

PRIMITIVE ELEMENTS IN FINITE FIELDS WITH ARBITRARY TRACE

by
MUSTAFA ÇOBAN

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science
Sabancı University
Spring 2003

PRIMITIVE ELEMENTS IN FINITE FIELDS WITH ARBITRARY TRACE

APPROVED BY

Assist. Prof. Cem GÜNERİ
(Thesis Supervisor)

Prof. Dr. Alev TOPUZOĞLU

Assist. Prof. Albert LEVİ

DATE OF APPROVAL: August 29th, 2003

©Mustafa Çoban 2003

All Rights Reserved

Anneme, babama
ve
biricik ağabeyime...

Acknowledgments

I would like to express my gratitude and deepest regards to my supervisor Assist. Prof. Cem Güneri for his motivation, guidance and encouragement throughout this thesis.

I also would like to thank Ismail Çoban, Mehmet Özdemir, Mustafa Parlak, and Ayça Çeşmeliöđlu for their friendship and endless support.

PRIMITIVE ELEMENTS IN FINITE FIELDS WITH ARBITRARY TRACE

Abstract

Arithmetic of finite fields is not only important for other branches of mathematics but also widely used in applications such as coding and cryptography. A primitive element of a finite field is of particular interest since it enables one to represent all other elements of the field. Therefore an extensive research has been done on primitive elements, especially those satisfying extra conditions.

We are interested in the existence of primitive elements in extensions of finite fields with prescribed trace value. This existence problem can be settled by means of two important theories. One is character sums and the other is the theory of algebraic function fields. The aim of this thesis is to introduce some important properties of these two topics and to show how they are used in answering the existence problem mentioned above.

Keywords: Finite field, primitive element, trace, character sum, algebraic function field.

SONLU CİSİMLERDE HERHANGİ TRACE DEĞERİNE SAHİP İLKEL ELEMANLAR

Özet

Sonlu cisimlerin aritmetiği matematiğin diğler alanlarındaki önemi dışında kodlama ve şifreleme gibi uygulamalarda da sıkça kullanılır. Cismin tüm diğler elemanlarının gösterilişine imkan verdiğı için sonlu cisimlerin ilkel elemanlarına özellikle ilgi duyulmaktadır. Bu sebepten genelde ilkel elemanlar, özellikle de bazı şartları sağılayan ilkel elemanlar konularında kapsamlı arařtırmalar yapılmaktadır.

Biz, sonlu cisimlerin genişlemelerinde herhangi bir trace değerine sahip ilkel elemanların varlığı problemiyle ilgileneceğiz. Bu varlık problemi iki önemli kuram yoluyla çözülebilir. Bunlardan birincisi karakter toplamları diğeri ise cebirsel fonksiyon cisimleridir. Bu tezin amacı sözü geçen iki önemli kuramın bazı temel özelliklerini açıklamak ve yukarda tanımlanan varlık probleminin cevaplanmasında nasıl kullanıldıklarını göstermektir.

Anahtar kelimeler: Sonlu cisim, ilkel eleman, trace, karakter toplamı, cebirsel fonksiyon cismi.

TABLE OF CONTENTS

Acknowledgments	v
Abstract	vi
Özet	vii
1 INTRODUCTION	1
1.1 Primitive Elements and the Trace Map in Finite Fields	2
1.2 Character Sums	4
1.3 Algebraic Function Fields	6
2 PRIMITIVE ELEMENTS WITH ARBITRARY TRACE USING CHARACTER SUMS	14
2.1 Strategy	14
2.2 Estimate for a Character Sum and Proof of Theorem 2.1.3	16
3 “GENERALIZATION” VIA ALGEBRAIC FUNCTION FIELDS	25
3.1 Artin-Schreier Extensions	25
3.2 Additive Polynomials and Primitive Elements	32
4 CONCLUSION AND FURTHER RESEARCH	37