</tr>
<tr>
<td>Group action on ( M )</td>
<td>47</td>
</tr>
<tr>
<td>Even degree extensions</td>
<td>51</td>
</tr>
<tr>
<td>APPENDIX</td>
<td>69</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>72</td>
</tr>
<tr>
<td>VITA</td>
<td>73</td>
</tr>
</tbody>
</table>
This work deals with the Fourier transform over finite fields. A notion of minimal function for the Fourier transform is defined. The minimal functions are shown to be a generalization of the famous Legendre symbol \( \mathbb{P} \). The minimal functions are studied here in terms of group actions, allowing both upper and lower estimates on the size of the set of all minimal functions. These estimates are sufficient to settle a conjecture of O.C. McGehee on the number of minimal functions.
INTRODUCTION

This work was motivated by a paper of O. C. McGehee dealing with the Fourier transform over finite fields. The problems and techniques in that paper are from analysis. In this dissertation, McGehee's problem is considered from the point of view of algebra.

Let $p$ be a prime, $p \neq 2$, $n$ a natural number, and let $(\mathbb{F}_{pn}, +)$ denote the additive group of the finite field $\mathbb{F}_{pn}$.

McGehee considers functions

$$\mu : (\mathbb{F}_{pn}, +) \longrightarrow (0, 1, -1)$$

with $\mu(x) = 0$ if and only if $x = 0$.

The Fourier transform $\hat{\mu}$ of $\mu$ is a function on additive characters $\chi : \mathbb{F}_{pn} \longrightarrow \mathbb{C}$. The norm of $\mu$ is defined to be the sup norm of $\hat{\mu}$, and it satisfies $\| \mu \| \leq p^{n/2}$.

A function $\mu$ is said to be minimal if $\| \mu \| = p^{n/2}$. The basic example of a minimal function is the \textit{quadratic function} $\chi$.
defined by: \( \psi(x) = 1 \) for \( x \) a nonzero square, \( \psi(x) = -1 \) for \( x \) nonsquare, and \( \psi(0) = 0 \).

McGehee's question is to describe the minimal functions, or at least to count them. When \( n = 1 \) or \( 2 \), McGehee gave a complete count of the minimal functions.

Chapter 1 contains basic material. Following McGehee, Plancherel's formula is used to prove \( \| \mu \| \leq p^{n/2} \) for any of the functions under consideration.

In Chapter 2 we consider the problem from the point of view of group rings. Any function on a group \( G \) with values on a ring \( K \) can be regarded as an element in the group ring \( KG \). Since 0, 1, -1 are rationals integers, the minimal functions "live" in the group ring \( ZG \) over the group \( G = (\mathbb{F}_p n \ , +) \).

It seems reasonable to think that the study of \( ZG \) should shed some light on the minimal functions on \( G \). For example the product in the group ring corresponds precisely to the convolution of functions on \( G \), explaining the standard but some-
what mysterious appearance of convolutions in the study of Fourier transforms. Moreover McGehee has shown that

$$\sum_{g \in G} \mu(g) = 0$$
whenever \( \mu \) is a minimal function, and this means that the minimal functions on \( G \) lie in the augmentation ideal \( IG \) of \( ZG \), i.e. each minimal \( \mu = \sum_{g \in G} \mu(g) g \) lies in the kernel of the map \( \varepsilon : ZG \rightarrow Z \), \( \varepsilon(\mu) = \sum_{g \in G} \mu(g) \).

Now, \( ZG \) is contained in \( \mathbb{Q}()G \) where \( \mathbb{Q}() \) is the \( p \)-th cyclotomic field, generated over \( \mathbb{Q} \) by a \( p \)-th root of unity \( \zeta \).

Algebraically, \( \mathbb{Q}()G \) decomposes as a direct sum of its simple factors. Standard techniques from algebra give a decomposition of \( \mathbb{Q}()G \) and, via the Perlis - Walker theorem, even a decomposition of the rational group ring \( \mathbb{Q}G \). This is explained in Chapter 2.

The integral group ring \( ZG \) is an order but unfortunately not a maximal order in \( \mathbb{Q}G \).
So chapter 2 is to suggest that one could perhaps account algebraically for the minimal functions if we could descend from \( G \) to \( ZG \) and then from \( ZG \) to the subset of functions with coefficients 0, 1, and -1. That remains to be done. The best we can say is that the group-ring point of view allows a new proof that, when \( n \) is even, minimal functions have the property that \( \mu(x)/\Psi(x) = \mu(cx)/\Psi(cx) \) for all \( c \) in \( F_p^* \) where \( \Psi \) is the quadratic function.

From this it follows that there is a function \( \rho \) in \( F_p^n \), with \( \mu(x) = \rho(x) \Psi(x) \) and \( \rho \) constant on lines through the origin i.e. \( \rho(cx) = \rho(x) \) for all \( c \) in \( F_p^* \). This is the basic relation connecting minimal functions \( \mu \) to the quadratic function \( \Psi \). It means that we can find all \( \mu \) by identifying the necessary restrictions on \( \rho \).

Chapter 3 contains some methods to produce minimal functions. The basic idea here consists of studying group actions
on the set of minimal functions.

By showing that $\text{GL}_n(F_p)$ acts on the set of minimal functions, we conclude that there are enough minimal functions to verify a conjecture of McGehee, which says that for $n > 1$ the number of minimal functions is greater than two. We show that for any $n \geq 1$ the number of minimal functions is at least $2^n$.

When $n = 2$ and $p \neq 3, 5$ we show that $\text{GL}_2(F_p)$ does not act transitively on the set of minimal functions (see section 3, of Chapter 3).

However when $n = 2$ we found a group even larger than $\text{GL}_2(F_p)$. If $G = (F_p^n, +)$, then $G$ is a vector space over $F_p$ and can be considered as a union of lines through the origin. Then the group $P_2$ of all permutations $\sigma$ of $G$, taking $0$ to $0$ and lines to lines, acts transitively on the minimal functions. Thus we obtain all minimal functions from the $P_2$-orbit of the quadratic function $\varphi$.

In general when $n = 2m$ is even, then the finite field $F_p$
\( \mathbb{F}_{p^{2m}} \) contains the subfield \( K = \mathbb{F}_{p^n} \), and \( G = ( \mathbb{F}_{p^{2m}}, + ) \) can be considered to be a \( K \)-vector space, and thus \( \mathbb{F}_{p^{2m}} \) is a union of \( K \)-lines through the origin. As before, we consider the group \( P_2(K) \) of permutations of \( \mathbb{F}_{p^{2m}} \) taking 0 to 0 and \( K \)-lines to \( K \)-lines. It is not known whether \( P_2(K) \) acts transitively on minimals when \( n > 2 \). But we can say that the action of \( P_2(K) \) gives that the number \( N_0 \) of minimal functions satisfies

\[
N_0 \geq \left[ \frac{t}{t/2} \right],
\]

where the binomial coefficient is computed with \( t = p^m + 1 \).

For example, when \( p = 7 \) and \( n = 6 \) we see

\[
N_0 \geq \left[ \frac{344}{172} \right],
\]

which is a number with over 100 digits.

Finally using numerical computations, we make a conjec-
ture for the size of the $GL_n$-orbit of the quadratic function.

This new conjecture has been numerically verified in all the easily-computable cases. Its statement is simple enough to give here:

conjecture: If $\sigma$ is an invertible $\mathbb{F}_p$-linear map on the finite field $L = \mathbb{F}_p^n$ and if $\sigma$ satisfies

1. $\sigma(1) = 1$

2. $\sigma(L^2) = L^2$,

then $\sigma(xy) = \sigma(x) \sigma(y)$ for all $x, y$ in $L = \mathbb{F}_p^n$.

This conjecture seems to be of independent interest.
CHAPTER 1
MINIMAL FUNCTIONS OVER FINITE FIELDS

1. FOURIER ANALYSIS

We start by considering a finite field $\mathbb{F}_q$, with $q = p^n$
where $p$ is a prime number $p \neq 2$, and $n$ a positive integer. Denote by
$G$ the additive group of $\mathbb{F}_q$, and let $\mathbb{C}^*$ be the multiplicative
group of the complex numbers.

A character on $G$, as a homomorphism $\varphi : G \rightarrow \mathbb{C}^*$ from
the additive group $G$ to the multiplicative group $\mathbb{C}^*$

Thus $\varphi(0) = 1$, and for all $a$ in $G$, the image $\varphi(a)$ is

a $p$-th root of unity. In particular $\varphi(s) = \varphi(-s)$.

The trivial character $\chi_0$ is the map given by $\chi_0(a) = 1$
for all $a$ in $G$.

The set of all characters becomes a group under the
multiplication of functions.
The group of all characters, denoted by \( \hat{G} \), is called the dual group of \( G \).

The trace homomorphism on \( F_q \) is defined as the additive map

\[
\text{tr} : F_q \rightarrow F_p
\]

\[
\text{tr}(x) = \sum_{i=1}^{n} \sigma_i(x);
\]

where \( \sigma_i \) runs over the Galois group of \( F_q \mid F_p \).

The trace induces a non-singular bilinear form:

\[
\langle \cdot , \cdot \rangle : F_q \times F_q \rightarrow F_p.
\]

\[
\langle x, y \rangle = \text{tr}(xy).
\]

Now, using this bilinear form, it is possible to identify \( G \) with its dual. Let \( g \) be an element in \( G \), let \( \xi \) be a primitive \( p \)-th root of unity, and put \( \psi_g(x) = \xi^{\langle x, g \rangle} \).

It is easy to show that \( \psi_g \) is a character on \( G \), and the map \( g \rightarrow \psi_g \) from \( G \) to \( \hat{G} \) is in fact a group isomorphism.

From this one obtain the following result:
(1.1) Theorem: Let \( \psi : G \to \mathbb{C}^* \) be any character then there exists a unique \( g \) on \( G \) such that, for all \( a \) in \( G \)
\[
\psi(a) = \zeta \langle a, g \rangle, \quad \zeta \text{ a } p\text{-th root of unity}.
\]
\[\square\]

(1.2) Definition: Let \( f : G \to \mathbb{C} \) be a function, and let \( \psi \) be a character on \( G \). The Fourier transform of \( f \) is the function \( \hat{f} : \hat{G} \to \mathbb{C} \) given by
\[
\hat{f}(\psi) = \sum_{g \in G} f(g) \psi(g).
\]
for \( \psi \) in \( \hat{G} \).

(1.3) Theorem (Plancherel): Let \( f : G \to \mathbb{C} \) be any function, and \( \hat{G} \) the dual group of \( G \). Then we have:
\[
\sum_{\psi \in \hat{G}} |\hat{f}(\psi)|^2 = |G| \sum_{g \in G} |f(g)|^2.
\]
Proof: Consider a character \( \psi \) on \( G \). Then
\[
|\hat{f}(\psi)|^2 = \hat{f}(\psi) \cdot \hat{f}(\psi).
\]
\[
= \left[ \sum_{g \in G} f(g) \psi(g) \right] \cdot \left[ \sum_{s \in G} \overline{f(s)} \psi(s) \right].
\]
\[ \sum_{g,s \in G} f(g) \overline{f(s)} \varphi(g-s) \], since

\[ \varphi(g) \overline{\varphi(s)} = \varphi(g-s) \]. After rearranging the summands we get

\[ |\hat{f}(\varphi)|^2 = \sum_{g \in G} f(g) \overline{f(g)} + \sum_{g \neq s \in G} f(g) \overline{f(s)} \varphi(g-s). \]

\[ = \sum_{g \in G} |f(g)|^2 + \sum_{g \neq s \in G} f(g) \overline{f(s)} \varphi(g-s). \]

Summing over all \( \varphi \) in \( \hat{G} \) on both sides, we get:

\[ \sum_{\varphi \in \hat{G}} |\hat{f}(\varphi)|^2 = |\hat{G}| \sum_{g \in G} |f(g)|^2 + \sum_{g \neq s \in G} f(g) \overline{f(s)} \sum_{\varphi \in \hat{G}} \varphi(g-s). \]

For \( s \) and \( g \) fixed and distinct, the last sum is zero.

Therefore we obtain

\[ \sum_{\varphi \in \hat{G}} |\hat{f}(\varphi)|^2 = |\hat{G}| \sum_{g \in G} |f(g)|^2 \]

Which is the statement of the theorem. \( \Box \)

(1.4) Definition: Let \( f : G \rightarrow \mathbb{C} \) be any function.

The norm of \( f \) is defined as

\[ \| f \| = \text{Sup}_{\varphi \in \hat{G}} |\hat{f}(\varphi)|. \]
Remark If \( f \) is a function on \( G \) put \( M = \operatorname{Sup}_{g \in G} |f(g)| \),
then we obtain:

\[
|\sum_{g \in G} f(g) \varphi(g)| \leq M \sum_{g \in G} |\varphi(g)|
\]

Using \( |\varphi(g)| \leq 1 \), for all \( g \in G \), gives

\[ |f| \leq |M| |G| .\]

2. McGehee's Problem

Consider the functions \( G \rightarrow \mathbb{C} \) given by

\[
f: G \rightarrow \{0, 1, -1\},
\]
and such that \( f(g) = 0 \) if and only if \( g = 0 \)

The set of these functions will be denoted by \( M \).

1.5 Definition: A function \( f \) in \( M \) is called a minimal function on \( G \) if \( |f| \leq |h| \), for all \( h \) in \( M \).

McGehee's problem is: Given \( G \), find the number of minimal functions.

Next, we introduce some definitions and basic results from Fourier analysis in order to find conditions on minimal
(1.6) Definition: Let $f$ and $h$ be two complex-valued functions on $G$. The convolution of $f$ and $h$ is the function $f \ast h$ given by:

$$f \ast h(x) = \sum_{g \in G} f(x-g)h(g), \text{ for all } x \in G$$

(1.7) Definition: Let $f : G \rightarrow \mathbb{C}$. Then $\hat{f}$ is the function $\hat{f} : G \rightarrow \mathbb{C}$ given by $\hat{f}(x) = \overline{f(-x)}$.

The following well known relations between Fourier transforms and convolutions can be found in the book of Graham and McGehee [G-M].

(1.8) Lemma: Let $f$, $h$ be functions on $G$ with values on $\mathbb{C}$. Then we have:

1) $\hat{\hat{f}} = \overline{f}$

2) $(f \ast h) = \hat{f} \cdot \hat{h}$. 
proof: i) Let $\varphi$ be in $\hat{G}$. Then

$$\hat{\hat{\varphi}}(\varphi) = \sum_{g \in G} \hat{\varphi}(g) \varphi(g)$$

$$= \sum_{g \in G} \frac{\varphi(-g)}{f(-g)} \varphi(g).$$

$$= \sum_{g \in G} \frac{\varphi(g)}{f(-g)} \varphi(-g).$$

$$= \left[ \sum_{g \in G} f(g) \varphi(g) \right] \varphi(g).$$

$$= \hat{\varphi}(\varphi).$$

Thus we have shown $\hat{\hat{\varphi}} = \hat{\varphi}$.

ii) Let $\varphi$ be in $\hat{G}$. Then

$$\hat{\varphi}(\varphi) = \sum_{g \in G} \varphi(g)$$

$$= \sum_{g \in G} \left[ \sum_{x \in G} \left[ \sum_{g-x \in G} f(g-x) h(x) \right] \varphi(g) \right] \varphi(g).$$

Make $g - x = t$ in the last sum, to obtain
\[
(f * h)(\varphi) = \sum_{x \in G} \sum_{t \in G} f(t) h(x) \varphi(x + t)
\]

\[
= \sum_{x \in G} \sum_{t \in G} f(t) h(x) \varphi(x) \varphi(t)
\]

\[
= \left( \sum_{t \in G} f(t) \varphi(t) \right) \left( \sum_{x \in G} h(x) \varphi(x) \right)
\]

\[
= \hat{\varphi} \left( \varphi \right) \hat{h} \left( \varphi \right).
\]

Therefore \( f * h = \hat{\varphi} \hat{h} \) as we claimed.

**iii)** In particular, putting \( h = \overline{\varphi} \) in ii) gives

\[
(f * \overline{\varphi})(\varphi) = \hat{\varphi}(\varphi) \overline{\hat{\varphi}(\varphi)}(\varphi).
\]

\[
= \hat{\varphi}(\varphi) \overline{\hat{\varphi}(\varphi)}(\varphi). \quad \text{(by i).}
\]

\[
= |\hat{\varphi}(\varphi)|^2.
\]

That finishes the proof. □

**(1.9) Lemma:** Let \( f : G \rightarrow \mathbb{C} \), and define:

\[
c(t) = f * \overline{\varphi(t)}, \text{ for } t \in G.
\]

Then we have

\[
\sum_{t \in G} c(t) = |\sum_{s \in G} f(s)|^2
\]
proof: Consider

$$\sum_{t \in G} c(t) = \sum_{t \in G} f \ast f(t)$$

$$= \sum_{t \in G} \sum_{s \in G} f(t-s) \overline{f(s)}$$

$$= \sum_{t \in G} \sum_{s \in G} f(t-s) f(-s)$$

Writing $g = t-s$, we get

$$\sum_{t \in G} c(t) = \sum_{g \in G} \sum_{s \in G} f(g) \overline{f(-s)}.$$  

$$= \left[ \sum_{g \in G} f(g) \right] \left[ \sum_{s \in G} f(s) \right]$$

$$= \left| \sum_{s \in G} f(s) \right|^2. \quad \square$$

McGehee found the following criterion for minimality (see [M]).

(1.10) Lemma: For $f \in M$, we have:

i) $\| f \| \geq \sqrt{q}$, where $q = |G|$.

ii) $\| f \| = \sqrt{q}$, if and only if $\hat{f}(\chi_0) = 0$, and
Proof: i) As in lemma (1.9) define \( c(t) = (f * \hat{f})(t) \), for 
\( t \in G \). Then \( c(t) \) is an integer and \( c(t) \) is odd for \( t \neq 0 \), 
since \( c(t) \) is a sum of \( q-2 \) terms ( \( q \) odd), all of which are 1 
or -1. So for \( t \neq 0 \) we have \( |c(t)|^2 \leq 1 \) and 

\[
\sum_{t \neq 0} |c(t)|^2 \leq q - 1.
\]

Now \( c(0) \) is given by

\[
c(0) = (f * \hat{f})(0) = \sum_{s \in G} f(-s) f(-s),
\]

\[
= \sum_{s \in G} |f(s)|^2 = q - 1.
\]

Therefore \( c(0)^2 = (q-1)^2 \) and thus

\[
(q-1)^2 + (q-1) \sum_{t \in G} |c(t)|^2 \quad (1).
\]

\[
= \sum_{t \in G} |f * \hat{f}(t)|^2 \quad (2).
\]

\[
= \frac{1}{q} \sum_{\varphi \in \hat{G}} |(f * \hat{f})(\varphi)|^2 \quad \text{(by Plancherel)}
\]
Thus we have shown: \((q-1)q \leq \|f\|^2 (q-1)\), and from this we get \(\|f\| \leq \sqrt{q}\).

ii) Assume that \(\|f\| = \sqrt{q}\). This forces all inequalities (1) - (4) to be equalities.

From (3) we get
\[
\sum_{\varphi \in \hat{G}} |\hat{f}(\varphi)|^4 = \|f\|^2 \sum_{\varphi \in \hat{G}} |f(\varphi)|^2. \tag{5}
\]

claim: For all \(\varphi \in \hat{G}\) we have either \(|\hat{f}(\varphi)| = \|f\|\) or \(|\hat{f}(\varphi)| = 0\).

Assume \(0 < |\hat{f}(\varphi)| < \|f\|\) for some \(\varphi\) in \(\hat{G}\). Then
we have

\[ | \hat{f}(\psi) |^4 < \| f \| \| \hat{f}(\psi) \|^2 \]  \hspace{1cm} (6)

On the other hand, for the remaining characters \( \chi \) in \( \hat{G} \) different from \( \psi \), we obtain

\[ | \hat{f}(\chi) |^4 \| f \| \| \hat{f}(\chi) \|^2 \]  \hspace{1cm} (7)

Adding up (6) and (7) gives

\[ \sum_{\chi \in \hat{G}} | \hat{f}(\chi) |^4 < \| f \| \sum_{\chi \in \hat{G}} | \hat{f}(\chi) |^2 . \]

The last inequality contradicts (5). So the claim is certainly true.

Next we want to prove that \( \hat{f}(\chi_0) = 0 \).

From equation (1) one gets

\[ \sum_{t \neq 0} | c(t) |^2 = q-1 , \]

which implies \( | c(t) | = 1 \) for all \( t \neq 0 \).

On the other hand

\[ \sum_{t \in G} c(t) = \left[ \sum_{t \in G} f(t) \right]^2 \hspace{1cm} (\text{by lemma 1.9}) \]
Therefore

\[ \sum_{t \neq 0} c(t) \leq q - c(0) = q - (q-1) = 1. \]

The above sum cannot be 1 since the number of summands is even and each value \( c(t) \) is odd. Thus we get

\[ |\hat{f}(\chi_0)|^2 = q - 1 + \sum_{t \neq 0} c(t) < q \quad \text{(8)} \]

From (8) and the claim we deduce that \( \hat{f}(\chi_0) = 0 \).

Finally, from the Plancherel relation it follows

\[ \sum_{\varphi \in \mathcal{G}} |\hat{f}(\varphi)|^2 = q (q-1) = \|f\|_2^2 (q-1) \]

Since we have already proved that \( \hat{f}(\chi_0) = 0 \), the last sum is taken over \( q-1 \) terms, all of which are less than or equal to \( \|f\|_2^2 \) and which sum to \( \|f\|_2^2 (q-1) \). Therefore we must conclude \( |\hat{f}(\varphi)|^2 = \|f\|_2^2 \), for all \( \varphi \neq \chi_0 \).

That proves \( |\hat{f}(\varphi)| = \sqrt{q} \), for all \( \varphi \neq \chi_0 \).
Conversely, if we assume:

\[ \hat{f}(\chi_0) = 0 \text{ and } |\hat{f}(\psi)| = \sqrt{q} \text{, for all } \psi \neq \chi_0, \]

then we clearly have \(|f| = \sqrt{q} \). \(\square\)

The next step will be to show that minimal functions exist.

(1.11) **Definition**: Let \( F_q \) be a finite field of \( q \) elements, then the quadratic function on \( F_q \), is defined as:

\[ \Phi(x) = \begin{cases} 
1 & \text{if } x \text{ is a non-zero square in } F_q, \\
-1 & \text{if } x \text{ is not a square in } F_q, \\
0 & \text{if } x = 0. 
\end{cases} \]

(1.12) **Lemma**: The quadratic function \( \Phi \) has the properties:

i) \( \Phi(a,b) = \Phi(a) \cdot \Phi(b) \), for all \( a,b \) in \( F_q \).

ii) \( \sum_{s \in F_q} \Phi(s) = 0. \)

Proof: i) Follows directly from the fact that \( F_q^* / F_q^{**} \) has order two.

ii) Use the fact that the number of non-zero squares in \( F_q \) is equal to the number of non squares. Hence the number
of 1's in the sum is the same as the number of -1's. □

(1.13) Theorem: The quadratic function \( \Psi : G \rightarrow \{0,1,-1\} \)

has norm \( \| \Psi \| = \sqrt{q} \), and is minimal.

**proof:** If we show \( \| \Psi \| = \sqrt{q} \), then \( \Psi \) is minimal by lemma 1.10, part i). By part ii) of the same lemma, the theorem will be proved if we can show

i) \( \hat{\Psi}(\chi_0) = 0 \), and

ii) \( |\hat{\Psi}(\Psi)| = \sqrt{q} \), for all \( \Psi \) in \( \hat{G} \), \( \Psi \neq \chi_0 \).

To show i), use the second part of lemma (1.12) to get

\[
\hat{\Psi}(\chi_0) = \sum_{s \in G} \Psi(s) = 0.
\]

In order to prove ii) take \( \Psi \) a non-trivial character in \( \hat{G} \). Then we have

\[
|\hat{\Psi}(\Psi)|^2 = \left[ \sum_{g \in G} \Psi(g) \Psi(g) \right] \left[ \sum_{s \in G} \Psi(s) \Psi(s) \right] = \sum_{g, s \in G} \Psi(g) \Psi(s) \Psi(g-s).
\]
In the last sum, the terms with $g = 0$ do not give any contribution. Thus, neglecting those terms, and setting $c = s/g$ we obtain:

$$\phi^2 = (q - 1) + \sum_{c \neq 1} \phi(c) \sum_{g \neq 0} \phi(g(1 - c)).$$

Observe that when $g$ runs over $G - \{0\}$, then $g(1 - c)$ also runs over $G - \{0\}$. Therefore, we can write

$$\sum_{g \neq 0} \phi(g(1 - c)) = \sum_{t \neq 0} \phi(t) = -\phi(0) = -1.$$

Thus we obtain

$$\phi^2 = (q - 1) - \sum_{c \neq 1} \phi(c)$$

$$= (q - 1) - (-1) \quad \text{(From lemma 1.12 ii)}$$

$$= q.$$

Therefore, we have shown $|\phi(\varphi)| = \sqrt{q}$, and that ends the proof. □
CHAPTER 2

THE GROUP RING

1. Introduction.

The aim of this chapter is to interpret the original problem in the context of group rings, where the relations between functions and their Fourier transforms become clear.

We start this chapter by recalling basic definitions and facts about the group ring.

2. THE GROUP RING $F_G$.

Let $G$ be a finite abelian group in which the operation is written multiplicatively. Let $F$ be any field.

(2.1) Definition: The group ring of $G$ over $F$ is the ring $F_G$ whose elements are formal sums:

$$
\sum_{g \in G} a_g \cdot g,
$$

where $a_g$ is in $F$.

The two rings operations are defined as follows:

addition is componentwise and multiplication is
\[
\sum_{g \in G} a_g \cdot g \sum_{s \in G} b_s \cdot s = \sum_{g,s \in G} a_g b_s \ g \cdot s.
\]

\[
= \sum_{t \in G} c_t \cdot t, \text{ where } c_t = \sum_{g,s = t} a_g b_s.
\]

Remark: We can think of the elements in the group ring as \( F \)-valued functions on \( G \), namely
\[
f = \sum_{g \in G} f(g) \cdot g
\]

For \( f_1 \) and \( f_2 \) in \( FG \), their product in the group ring (not as functions) can be expressed in terms of convolutions (see definition 1.6)
\[
f_1 \cdot f_2 = \sum_{g,h \in G} f_1(g) f_2(h) \ g h
\]

\[
= \sum_{t \in G} \left( \sum_{g \in G} f_1(g) f_2(t-g) \right) t
\]

\[
= \sum_{t \in G} f_1 \ast f_2 (t) \ t
\]

Remark: \( FG \) is a vector space over \( F \) of dimension \( |G| \) over \( F \).

One choice of the basis for \( FG \) over \( F \) is \( \{ g \ | \ g \in G \} \).
(2.2) Lemma: For characters $\chi$ and $\chi'$ in $\hat{G}$ we have:

a) $\sum_{g \in G} \chi'(g^{-1}) \chi(g) = \delta_{\chi, \chi'} |G|$. 

For $\chi \neq \chi_0$ and for $h, g$ in $G$:

b) $\sum_{\chi \in \hat{G}} \chi(h) \chi(g^{-1}) = \delta_{h, g} |G|$. 

These equations are the orthogonality relations for characters.

proof: a) Assume first that $\chi = \chi'$. Then the sum becomes

$$\sum_{g \in G} \chi'(g^{-1}) \chi(g) = \sum_{g \in G} \chi(1) = |G|.$$ 

Assume now $\chi \neq \chi'$. Since $\hat{G}$ is a group, there exists $\varphi \neq \chi_0$ in $\hat{G}$ such that $\chi' = \varphi \chi$. Hence

$$\sum_{g \in G} \chi'(g^{-1}) \chi(g) = \sum_{g \in G} \varphi(g^{-1}) \chi(g^{-1}) \chi(g) = \sum_{g \in G} \varphi(g^{-1}) = 0.$$ 

b) Let $h$ and $g$ be in $G$. We consider two cases.

If $g = h$, we have
\[
\sum_{\chi \in \hat{G}} \chi(h) \chi(g^{-1}) = \sum_{\chi \in \hat{G}} \chi(1) = \sum_{\chi \in \hat{G}} 1 = |G|.
\]

If \( g \neq h \), put \( h.g^{-1} = k \). Then \( k \neq 1 \) and

\[
\sum_{\chi \in \hat{G}} \chi(h) \chi(g^{-1}) = \sum_{\chi \in \hat{G}} \chi(k) = 0. \quad \Box.
\]

3. **The Isomorphism Theorem for the Rational Group Ring \( \otimes G \)**

Let \( G \) be a finite abelian group with \( |G| = p^n = q \).

Let \( F \) be any field of characteristic zero which contains a primitive \( p \)-th root of unity.

As above, \( FG \) denotes the group ring of \( F \) over \( G \), and \( \otimes F \) will be the direct sum \( F \otimes \ldots \otimes F \) of \( q \) copies of \( F \).

We write the elements of \( \otimes F \), as formal sums

\[
\sum_{\chi \in \hat{G}} A_\chi \chi
\]

where \( A_\chi \) is in \( F \), for all \( \chi \) in \( \hat{G} \). Addition and multiplication in \( \otimes F \) are componentwise.

Consider the \( F \)-linear map
\[
\psi : F G \longrightarrow \Phi F
\]
\[
g \longrightarrow \sum_{\chi \in \hat{G}} \chi(g) \chi
\]

Remark: If \( f = \sum_{g \in G} f(g) g \) in \( F G \), we will see
\[
\psi(f) = \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi
\]

\((2.3)\) Theorem: Let \( \psi \) be the map given in (1). Then

\( a) \) For
\[
v = \sum_{g \in G} a_g g \text{ in } F G, \text{ then }
\]
\[
\psi(v) = \sum_{\chi \in \hat{G}} A_{\chi} \chi, \text{ where }
\]
\[
A_{\chi} = \sum_{g \in G} a_g \chi(g), \text{ for all } \chi \text{ in } \hat{G}.
\]

\( b) \) Define \( 0 : \Phi F \longrightarrow F G \) by
\[
\sum_{\chi \in \hat{G}} r_{\chi} \chi \longrightarrow \sum_{g \in G} a_g g,
\]
where:
\[
a_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} r_{\chi} \chi(g^{-1}).
\]
Then $\emptyset = \psi^{-1}$

c) $\psi$ is a ring isomorphism.

**proof:** a) This is the definition of "linear extension".

b) Here we need to show:

i) $\emptyset \psi(v) = v$ for all $v$ in $FG$.

ii) $\psi \emptyset(v) = V$, for all $V$ in $\Phi F$.

In order to prove i) let $v = \sum_{g \in G} a_g g$ in $FG$. Thus

$$
\psi(v) = \sum_{\chi \in \hat{G}} A_{\chi} \chi = \sum_{\chi \in \hat{G}} \left[ \sum_{g \in G} a_g \chi(g) \right] \chi
$$

Therefore the coefficient of $g$ in $\emptyset \psi(v)$ is

$$
(\emptyset \psi(v))_g = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \left[ \sum_{h \in G} a_h \chi(h) \right] \chi(g^{-1})
$$

$$
= \frac{1}{|G|} \sum_{h \in G} a_h \sum_{\chi \in \hat{G}} \chi(h) \chi^{-1}(g)
$$

$$
= \frac{1}{|G|} \sum_{h \in G} a_h \cdot h, g |G| \text{ (by 2.2 b )}
$$

$$
= \frac{1}{|G|} \left[ |G| a_g \right] = a_g
$$
Hence we conclude $\psi(v) = v$, proving part i).

We proceed to show ii)

Let $V = \sum_{\chi \in \hat{G}} r_{\chi} \chi$ in $\Phi F$. Then

$$\psi(V) = \sum_{g \in G} \left[ \frac{1}{|G|} \sum_{\chi \in \hat{G}} r_{\chi} \chi(g^{-1}) \right] g$$

Therefore the $\chi$-th component of $\psi(V)$ is

$$(\psi(V))_\chi = \frac{1}{|G|} \sum_{g \in G} \left[ \sum_{\varphi \in \hat{G}} r_{\varphi} \varphi(g^{-1}) \right] \chi(g)$$

$$= \frac{1}{|G|} \sum_{\varphi \in \hat{G}} r_{\varphi} \left[ \sum_{g \in G} \varphi(g^{-1}) \chi(g) \right]$$

$$= \frac{1}{|G|} \sum_{\varphi \in \hat{G}} r_{\varphi} |G| \varphi, \chi \quad \text{(by (2.2 a)).}$$

$$= r_{\chi}.$$

That ends the proof of ii).

It remains to show that $\psi$ preserves sums and products.

Consider any two elements $v$ and $w$ in $G$. Write

$$v = \sum_{g \in G} a_g g, \quad \text{and} \quad w = \sum_{g \in G} b_g g \quad (2)$$
where \( a_g, b_g \) are elements in \( F \). Thus we have

\[
\psi(v + w) = \psi \left( \sum_{g \in G} (a_g + b_g) g \right)
\]

\[
= \sum_{\chi \in \hat{G}} \left( \sum_{g \in G} (a_g + b_g) g \right) \chi
\]

\[
= \sum_{\chi \in \hat{G}} \left[ \sum_{g \in G} a_g g \right] \chi + \sum_{\chi \in \hat{G}} \left[ \sum_{g \in G} b_g g \right] \chi
\]

\[
= \psi(v) + \psi(w).
\]

We want to prove the multiplicative property of \( \psi \) first on elements of \( G \). For \( g \) and \( h \) in \( G \) we get

\[
\psi(g \cdot h) = \sum_{\chi \in \hat{G}} \chi(g \cdot h) \chi
\]

\[
= \sum_{\chi \in \hat{G}} \chi(g) \cdot \chi(h) \chi
\]

\[
= \left( \sum_{\chi \in \hat{G}} \chi(g) \chi \right) \left( \sum_{\chi \in \hat{G}} \chi(h) \chi \right)
\]

\[
= \psi(g) \psi(h).
\]

Let \( v \) and \( w \) be any two elements in \( FG \), as in (2). Then

\[
\psi(v \cdot w) = \psi \left( \left[ \sum_{g \in G} a_g g \right] \left[ \sum_{h \in G} b_g h \right] \right)
\]
\[
\psi \left( \sum_{g, h \in G} a_g b_h g h \right)
\]

\[
= \psi \left( \sum_{g \in G} a_g \left( \sum_{h \in G} b_h \psi(h) \right) \psi(g) \right)
\]

\[
= \sum_{g \in G} a_g \psi(g) = \psi(w) \psi(v) \quad \square
\]

Remark: if we take \( F = \mathbb{Q} (\xi) \), where \( \xi \) is a primitive \( p \)-th root of unity we get the isomorphism:

\[\mathbb{Q} (\xi) G \cong \mathbb{Q} (\xi) \oplus \ldots \oplus \mathbb{Q} (\xi), \quad |G| \text{ - times}\]

For \( \chi \in \hat{G} \), set \( \varepsilon_\chi = (0, \ldots, 0, 1, 0, \ldots 0) \in \mathbb{Q} (\xi) \), where 1 is in the \( \chi \)-th position. Then the set \( \{ \varepsilon_\chi \mid \chi \in \hat{G} \} \)

is a basis for \( \mathbb{Q} (\xi) \) consisting of orthogonal idempotents.

Define: \( e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) g = \psi^{-1} (\varepsilon_\chi) \)

Then the elements \( e_\chi \) are also idempotents.
since $e_{\chi}^2 = \psi^{-1}(\varepsilon_{\chi}) \psi^{-1}(\varepsilon_{\chi}) = \psi^{-1}(\varepsilon_{\chi}^2) = \psi^{-1}(\varepsilon_{\chi}) = e_{\chi}$

Moreover, if $\chi \neq \chi'$ we get

$$e_{\chi} e_{\chi'} = \psi^{-1}(\varepsilon_{\chi}) \psi^{-1}(\varepsilon_{\chi'}) = \psi^{-1}(\varepsilon_{\chi} \varepsilon_{\chi'}) = \psi^{-1}(0) = 0.$$ 

Therefore the set $\{ e_{\chi} \mid \chi \in \hat{G} \}$ is a basis for $\mathbb{Q}(\xi)G$

consisting of orthogonal idempotents.

Remark: if $f = \sum_{g \in G} f(g) g$, then we can express $f$ in terms

of the idempotents as follows:

$$f = \sum_{\chi \in \hat{G}} \hat{f}(\chi) e_{\chi}.$$ 

Our next goal will be to obtain a similar isomorphism

for the rational group ring $\mathbb{Q}G$. Combining the isomorphism

$\psi$ given (2.3) with the inclusion $\mathbb{Q}G \longrightarrow \mathbb{Q}(\xi)G$ gives

the injection

$$\mathbb{Q}G \xrightarrow{\text{inc}} \mathbb{Q}(\xi)G \xrightarrow{\psi} \mathbb{Q}(\xi) \oplus \cdots \oplus \mathbb{Q}(\xi).$$

We wish to find the image of $\mathbb{Q}G$ under this map.

First, we study the action of the group $\text{Gal}(\mathbb{Q}(\xi) : \mathbb{Q})$
on the rings \( \mathbb{Q}(\xi)G \) and \( \mathfrak{g} \mathbb{Q}(\xi) \).

Observe that \( \text{Gal}(\mathbb{Q}(\xi) : \mathbb{Q}) \) acts on \( \mathbb{Q}(\xi)G \) by its natural action on \( \mathbb{Q}(\xi) \).

For \( \sigma \) in \( \text{Gal}(\mathbb{Q}(\xi) : \mathbb{Q}) \) and \( \nu = \sum_{g \in G} a_g g \) in \( \mathbb{Q}(\xi)G \), define

\[
\sigma(\nu) = \sigma \left( \sum_{g \in G} a_g g \right) = \sum_{g \in G} \sigma(a_g) g.
\]

It is clear that every \( \sigma \) induces in this way a \( \mathfrak{g} \)-algebra isomorphism on \( \mathbb{Q}(\xi)G \). Moreover, \( \mathbb{Q}G \) is fixed under \( \sigma \).

The action of \( \text{Gal}(\mathbb{Q}(\xi) : \mathbb{Q}) \) over \( \mathfrak{g} \mathbb{Q}(\xi) \) is defined as follows:

For \( \nu = \sum_{\chi \in \hat{G}} A_\chi \chi \), in \( \mathfrak{g} \mathbb{Q}(\xi) \), define:

\[
\sigma(\nu) = \sum_{\chi \in \hat{G}} \sigma(A_\chi) \sigma(\chi)
\]

where \( \sigma(\chi)(g) = \sigma(\chi(g)) \), for all \( g \in G \).

Remark: The value of \( \sigma \) on \( \nu \) can be also written as

\[
\sigma(\nu) = \sum_{\chi \in \hat{G}} B_\chi \chi,
\]
where $B_\chi = \sigma(\Lambda_{\sigma^{-1}(\chi)})$.

(2.4) Lemma: The following diagram commutes

\[
\begin{array}{ccc}
\mathbb{Q}(\xi)G & \xrightarrow{\psi} & \mathbb{Q}(\xi)G \\
\sigma \downarrow & & \sigma \downarrow \\
\mathbb{Q}(\xi)G & \xrightarrow{\psi} & \mathbb{Q}(\xi)G
\end{array}
\]

for all $\sigma$ in Gal($\mathbb{Q}(\xi): \mathbb{Q}$).

Proof: We need to show $\sigma \psi = \psi \sigma$. For $v$ in $\mathbb{Q}(\xi)G$ then

\[
\psi \sigma (v) = \psi \sigma \left( \sum_{g \in G} a_g g \right) \\
= \psi \left( \sum_{g \in G} \sigma(a_g) g \right) = \sum_{\chi \in \hat{G}} B_\chi \chi,
\]

where $B_\chi = \sum_{g \in G} \sigma(a_g) \chi(g)$.

On the other hand,

\[
\sigma \psi (v) = \sigma \left( \sum_{\chi \in \hat{G}} A_\chi \chi \right) = \sum_{\chi \in \hat{G}} \sigma(A_\chi) \sigma(\chi) \\
= \sum_{\chi \in \hat{G}} \sigma(\Lambda_{\sigma^{-1}(\chi)}) \chi,
\]
where $A_\chi = \sum_{g \in G} a_g \chi(g)$. 

Thus $\sigma(A_{\chi^{\sigma^{-1}}}) = \sigma\left(\sum_{g \in G} a_g \sigma^{-1}\chi(g)\right)$

$= \sum_{g \in G} \sigma(a_g) \chi(g) = B_\chi$.

Therefore $\sigma \psi = \psi \sigma$. □

(2.5) Corollary: Let $a$ be in $\mathbb{Q}(\xi)G$. Then $a$ is in $\mathbb{Q}G$ if and only if $\sigma(\psi(a)) = \psi(a)$, for all $\sigma$ in $\text{Gal}(\mathbb{Q}(\xi): \mathbb{Q})$.

Proof: Observe that $\sigma(\psi(a)) = \psi(\sigma(a))$, by the previous theorem. Thus $\sigma \psi(a) = \psi(a)$ if and only if $\sigma(a) = a$ which happens if and only if the coefficient of $a$ lie in $\mathbb{Q}$. □

Definition: Let $\chi_1$ and $\chi_2$ be in $\hat{G}$. We say that $\chi_1$ is a conjugate to $\chi_2$ via $\text{Gal}(\mathbb{Q}(\xi): \mathbb{Q})$ if for some $\sigma$ in $\text{Gal}(\mathbb{Q}(\xi): \mathbb{Q})$ we have: $\chi_1 = \sigma \chi_2$.

Remark: If $\chi_0$ is the trivial character, its class consists of $\chi_0$ alone. If $\chi \neq \chi_0$, $\overline{\chi}$ has $p-1$ elements. Therefore, if
t is the number of classes, we have

\[(t-1)(p-1) + 1 = |G| = p^n.\]

Thus \[t = \frac{p^n - 1}{p - 1} + 1 = s + 1,\] where \[s = \frac{p^n - 1}{p - 1}.\]

(2.6) Lemma: Let \(\chi_0, \chi_1, \ldots, \chi_s, s = \frac{p^n - 1}{p - 1}\) be representatives of the conjugacy classes. Then if \((\phi \otimes (\xi))_{\text{Gal}}\) denotes the set elements in \(\phi \otimes (\xi)\) fixed under \(\text{Gal}(\mathbb{Q}(\xi) : \mathbb{Q})\), we have:

\[(\phi \otimes (\xi))_{\text{Gal}} \cong \phi \otimes (\xi) \chi_1 \otimes \ldots \otimes (\xi) \chi_s\]

Proof: Observe that \(\sum_{\chi} A_{\chi} \chi\) is fixed by \(\text{Gal}(\mathbb{Q}(\xi) : \mathbb{Q})\) if and only if

\[\sigma \left( \sum_{\chi} A_{\chi} \chi \right) = \sum_{\chi} A_{\chi} \chi,\]

so

\[\sum_{\chi} \sigma (A_{\chi}) \sigma (\chi) = \sum_{\chi} A_{\chi} \chi.\]

Therefore \(\sigma (A_{\phi^{-1}(\chi)}) = A_{\chi}\) for all \(\chi\), or
\[ A_{\sigma^{-1}} \chi = \sigma^{-1} ( A_\chi ) \]

or

\[ A_{\sigma} \chi = \sigma ( A_\chi ) \text{ for all } \chi . \]

So, if \( \chi_i \) represents the conjugacy class of \( \chi \), then

we know \( A_{\sigma} \chi \) by knowing \( A_{\chi_i} \).

Map \( \sum_{\chi \in \hat{G}} A_\chi \chi \) to: \( A_{\chi_0} \chi_0 + \sum_{i=1}^{s} A_{\chi_i} \chi_i \).

Conversely, given \( A_{\chi_0}, A_{\chi_1}, \ldots, A_{\chi_s} \) in \( \mathbb{Q}(\xi) \), take \( \chi \in \hat{G} \) and write: \( \chi = \sigma ( \chi_i ) \) for some \( \sigma \in \text{Gal}( \mathbb{Q}(\xi): \mathbb{Q} ) \), some \( i \in \{ 0, 1, \ldots, s \} \) and define

\[ A_\chi = \sigma A_{\chi_i} \]

Then \( \sum_{\chi \in \hat{G}} A_\chi \chi \) is fixed by \( \text{Gal}( \mathbb{Q}(\xi): \mathbb{Q} ) \). \( \square \)

The following is the Perlis - Walker Theorem (see [K], page 56). We include a proof for completeness.
(2.7) Theorem: Let \( \chi_0, \chi_1, \ldots, \chi_s \) be a set of representatives of the different conjugacy classes of characters under the action of \( \text{Gal}(\mathbb{Q}(\xi): \mathbb{Q}) \). Then the map

\[
\psi': \mathbb{Q} G \longrightarrow \mathbb{Q} \oplus \mathbb{Q}(\xi) \oplus \ldots \oplus \mathbb{Q}(\xi)
\]

\[
g \longrightarrow (1, \chi_1(g), \ldots, \chi_s(g))
\]

is a \( \mathbb{Q} \)-algebra isomorphism.

**proof:** By the previous lemma we have the isomorphism

\[
(\mathbb{Q} \oplus \mathbb{Q}(\xi))^{\text{Gal}} \cong \mathbb{Q} \oplus \mathbb{Q}(\xi) \chi_1 \oplus \ldots \oplus \mathbb{Q}(\xi) \chi_s.
\]

On the other hand, \( \psi \) induces an isomorphism \( \psi' \)

\[
\mathbb{Q} G = (\mathbb{Q}(\xi) G)^{\text{Gal}} \cong (\mathbb{Q} \oplus \mathbb{Q}(\xi) G)^{\text{Gal}}.
\]

Then \( \psi' \) is the composition of both isomorphisms. \( \Box \).

4. **GROUP ACTION ON \( \mathbb{Q} G \).**

We consider here an action of the multiplicative group \( \mathbb{F}_p^* \) on the rational group ring \( \mathbb{Q} G \), for \( G = (\mathbb{F}_q, +) \). As before, the operation in \( G \) will be written multiplicative.

So the identity is 1, not 0.
For \[ \sum_{g \in G} a_g g \] in \( \mathbb{Q} G \) and for \( b \in F_p^* \), we define

\[
\left[ \sum_{g \in G} a_g g \right]^b = \sum_{g \in G} a_g (g^b),
\]

where \( g^b = g \cdot g \cdots g \) (\( b \) times) in \( (G, \cdot) = (F_q, +) \) really means \( g + g + \cdots + g \) \( b \) times.

Notice that (additively), \( F_q \) has \( p \)-torsion, so multiplication by \( b \in F_p^* \) makes sense.

We can also define an action of \( F_p^* \) on \( \mathfrak{g} \mathbb{Q}(\xi) \). Let \( V \) be in \( \mathfrak{g} \mathbb{Q}(\xi) \). Thus \( V = \sum_{\chi \in \hat{G}} A_{\chi} \chi \), where \( A_{\chi} \in \mathbb{Q}(\xi) \).

Hence we can write \( A_{\chi} = \sum_{i=1}^{p-1} a_i \xi^i \), where \( a_i \in \mathbb{Q} \) for all \( 1 \leq i \leq p-1 \).

For \( b \in F_p^* \) define

\[
\left[ \sum_{\chi \in \hat{G}} A_{\chi} \chi \right]^b = \sum_{\chi \in \hat{G}} (A_{\chi})^b \chi,
\]
where \((A_x)_b = \sum_{i=1}^{p-1} a_i \xi^{bi}\).

Since \(\xi^p = 1\), \(\xi^{bi}\) is well defined for \(b \in \mathbb{F}_p^*\).

Let \(\sigma_b\) denote the map induced by the action of \(b \in \mathbb{F}_p^*\) over \(\mathbb{Q}G\). Then it is easy to check that the following diagram commutes

\[
\begin{array}{c}
\mathbb{Q}G \\ \sigma_b \downarrow \\
\mathbb{Q}G
\end{array} 
\begin{array}{c}
\psi' \rightarrow \mathbb{Q} \oplus \mathbb{Q}(\xi) \oplus \ldots \oplus \mathbb{Q}(\xi) \\ \sigma_b \downarrow \\
\psi' \rightarrow \mathbb{Q} \oplus \mathbb{Q}(\xi) \oplus \ldots \oplus \mathbb{Q}(\xi)
\end{array}
\]

As a result of this, we get

(2.8) Lemma: Let \(v = \sum_{g \in G} a_g g\) in \(\mathbb{Q}G\), such that \(\psi'(v)\) is invariant under \(\mathbb{F}_p^*\). Then, for all \(g \in G\) we have

\[a_g b = a_g\], for all \(b \in \mathbb{F}_p^*\).

Proof: By hypothesis we get \(\psi'(v) = (\psi'(v))^b = \psi'(v)^b\),

for all \(b \in \mathbb{F}_p^*\). Thus \(v = (v)^b\), since \(\psi'\) is injective.

Hence, we can write
Comparing coefficients in both sides gives

\[ a_g b = a_g, \text{ for all } g \in G. \]

Thus the lemma is proved. \( \square \)

5. SOME CONDITIONS FOR MINIMALITY.

Now take \((G, \cdot) = (F_q, +)\). Note that the operation in \(F_q\) is addition, but in the group ring, we call the operation in \(F_q\) multiplication. So 0 in \((F_q, +)\) becomes 1 in \((G, \cdot)\).

We will consider a function \(f: G \rightarrow \{0, 1, -1\}\) such that \(|f(x)| = 1\), for \(x \neq 0\), and \(f(0) = 0\). We have seen in Chapter 1, that \(f\) is minimal if and only if it satisfies the following "condition A"

a) \(f(x_0) = 0\).
b) \( |\hat{f}(\chi)| = |G|^{1/2} = p^{n/2} \), for all \( \chi \neq \chi_0 \).

We can express condition A in terms of equations in the group ring \( \mathbb{Q}G \) by considering \( f \) as an element in \( \mathbb{Q}G \).

\[
f = \sum_{g \in G} f(g) \cdot g
\]

Recall from (2.7) the isomorphism \( \psi' \)

\[
\psi': \mathbb{Q}G \longrightarrow \mathbb{Q}(+) \mathbb{Q}(\xi)(+) \ldots(+) \mathbb{Q}(\xi)
\]

\[
f \longrightarrow (\hat{f}(\chi_0), \hat{f}(\chi_1), \ldots, \hat{f}(\chi_s))
\]

where \( \chi_0, \chi_1, \ldots, \chi_s \) are all the representatives of the conjugacy classes of \( \text{Gal}(\mathbb{Q}(\xi):\mathbb{Q}) \).

The following result is due to R. Perlis.

(2.9) Lemma: Let \( f \) be a minimal function, and \( \chi \) be any character on \( G \). Then we have

\[
\hat{f}(\chi) = \pm \hat{\mathbb{I}}(\chi)
\]

where \( \mathbb{I} \) is the quadratic function.
theory. The elements $\hat{f}(x_i)$ lie in $\mathbb{Z}(\xi)$, which is the ring of integers of the cyclotomic field $\mathbb{Q}(\xi)$. From condition A we get

$$\hat{f}(x_i) \cdot \hat{f}(x_i) = p^n, \quad x_i \neq x_0.$$ (1)

This equation gives a condition at the level of ideals in $\mathbb{Q}(\xi)$:

$$\left(\hat{f}(x_i)\right) \cdot \left(\hat{f}(x_i)\right) = (p)^n$$ (2)

But the ideal $(p)$, generated by $p$, has prime ideal decomposition

$$(p) = (1 - \xi)^{p-1}.$$ (3)

From (2) and (3), and the uniqueness of prime ideal factorization we conclude that the ideals $(\hat{f}(x_i))$ and $(\hat{f}(x_i))$, can be factored into powers of $(1 - \xi)$ namely:

$$\left(\hat{f}(x_i)\right) = (1 - \xi)^k, \quad \text{and} \quad \left(\hat{f}(x_i)\right) = (1 - \xi)^l,$$
where \( k + 1 = n(p-1) \). Also observe that

\[
\left[ \hat{f}(x_i) \right] = (\hat{f}(x_i)) = (1 - \xi)^k
\]

\[= (1 - \xi)^k = (1 - \xi)^k.\]

From this we conclude \( k = 1 = n(p-1)/2 \), which implies

\[
(\hat{f}(x_i)) = (1 - \xi)^{n(p-1)/2}, \text{ for } x_i \neq x_0 \quad (4)
\]

The same argument works for the quadratic function \( \Phi \), in which case we obtain

\[
\hat{\Phi}(x_i) = (1 - \xi)^{n(p-1)}, \text{ for } x_i \neq x_0. \quad (5)
\]

From (4) and (5) we get : \( (\hat{f}(x_i)) = (\hat{\Phi}(x_i)) \) which implies : \( \hat{f}(x_i) \) and \( \hat{\Phi}(x_i) \) are associated. Thus they are equal up to a unit \( u \) in \( \mathbb{Q} \& \mathbb{Q} \)

\[
\hat{f}(x_i) = u \hat{\Phi}(x_i) \quad (6)
\]

By Kummer's lemma, the units in \( \mathbb{Q}(\xi) \) are of the form

\[
\rho \xi^k, \text{ for some real unit } \rho \text{ and some positive integer } k.
\]
Taking absolute values in (6) gives \( |u| = 1 \). Hence \( p = \pm 1 \).

Thus (6) becomes

\[ \hat{f}(\chi_i) = \pm \xi^k \hat{\varphi}(\chi_i), \quad \text{for all } \chi_i \neq \chi_0. \quad (7) \]

The next step will be to prove \( k = 0 \).

Without loss of generality, we may assume that the sign in (7) is positive. For \( \chi \) in the dual of \( G \), there is an element in \( G \), say \( a \), such that:

\[ \chi(x) = \xi \text{tr}(ax), \quad \text{for all } x \text{ in } G. \]

Define

\[ A_i = \sum_{\text{tr}(ag) = i} f(g), \quad 0 \leq i \leq p - 1. \]

Thus we get:

\[ \hat{f}(\chi) = \sum_{i = 0}^{p-1} A_i \xi^i \]

Similarly, we have:

\[ \hat{\varphi}(\chi) = \sum_{i = 0}^{p-1} B_i \xi^i \]

where

\[ B_i = \sum_{\text{tr}(ag) = i} \hat{\varphi}(g). \]

Thus (7) becomes
\[ \sum_{i=0}^{p-1} A_i \xi^i = \xi^k \sum_{i=0}^{p-1} B_i \xi^i \]
\[ = \sum_{i=0}^{p-1} B_i \xi^{i+k} . \]

Making \( i+k = j \), in the last sum, produces
\[ \sum_{i=0}^{p-1} A_i \xi^i = \sum_{i=0}^{p-1} B_{j-k} \xi^j \]

From this we get
\[ \sum_{i=1}^{p-1} A_i \xi^i + A_0 = \sum_{j=1}^{p-1} A_{j-k} \xi^j + B_{-k} . \]

Using the fact \( 1 + \xi + \xi^2 + \ldots + \xi^{p-1} = 0 \), gives
\[ \sum_{i=1}^{p-1} A_i \xi^i - A_0 \left( \sum_{i=1}^{p-1} \xi^i \right) = \sum_{i=j}^{p-1} B_{j-k} \xi^j - B_{-k} \left( \sum_{i=1}^{p-1} \xi^i \right) \]

Thus, after collecting all terms in one side we obtain
\[ \sum_{i=1}^{p-1} \left[ A_i - A_0 - (B_{i-k} - B_{-k}) \right] \xi^i = 0 \quad (8) . \]

Next, observe that the elements \( \xi, \xi^2, \ldots, \xi^{p-1} \)

are linearly independent in \( \mathbb{Z}(\xi) \). As a result, we conclude
\[ A_i - A_0 = B_{i-k} - B_{-k} \]
\[ \ldots \quad \ldots \quad \ldots \quad (9) \]
Adding up these \(p-1\) equations gives

\[
\sum_{i=0}^{p-1} A_i - p A_0 = \sum_{i=0}^{p-1} B_i - p B_{-k}.
\]

(10)

Using the condition \(\hat{\psi}(x_0) = \hat{f}(x_0) = 0\), gives us

\[
\sum_{i=0}^{p-1} A_i = \sum_{i=0}^{p-1} B_i = 0
\]

(11)

From (10) and (11), it follows that \(A_0 = B_{-k}\).

Finally, to prove that \(k = 0\), we discuss the parity of \(A_0\) and \(B_{-k}\). Notice that \(A_0\), is a sum of \(p^{n-1}\) terms of the form \(f(g)\), all of which are either 1 or -1, except for \(f(0)\) which is equal to 0. Thus \(A_0\) is even.

Similarly, \(B_{-k}\) is a sum of \(p^{n-1}\) terms each of them being 1 or -1. Thus \(B_{-k}\) is odd if \(k \neq 0\).

Therefore \(A_0 \neq B_{-k}\) if \(k \neq 0\) which is a contradiction.

That ends the proof. \(\square\)
(2.10) Corollary: Let \( f \) be a minimal function, then there exists a function \( \rho : G \rightarrow \{1, -1\} \), such that

i) \( f(g) = \rho(g) \Phi(g) \), for all \( g \) in \( G \).

ii) \( \rho(bg) = \rho(g) \), for \( b \) in \( \mathbb{F}_p^* \) and \( g \) in \( G \).

Proof: First, observe that \( f(g) = \pm \Phi(g) \), for all \( g \) in \( G \) since \( f \) and \( g \) take the values 1 or -1, except for \( f(0) = \Phi(0) \) which is 0. Thus, there exists a function

\[
\rho : G \rightarrow \{1, -1\}
\]

such that \( f(g) = \rho(g) \Phi(g) \), for all \( g \) in \( G \).

It remains to show \( \rho \) is constant on the lines.

Consider the isomorphism \( \psi' \), given in (2.7). From the lemma (2.9) it follows:

\[
\psi'(f) = \varepsilon \psi'(\Phi)
\]  

(1)

where \( \varepsilon = (1, \varepsilon_1 \ldots \varepsilon_s) \), \( \varepsilon_i \in \{1, -1\} \) if \( i \neq s \).

with \( \varepsilon_i = \pm 1 \), \( 1 \neq i \neq s \).

Applying \( \psi'^{-1} \) on both sides of (1), gives
where $u = \psi^{-1}(\xi)$ is an element in $\mathbb{G}$.

Notice that $\xi$ is invariant under $F_p^*$. Then $u$ is also invariant under $F_p^*$. Therefore by lemma (2.8) we have $u(bg) = u(g)$, for all $g$ in $G$, and $b$ in $F_p^*$.

Let $g \in G$, then from equation (2), it follows

$$f(g) = u \ast \varphi(g)$$

$$= \sum_{h \in G} u(h) \varphi(h - g).$$

Similarly, for $b$ in $F_p^*$

$$f(bg) = u \ast \varphi(bg) = \sum_{h \in G} u(h) \varphi(h - bg).$$

$$= \sum_{h \in G} u(bh) \varphi(bh - bg),$$

$$= \left[ \sum_{h \in G} u(h) \varphi(h - g) \right] \varphi(b),$$

$$= f(g) \varphi(b).$$

Thus

$$\phi(bg) = \frac{f(bg)}{\varphi(bg)} = \frac{f(g) \varphi(b)}{\varphi(g) \varphi(b)}.$$
and that ends the proof.
CHAPTER 3

GROUPS ACTING ON THE SET OF MINIMAL FUNCTIONS

1. INTRODUCTION

Let \( G = \mathbb{F}_q \), where \( q = p^n \). Let \( M \) denote the set of functions \( f : G \rightarrow \{0, 1, -1\} \), such that \( f(0) = 0 \) and \( |f(x)| = 1 \), for \( x \neq 0 \). Let \( M_1 \) be the subset of consisting of all functions \( f \) in \( M \) of the form \( p \cdot \Phi \), where \( \Phi \) is the quadratic function on \( G \), and \( p \) is a function on \( G \) with values \( \pm 1 \) satisfying \( p(cx) = p(x) \) for all \( x \) in \( \mathbb{F}_q \) and all \( c \) in \( \mathbb{F}_p \) (We say "\( p \) is constant on the lines ").

(3.1) Definition: For any \( f \) in \( M \) the minimality conditions on \( f \) are given by:

a) \( \hat{f}(x_0) = 0 \), b) \( |\hat{f}(x)| = q^{1/2} \), for \( x \neq x_0 \).

The set of minimal functions denote by \( M_0 \), is the subset of \( M \), whose members satisfy the minimality conditions.

-45-
By corollary 2.10 of chapter 2 we have

$$m_0 \leq m_1 \leq m.$$  \hspace{1cm} (1)

Remark: In general, we don't have equality in (1). As an example consider $G = ([F_9, +] \times [F_3, +])$, whose elements are labeled

- $a_1 = (0, 0)$
- $a_2 = (0, 1)$
- $a_3 = (0, 2)$
- $a_4 = (1, 0)$
- $a_5 = (1, 1)$
- $a_6 = (1, 2)$
- $a_7 = (2, 0)$
- $a_8 = (2, 1)$
- $a_9 = (2, 2)$

Put $f_1(a_1, \ldots, a_9) = (0, -1, 1, 1, 1, 1, 1, 1, 1, 1)$

$f_2(a_1, \ldots, a_9) = (0, 1, 1, 1, 1, 1, -1, -1, 1, 1)$

$f_3(a_1, \ldots, a_9) = (0, 1, 1, -1, 1, 1, -1, -1, 1, 1)$

Then $f_1$ is in $M$ but not in $M_1$, $f_2$ is in $M_1$ but not in $M_0$. The only minimal function among them is $f_3$.

We want to determine the conditions under which a function in $M_1$ is in $M_0$. 
2. GROUP ACTION ON \( \mathbb{M} \).

There are several groups acting on the set \( \mathbb{M} \). The first group to deserve our attention is the general linear group \( GL_n(\mathbb{F}_p) \), whose elements are \( \mathbb{F}_p \)-linear invertible maps

\[
\sigma : G \rightarrow G.
\]

The group \( GL_n(\mathbb{F}_p) \) acts on \( \hat{G} \) as follows:

- For \( \chi \) in \( \hat{G} \) and \( \sigma \) in \( GL_n(\mathbb{F}_p) \) define

\[
\chi^\sigma(g) = \chi(\sigma(g)), \text{ for } g \text{ in } G.
\]

It is easy to check that the map \( \chi^\sigma \) is a character on \( G \).

\((3.1)\) Lemma: The group \( GL_n(\mathbb{F}_p) \) acts on the set of minimal functions \( \mathbb{M}_0 \) by

\[
(\mathbf{f})^\sigma = \mathbf{f} \sigma, \text{ for } \mathbf{f} \text{ in } \mathbb{M}_0 \text{ and } \sigma \text{ in } GL_n(\mathbb{F}_p).
\]

Proof: Let \( \mathbf{f} \) be in \( \mathbb{M}_0 \) and \( \sigma \) in \( GL_n(\mathbb{F}_p) \) we want to show that the composite function \( \mathbf{h} = \mathbf{f} \sigma \) is a minimal function. Thus we need to check the two minimality conditions.
We have: \( h = f \sigma \), so

\[
\hat{h}(\chi_0) = \sum_{g \in G} f(\sigma(g)) = \sum_{g \in G} f(g) = 0,
\]

since \( \sigma(g) \) runs over all of \( G \) as \( g \) runs on \( G \).

Thus the first condition is satisfied.

To show the second part, take \( \chi \neq \chi_0 \) in \( \hat{G} \). Then

\[
| \hat{h}(\chi) | = | \sum_{g \in G} f(\sigma(g)) \chi(g) |
\]

\[
= | \sum_{g \in G} f(g) \chi(\sigma^{-1}(g)) |
\]

\[
= | \sum_{g \in G} f(g) \chi^{\sigma^{-1}}(g) |
\]

\[
= | \hat{f}(\chi^{\sigma^{-1}}) | = p^{n/2},
\]

since \( f \) is minimal and \( \chi^{\sigma^{-1}} \neq \chi_0 \).

That ends the proof.

(3.2) Lemma: Let \( |M_0| \) denote the number of minimal functions on \( \mathbb{F}_q \). Then: \( 2 \leq |M_0| \leq 2^s \), with \( s = (p^n-1)/(p-1) \).

proof: We have shown that the quadratic function and its
negative are minimal functions. Thus $2 \mid \mathcal{M}_0 \mid$.

On the other hand, every minimal function looks like $f = \rho \varphi$, where $\rho$ is $\pm 1$ function constant on the lines. So any function $f$ is determined by the values of $\rho$ on the different lines. Since $\rho$ can take only two values $\pm 1$ at each of the lines, there are at the most $2^n$ different choices for $\rho$ and thus for $f$. $\square$

If we let $G = \text{GL}_n(F_p)$ act on the quadratic function $\varphi$, the size of the orbit is given by

$$| G - \text{orbit of } \varphi | = \frac{|G|}{|\text{Stab } \varphi|}.$$

Here, $\text{Stab } \varphi = \{ \sigma \in G \mid \varphi \sigma = \varphi \} = \{ s \in G \text{ such that } \sigma \text{ (square) } = \text{square} \}$.

By Jacobson, chapter 7 [J], the order $G = \text{GL}_n(F_q)$ is

$$|G| = (p^n - 1)(p^n - p) \ldots (p^n - p^{n-1}).$$

To find the order of $\text{Stab } \varphi$ is more difficult than one
might expect. It is easy, however, to identify a large
subgroup inside of the stabilizer.

Let \( \mathcal{H} \) denote the direct product of \( \mathbb{F}_q^* \times \text{Gal}(\mathbb{F}_q / \mathbb{F}_p) \).

(3.3) Lemma \( \mathcal{H} \) is a subgroup of \( \text{Stab} \Phi \).

proof: The elements of \( \mathcal{H} \) are of the form \( c \Phi \) with \( c \) a non-zero square in \( \mathbb{F}_q \) and \( \Phi \) a field automorphism of \( \mathbb{F}_q \). We need to show that \( c \Phi \) sends squares to squares.

Let \( x = y^2 \) with \( y \neq 0 \). Then \( c \Phi (x) = c \Phi (\Phi(y))^2 \), and that proves the claim. \( \Box \).

Remark: We have found by numerical computations the order of
\( \text{Stab} \Phi \), for the fields \( \mathbb{F}_9, \mathbb{F}_{25}, \mathbb{F}_{49}, \mathbb{F}_{121}, \mathbb{F}_{169}, \mathbb{F}_{289}, \mathbb{F}_{27}, \mathbb{F}_{125} \) and \( \mathbb{F}_{343} \) in these cases were given by the formula

\[
|\text{Stab} \Phi| = \frac{p^n - 1}{2} n \quad (2)
\]

Also, for \( n = 1 \) and \( p \) arbitrary, the above formula is obviously true.
Therefore we have in these examples |\text{Stab } \Psi | = |\mathbb{H}|.

We conjecture that \text{Stab } \Psi = \mathbb{H} always. An equivalent formulation of this conjecture is:

**Conjecture:** If \( \sigma \in \text{GL}_n(\mathbb{F}_p) \) satisfies \( \sigma(1) = 1 \), \( \sigma(x) \) square in \( \mathbb{F}_q \) = square in \( \mathbb{F}_q \), then \( \sigma(xy) = \sigma(x)\sigma(y) \).

Using formula 2 in (1), we can get the size of the orbit of \( \Psi \) for the fields \( \mathbb{F}_{27} \), \( \mathbb{F}_{125} \), and \( \mathbb{F}_{343} \). These values are 288, 9600, and 65856.

**Comment:** McGehee has found by computer methods that there are exactly 288 minimal functions for the field \( \mathbb{F}_{27} \). In this case all minimal functions lie in the \( \text{GL}_3(\mathbb{F}_3) \)-orbit of \( \Psi \).

**3. EVEN DEGREE EXTENSIONS**

In this section we devote our attention to functions over \( \mathbb{F}_p^n \) where \( n \) is even.

From now on \( G \) is the group \( (\mathbb{F}_p^n,+ ) \) \( n \) is even. We consider \( G \) as a vector space over \( \mathbb{F}_p \). By a line in \( G \), we mean
an $\mathbb{F}_p$-line through the origin in $\mathbb{F}_p^n$

Let $\mathcal{G}$ be the group of all invertible maps $\sigma$ on $G$ taking hyperplanes to hyperplanes.

(3.4) Lemma: Let $(x_1, \ldots, x_S)$ be representatives of the lines in $G$ over $\mathbb{F}_p$. Let $f$ be in $\mathcal{M}_1$. Then $f$ is minimal if and only if

\begin{enumerate}
  \item \[ \sum_{i=1}^{S} f(x_i) = 0 \]
  \item \[ \left| \sum_{x_i \in \ker \chi} f(x_i) \right| = p^{n/2-1}, \quad \text{for all } \chi \neq \chi_0. \]
\end{enumerate}

proof: Since $f$ is in $\mathcal{M}_1$, we have $f(x) = \rho(x) \Psi(x)$, for all $x$ in $G$. Now $G$ is an extension of $\mathbb{F}_p$ of even degree and therefore the elements in $\mathbb{F}_p$ are squares in $G$. From this we obtain: $\Psi(cx) = \Psi(x)$, for any $c$ in $\mathbb{F}_p^*$ and any $x$ in $G$

This implies that $f$ is constant on the lines of $G$.

Next assume that $f$ satisfy the minimality conditions.
Then
\[ 0 = \hat{\chi}(\chi_0) = \sum_{g \in G} f(g) = \sum_{i=1}^{S} \sum_{c \in F_p^*} f(cx_i) \]
\[ = (p-1) \sum_{i=1}^{S} f(x_i). \]

From this we get a).

To show b), take a character \( \chi \neq \chi_0 \). Then we have
\[ p^{n/2} = \left| \sum_{g \in G} f(g) \chi(g) \right| = \left| \sum_{i=1}^{S} f(x_i) \sum_{c \in F_p^*} \chi(cx_i) \right|. \]

Notice that
\[ \sum_{c \in F_p^*} \chi(cx_i) = \begin{cases} p-1 & \text{if } x_i \in \text{Ker} \chi \\ -1 & \text{otherwise} \end{cases}. \]

Thus we obtain
\[ p^{n/2} = |(p-1) \sum_{x_i \in \text{Ker} \chi} f(x_i) - \sum_{x_i \notin \text{Ker} \chi} f(x_i)|. \]

Using part a) we get
\[ \sum_{x_i \notin \text{Ker} \chi} f(x_i) = -\sum_{x_i \in \text{Ker} \chi} f(x_i) \]
Therefore

\[ p^{n/2} = \prod_{x_i \in \text{Ker} \chi} f(x_i) \]

From this it follows

\[ p^{(n/2)-1} = \prod_{x_i \in \text{Ker} \chi} f(x_i) \]

for all \( x \neq x_0 \).

Conversely, the minimality condition (3.1) follows immediately from a) and b). Thus the proof is complete. \( \square \).

(3.5) Lemma: The group \( \mathcal{G} \) acts on the set \( M_0 \) of minimal functions.

Proof: Let \( f \in M_0 \) and \( \sigma \in \mathcal{G} \). We want to show that \( f \sigma \) satisfies the conditions of lemma (3.4).

In the first place as \( x_i \) runs over representatives of the s lines, so does \( \sigma(x_i) \). Thus

\[ \sum_{i=1}^{S} f(\sigma(x_i)) = \sum_{j=1}^{S} f(x_j) = 0. \]

Hence a) is true.
To show b), take a character \( \chi \neq \chi_0 \). Then

\[
| \sum_{x_i \in \text{Ker} \chi} f(\sigma(x_i)) | = | \sum_{x_j \in \sigma(\text{Ker} \chi)} f(x_j) | = | \sum_{x_j \in \text{Ker} \chi'} f(x_j) | = p^{n/2-1}
\]

where \( \chi' = \sigma \chi \)

Therefore b) is also true, and that ends the proof. \( \Box \).

Now consider the smallest value of the even integer \( n \):

\( n = 2 \).

The elements of \( \mathcal{E} \) are all maps taking lines to lines.

Thus \( | \mathcal{E} | = s! \) where \( s = \frac{p^2 - 1}{p - 1} = p+1 \) is the number of lines in \( \mathbb{F}_{p^2} \).

A line \( \mathbb{F}_p \cdot x_i \) is said to be **positive** if \( x_i \) is a square in \( \mathbb{F}_q \), otherwise is said to be **negative**.

There are \( s/2 \) positive lines and \( s/2 \) negative lines.

The stabilizer of \( \Phi \) consists of those maps \( \sigma \) taking positive
lines to positive lines and negative lines to negative lines.

Thus we get $|\text{stab} \mathbb{E}| = (s/2)! (s/2)!$. Hence

$$| \mathcal{E}, \mathbb{E} | = \frac{| \mathcal{E} |}{|\text{Stab} \mathbb{E}|} = \frac{s!}{(s/2)! (s/2)!}$$

= binomial coefficient $\binom{s}{s/2}$.

We will see that the number $\binom{s}{s/2}$ is equal to $|\mathbb{W}_0|$ for the field $\mathbb{F}_p^2$.

(3.6) Proposition: Let $G = \mathbb{F}_p^2$, and let $f$ be a function on $\mathbb{W}_0$. Then $f$ is minimal if and only if

$$\sum_{i=1}^{s} f(x_i) = 0. \quad (1)$$

proof: By the previous lemma, it is enough to show that for any character $\chi \neq \chi_0$, condition b) holds. Since $\chi \neq \chi_0$ we see that $\dim \text{Ker} \chi = 1$, so there is only one line in $\text{Ker} \chi$, say $\text{Ker} \chi = \mathbb{F}_p \cdot x_1$. Thus we have

$$\left| \sum_{x_1 \in \text{Ker} \chi} f(x_1) \right| = \left| f(x_1) \right| = | \pm 1 | = p^{(2/2)-1}.$$
This proves b) of the lemma 3.4. □.

(3.7) Corollary: The number of minimal functions for $F_{p^2}$

is given by

$$|M_0| = \left\lfloor \frac{s}{2} \right\rfloor , \text{ with } s = p+1$$

proof: Let $x_1, \ldots, x_s$ be the representatives of the lines in $F_{p^2}$. A function on $M_1$ can be thought as a $s$-tuple

$$(f(x_1), \ldots, f(x_s)) \text{ with } f(x_i) = \pm 1.$$

Condition (1) in 3.6 tells us that the number of 1's in the $s$-tuple is the same as the number of -1's. Thus the number of 1's is $(p+1)/2$.

Observe that every function $f$ is completely determined once we choose the position of the 1's in the $s$-tuple. The remaining positions are then filled by -1's. Therefore, there are $\left\lfloor \frac{s}{2} \right\rfloor$ different ways to construct the $s$-tuple. □.

Remark: Using the same argument as in the last proof, one obtains for arbitrary even $n$
1) For \( n = 2 \) and \( p > 17 \), it is easy to show that

\[
| \text{GL}_2(\mathbb{F}_p) | = (p^2 - 1)(p^2 - p) < \left\lfloor \frac{p^3}{(p+1)/2} \right\rfloor.
\]

Thus, the group \( \text{GL}_2(\mathbb{F}_p) \) does not act transitively for \( p > 17 \).

2) We did numerical computations to find the size of the \( \text{GL}_2(\mathbb{F}_p) \)-orbit of \( \bar{\Psi} \) for \( p = 3, 5, 7, 11, 13 \) and \( 17 \) (see page 50). We obtained

\[
| \text{GL}_2(\mathbb{F}_p) \cdot \bar{\Psi} | < \left\lfloor \frac{p^3}{(p+1)/2} \right\rfloor , \text{ for } p = 7, 11, 13 \text{ and } 17 ,
\]

and

\[
| \text{GL}_2(\mathbb{F}_p) \cdot \bar{\Psi} | = \left\lfloor \frac{p^3}{(p+1)/2} \right\rfloor , \text{ for } p = 3 \text{ and } 5 .
\]

Combining these remarks, we can say:

The group \( \text{GL}_2(\mathbb{F}_p) \) acts transitively on the set of minimals for \( p = 3 \) and \( 5 \), and intransitively for \( p \geq 7 \).

Let \( F = \mathbb{F}_{p^2} \). Then \( F \) has a subfield \( K \) such that \([F:K] = \cdots \)
2 namely, \( K = \mathbb{F}_p^m \). We consider \( F \) as a \( K \)-vector space. Let
\[
\gamma_1, \ldots, \gamma_t
\]
be representatives of the \( K \)-lines through the origin. The number \( t \) of these lines is
\[\tag{3.8} t = \frac{p^m-1}{p^n-1}.\]

Lemma (3.8) : Let \( \chi \) be any additive character on \( F \). Then there exists an element \( \gamma_{i_0} \) in \( \{ \gamma_1, \ldots, \gamma_t \} \) such that:
\[\tag*{\text{proof}}\]
\[\text{i) } |\text{Ker } \chi \cap K.\gamma_{i_0}| = p^m \text{ and }\]
\[\text{ii) } |\text{Ker } \chi \cap K.\gamma_i| = p^{m-1},\]
for all \( 1 \leq i \leq t \) and all \( i \neq i_0 \).

Given a character \( \chi \) of \( (F,+) \), we can find an element c in \( F \) such that
\[\chi(x) = \frac{\text{tr}_F}{\text{tr}_p}(cx) = \frac{\text{tr}_K/\mathbb{F}_p}{\text{tr}_p}(\text{tr}(cx))\]
\[= \text{tr}_K/\mathbb{F}_p(T_c(x)) , \text{ for all } x \in F , \text{ where }\]
\[T_c(x) = \text{Tr}(cx) \quad \text{for } x \in F.\]

Since \( \text{Ker } \text{Tr} \) is a subgroup of \( \text{Ker } \chi \). Thus we have a
coset decomposition for Ker $\chi$:

$$\text{Ker } \chi = \bigcup a + \text{Ker } T_c, \quad (1)$$

where the elements $a$ are in a set $A$ of representatives of cosets.

To show $i)$, we use the fact that Ker $T_c$ consists of a union of $K$-lines. Since $\dim_K(\text{Ker } T_c) = 1$, we conclude

$$\text{Ker } T_c = K \cdot y_{i_0}, \text{ for some } 1 \leq i_0 \leq t.$$ Therefore

$$|\text{Ker } \chi \cap K \cdot y_{i_0}| = |K \cdot y_{i_0}| = |K| = p^m.$$ That shows part $i)$.

To prove the second part, let $i \neq i_0$, then from (1) we get

$$|\text{Ker } \chi \cap K \cdot y_i| = \sum_{a \in A} |(a + \text{Ker } T_c) \cap K \cdot y_i|. \quad (2)$$

We claim that $|(a + \text{Ker } T_c) \cap K \cdot y_i| = 1$ for all $i \neq i_0$.

Fix $a$ in $A$. First suppose $T_c(a) \neq 0$.

Let $x_1, x_2$ be in $(a + \text{Ker } T_c) \cap K \cdot y_i$. Then we have

$$T_c(x_1) = T_c(x_2) = T_c(a).$$ Also, there exist elements $c_1$,
c_2 in K such that x_1 = c_1 y_i, x_2 = c_2 y_i. Combining these facts we get

\[ T_c(y_1) = c_1 T_c(y_1), \text{ and } T_c(y_2) = c_2 T_c(y_1). \]

From this it follows

\[ c_1 T_c(y_1) = c_2 T_c(y_1). \]

Since \( T_c(y_1) \neq 0 \), the last equation implies \( c_1 = c_2 \).

Thus \( x_1 = x_2 \), and that proves that

\[ |(a + \ker T_c) \cap K.y_i| = 1 \]

when \( i \neq i_0 \) and \( a \notin \ker T_c \). Next, suppose \( a \in \ker T_c \). Then

\[ T_c(x_1) = T_c(x_2) = 0. \]

In this case \( x_1 = 0, y_i = x_2 \). So

\[ x_1 = x_2. \]

Hence, \( |(a + \ker T_c) \cap K.y_i| = 1 \) for all \( a \) and all \( i \neq i_0 \).

Going back to equation (2), and using the claim already proved, gives

\[ |\ker \chi \cap K y_i| = |A| = \frac{|\ker \chi|}{|\ker T_c|} = \frac{p^{2m-1}}{p^m} = p^{m-1}, \]

for all \( i \neq i_0 \).
That finishes the proof. 0.

(3.9) Proposition: Let $F = \mathbb{F}_p^{2m}$ and $K = \mathbb{F}_p^m$. Let $K, y_i$ be the $K$-lines of $F$, $i = 1, \ldots, t$. Then every function $f$ on $M_1$ constant on the $K$-lines and satisfying

$$\sum_{i=1}^{t} f(y_i) = 0 \quad (1)$$

is a minimal function.

Proof: We want to prove the minimality conditions 3.1 or , equivalently the two conditions in lemma 3.4.

Let $x_1, \ldots, x_s$ be representatives of the $\mathbb{F}_p$-lines for the field $F$. Then it is clear that (1) implies

$$\sum_{i=1}^{s} f(x_i) = 0$$

which shows a) in 3.4 is true.

Let $\chi \not= \chi_0$ be a character on $F$. Then
\[
\sum_{x_i \in \text{Ker} \chi} f(x_i) = (p-1)^{-1} \sum_{i=1}^{t} f(y_i) | \text{Ker} \chi \cap K \cdot y_i |
\]

\[
= (p-1)^{-1} \left[ f(y_{i_0}) p^m + p^{m-1} \sum_{i \neq i_0} f(y_i) \right]
\]

by lemma 3.8.

By hypothesis we get

\[
\sum_{i \neq i_0} f(y_i) = -f(y_{i_0})
\]

Therefore we have

\[
| \sum_{x_i \in \text{Ker} \chi} f(x_i) | = (p-1)^{-1} | f(y_{i_0}) p^m - f(y_{i_0}) p^{m-1} |
\]

\[
= p^{m-1}. \text{ Therefore } f \text{ is minimal by lemma 3.4 } \square
\]

Define \( P_2(K) = \{ \text{permutations } \sigma : F^* \rightarrow F^* \text{ taking K-lines through the origin in } F \text{ to K-lines through the origin in } F \} \). Then \( P_2(K) \) is a group.

Let \( t \) be the number of K-lines through the origin in \( F \).

Then

\[
t = \frac{p^{2m} - 1}{p^m - 1} = p^m + 1.
\]
and the order of $P_2(F)$ is $t! [ (p^m - 1)!]^t$, since we can permute the $t$ lines at will, and within each line we can permute the $p^m - 1$ non-zero elements at will.

(3.10) Corollary: $P_2(K)$ acts on $M_0$. The $P_2(K)$-orbit of the quadratic function contains $\left\lfloor \frac{t}{2} \right\rfloor$ elements.

Proof: By (3.9), $P_2(K)$ acts on $M_0$. The size of the orbit is given by:

$$|P_2(K)\text{-orbit of } \Phi| = \frac{|P_2(K)|}{|\text{Stab } \Phi|},$$

where the stabilizer of $\Phi$ consists of those maps in $P_2(K)$ taking square lines to square lines and non-square lines to non-square lines. Thus

$$|P_2(K)\text{-orbit of } \Phi| = \frac{t! [ (p^m - 1)!]^t}{(t/2)! (t/2)! [ (p^m - 1)!]^t} = \left\lfloor \frac{t}{2} \right\rfloor.$$

That ends the proof. □

Remark: For $n > 2$, the action of $L$ on $M_0$ is induced by the action from $\text{GL}_n(\mathbb{F}_p)$. For, let $\sigma$ be a collineation on
F. Then by the Fundamental Theorem of Projective Geometry (see Artin Chapter 2, [A]), there exists an invertible linear map $\psi$ such that $\psi(F_p x) = \sigma(F_p x)$, for every $x$ in $F_p^n$.

Let $f$ be a minimal function on $F$. We want to show $f^\sigma = f^\psi$. From (1) it follows that $\sigma = \Theta \cdot \psi$ for some permutation $\Theta$ of $F$ that fixes lines. Since $f$ is constant on the lines any permutation of the elements of each line does not affect the values of $f$. Thus

$$f(\sigma(x)) = f(\Theta(\psi(x))) = f(\psi(x)),$$

for all $x$ in $F$.

Therefore we have $f^\sigma = f^\psi$.

We finish this chapter by solving a conjecture of McGehee which says: for all $n > 1$, $|M_0| > 2$. See [M]

In fact we show: for all $n \geq 1$ we have $|M_0| \geq 2^n$.

We begin with

\textbf{(3.11) Lemma: a)} There is a basis $\{v_1, \ldots, v_n\}$ of $F_p^n$ over
\( \mathbb{F}_p \) with each \( v_i \) square in \( \mathbb{F}_{p^n} \).

b) There is a basis \{ \( w_1, \ldots, w_n \) \} of \( \mathbb{F}_{p^n} \) over \( \mathbb{F}_p \) with each \( w_i \) non square in \( \mathbb{F}_{p^n} \).

**proof:** Consider the span of all squares \( \text{Span}(\mathbb{F}_{p^n}^{\times 2}) \) which is a subspace of \( \mathbb{F}_{p^n} \). Notice that

\[
|\text{Span}(\mathbb{F}_{p^n}^{\times 2})| = \frac{p^n - 1}{2} > p^{n-1}.
\]

Therefore it follows \( \dim \mathbb{F}_p \text{Span}(\mathbb{F}_{p^n}^{\times 2}) = n \). From this we get \( \text{Span}(\mathbb{F}_{p^n}^{\times 2}) = \mathbb{F}_{p^n} \). Then a) is proved. A similar argument works for b). \( \square \)

(3.12) **Corollary:** For all \( n \) and all \( p \mid M_0 \mid \leq 2^n \).

**proof:** Let \( B_1 = \{ v_1, \ldots, v_n \} \) be a basis with \( v_1 \) square in \( \mathbb{F}_{p^n} \) and let \( B_2 = \{ w_1, \ldots, w_n \} \) be another basis with \( w_1 \) non square in \( \mathbb{F}_{p^n} \). Then by Steinitz exchange lemma given any
set $S \subseteq B_1$, with $|S| = s$, there exists a set $T \subseteq B_2$, with $|T| = s$, such that $(B_1 \setminus S) \cup T$ is a basis of $F_{pn}$.

Next consider a $n$-tuple $c = (\varepsilon_1, \ldots, \varepsilon_n)$, where

$\varepsilon_i \in \{1, w_i, v_i^{-1}\}$ and define a $F_p$ linear map

$$\varphi_c : F_q \rightarrow F_q$$

$$v_i \rightarrow \varepsilon_i v_i$$

Then $\varphi_c$ exchange the elements of the basis $B_1$ and $B_2$.

By Steinitz lemma $\varphi_c$ takes a basis into another basis. Thus $\varphi_c$ is a linear invertible map.

If $\Psi$ is the quadratic function, it is clear that $\Psi \varphi_c$ is a minimal function. Also notice that for two different $n$-tuples $c_1 = (\varepsilon_1, \ldots, \varepsilon_n)$ and $c_2 = (\overline{\varepsilon_1}, \ldots, \overline{\varepsilon_n})$ we have $\varepsilon_i \neq \overline{\varepsilon}_i$ for some $i$. Thus

$$\Psi (\varphi_{c_1} (v_i)) = \Psi (\varepsilon_i v_i) = \Psi (\varepsilon_i) \Psi (v_i),$$

and
Since \( \varphi ( \varepsilon_1 ) \neq \varphi ( \bar{\varepsilon}_1 ) \), we conclude \( \varphi \varphi_{c_1} \neq \varphi \varphi_{c_2} \).

Then we have \( 2^n \) minimal functions of the form \( \varphi \varphi_{c} \). That finishes the proof. \( \square \).

**Remark:** The \( 2^n \) pairwise distinct minimal functions constructed above lie in the \( \text{GL}_n(F_p) \)-orbit of the quadratic function \( \varphi \). Thus we have actually showed that

\[
\frac{|\text{GL}_n(F_p)|}{|\text{Stab}(\varphi)|} \leq 2^n.
\]

Hence \( |\text{Stab}(\varphi)| \leq \frac{n}{2^n} \left[ \prod_{i=1}^{n-1} \left( \frac{p^n - p^i}{2} \right) \right] \)

This together with lemma (3.3) gives

\[
\left( \frac{p^{n-1}}{2} \right)_n \leq |\text{Stab}(\varphi)| \leq \prod_{i=1}^{n-1} \left( \frac{p^n - p^i}{2} \right).
\]

And our conjecture (see page 51) is that the left-hand side inequality is actually equality.
APPENDIX

PROGRAM FIELD19

Francisco Rivero  6-11-87.
Running time 6hrs 25 min.

program field19;
    type coord = ARRAY[1..171] of integer;
    var
        r,s,t: coord ;
        is_square : ARRAY[0..342] of boolean ;

    procedure square ;
        (* this procedure find all squares in F(343) *)
        (* x = (I,J,K) is any element in F(343) , with x^2 =
          (r,s,t)*) 
        var
            I,J,K,e,w : integer ;
    begin
        writeln ( '******* list of all squares in F(343) ******* ');
        writeln ;
        e := 0;
        for I := 1 to 3 do
            for J := 1 to 7 do
                for K := 1 to 7 do
                    begin
                        e := e +1 ;
                        r[e] := ( I*I + 3*J*K ) MOD 7 ;
                        s[e] := ( 2*I*J + 5*K*K ) MOD 7 ;
                        t[e] := ( 2*I*K + J*J ) MOD 7 ;
                    end;
        for J := 1 to 3 do
            for K := 1 to 7 do
                begin
                    e := e +1 ;
                    r[e] := ( 3*J*K ) MOD 7 ;
                    s[e] := ( 5*K*K ) MOD 7 ;
                    t[e] := ( J*J ) MOD 7 ;
                end;
        for K := 1 to 3 do
            begin
                e := e +1 ;
                r[e] := 0;
                s[e] := ( 5*K*K ) MOD 7 ;
                t[e] := 0;
            end;
        (* next we generate the set of squares is_square*)
        for I := 0 to 342 do
            is_square[I] := false;
is_square[I] := false;
for I := 1 to 171 do
begin
  w := 49*r[I] + 7*s[I] + t[I];
  is_square[w] := true;
  writeln ( r[I]:6 , s[I]:6 , t[I]:6 , I:10 );
end;
end;

procedure linear_map;
(* Generates all linear, invert maps on F(343) *)
var
  al , a2 , a3 ,
  b1 , b2 , b3 ,
  c1 , c2 , c3 ,
  z1 , z2 , z3 ,
  I , J , K , L , y, det : integer ;
begin
  for I := 1 to 171 do
begin
    writeln (1st.) ;
    a1 := r[I] ;
    a2 := s[I] ;
    a3 := t[I] ;
    for J := 1 to 171 begin
      c1 := r[J] ;
      c2 := s[J] ;
      c3 := t[J] ;
      for K := 1 to 171 do
      begin
        b1 := r[K] ;
        b2 := s[K] ;
        b3 := t[K] ;
        det := ( a1*b2*c3 + c1*a2*b3 + b1*c2*a3
          -a1*c2*b3 - c1*b2*a3 - a2*b1*c3 ) MOD 7;
        if ( det <> 0 ) then begin
          L := 1;
          repeat
            (* z is the value of the map at (r,s,t) *)
            z1 := ( r[L]*a1 + 3*s[L]*b1 + t[L]*c1 ) MOD 7;
            z2 := ( r[L]*a2 + 3*s[L]*b2 + t[L]*c2 ) MOD 7;
            z3 := ( r[L]*a3 + 3*s[L]*b3 + t[L]*c3 ) MOD 7;
            y := 49*z1 + 7*z2 + z3 ;
            L := L + 1 ;
          until ( L > 171 ) or not is_square[y];
          if ( is_square[y] ) then begin
            write (1st , ' ' );
            write (1st , ' a = (' , a1 , ',',a2 , ',',a3);
write (1st, ' b = (' , b1 , ' , ' , b2 , ' , ' , b3 );
write (1st, ' c = (' , c1 , ' , ' , c2 , ' , ' , c3 );
end
end
end
end
end;
9
begin (*field19*0
square ;
 linemap ;
end.
REFERENCES

[ A ] - E. Artin - Geometric Algebra
   Interscience Publishers, Inc
   New York, 1957.

   Harmonic Analysis - Springer Verlag

[ J ] - Nathan Jacobson - Basic Algebra
   W. H. Freeman and Company
   San Francisco, 1974.

[ K ] - G. Karpilovsky - Commutative Group Algebras
   Marcel Dekker, Inc
   New York, 1983.

[ M ] - O.C. McGehee - Gaussian Sums and Harmonic Analysis
   on Finite Fields (To be published), 1987.

[ R ] - P. Ribenboim - Algebraic Numbers
   Wiley-Interscience.
VITA

Francisco Rivero, son of Beatriz Rivero and Jesus Rivero was born in Puerto Plata, Dominican Republic, September 15, 1950. In July 1969 he was graduated from Liceo Agustin Codazzi (High School), Maracay, Venezuela. In 1970 he entered Universidad de Los Andes, Merida, Venezuela, where he obtained a Bachelor's degree in Mathematics. He taught at Universidad de Los Andes from 1977 to 1982. In 1981, while teaching, he completed a M.S. in Mathematics from Universidad de Los Andes. In the spring of 1983 he enrolled at Louisiana State University to pursue a Ph.D. degree in Mathematics. In the fall of 1984 he obtained a M.S. degree in Mathematics at L.S.U.

The author was married to Nancy Perez on July 31, 1977. They have two children Francisco Jose (10) and Paola Stephanie (1).
DOCTORAL EXAMINATION AND DISSERTATION REPORT

Candidate: Francisco Rivero

Major Field: Mathematics

Title of Dissertation: Group Actions on Minimal Functions over Finite Fields

Approved:

[Signatures]

Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

[Signatures]

Date of Examination:

November 20, 1987