Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

536

Wolfgang M. Schmidt

Equations over Finite Fields
An Elementary Approach

Springer-Verlag
Berlin · Heidelberg · New York 1976

Author
Wolfgang M. Schmidt
Department of Mathematics
University of Colorado
Boulder, Colo., 80309/USA

Library of Congress Cataloging in Publication Data

Schmidt, Wolfgang M
Equations over finite fields.

(Lecture notes in mathematics ; 536)
Bibliography: p.
1. Diophantine analysis. 2. Modular fields.
I. Title. II. Series: Lecture notes in mathematics (Berlin) ; 536.
QA3.L28 vol.536 [QA242] 510'.8s [512.9'4]
76-26612

AMS Subject Classifications (1970): 10A10, 10B15, 10G05, 12C25, 14G15

ISBN 3-540-07855-X Springer-Verlag Berlin · Heidelberg · New York
ISBN 0-387-07855-X Springer-Verlag New York · Heidelberg · Berlin

Printed in Germany
Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.

Preface

These Lecture Notes were prepared from notes taken by M. Ratliff and K. Spackman of lectures given at the University of Colorado.

I have tried to present a proof as simple as possible of Weil's theorem on curves over finite fields. The notions of "simple" or "elementary" have different interpretations, but I believe that for a reader who is unfamiliar with algebraic geometry, perhaps even with algebraic functions in one variable, the simplest method is the one which originated with Stepanov. Hence it is this method which I follow.

The length of these Notes is perhaps shocking. However, it should be noted that only Chapters I and III deal with Weil's theorem. Furthermore, the style is (I believe) leisurely, and several results are proved in more than one way. I start in Chapter I with the simplest case, i.e., with curves $y^d = f(x)$. At first I do the simplest subcase, i.e., the case when the field is the prime field and when d is coprime to the degree of f . This special case is now so easy that it could be presented to undergraduates. The general equation $f(x,y) = 0$ is taken up only in Chapter III, but a reader in a hurry could start there. The second chapter, on character sums and exponential sums, is included at such an early stage because of the many applications in number theory. Chapters IV, V and VI deal with equations in an arbitrary number of variables.

Possible sequences are chapters

I by itself, or

I, III for Weil's theorem, or

I.1,III for a reader who is in a hurry, or

I, II for character sums and exponential sums, or

I, II, IV, or

I, III, IV.3 and V .

Originally I had planned to include Bombieri's version of the Stepanov method. I did include it in my lectures at the University of Colorado, but I first had to prove the Riemann-Roch Theorem and basic properties of the zeta function of a curve. A proof of these basic properties in the Lecture Notes would have made these unduly long, while their omission would have made the Bombieri version not self complete. Hence I decided after some hesitation to exclude this version from the Notes.

Recently Deligne proved far reaching generalizations of Weil's theorem to non-singular equations in several variables, thereby confirming conjectures of Weil. It is to be noted, however, that Deligne's proof rests on an assertion of Grothendieck concerning a certain fixed point theorem. To the best of my knowledge, a proof of this fixed point theorem has not appeared in print yet. It is perhaps needless to say that at present there is no elementary approach to such a generalization of Weil's theorem. But it is to be hoped that some day such an approach will become available, at least for those cases which are used most often in analytic number theory.

November, 1975 W. M. Schmidt

Notation

F^* is the multiplicative group of a field F .

$\bar{F}$ is the algebraic closure of a field F .

F^n is the product $F \times \ldots \times F$, i.e., the set of n-tuples $(x_1, \ldots, x_n)$ with $x_i \in F$ $(i = 1, \ldots, n)$.

$[F_1 : F_2]$ denotes the degree of a field extension $F_1 \supseteq F_2$.

$\mathfrak{T}$ denotes the trace and $\mathfrak{N}$ the norm.

F_q will denote the finite field with q elements.

p will be the characteristic.

$\mathbb{Q}$ is the field of rational numbers,

$\mathbb{R}$ the field of reals,

$\mathbb{C}$ the field of complex numbers,

$\mathbb{Z}$ the ring of (rational) integers.

$\cong$ denotes isomorphism of fields or groups.

Quite often, $x, y, z \ldots$ will be elements which lie in a ground field or are algebraic over a ground field, $X, Y, Z, \ldots$ will be variables, i.e., will be algebraically independent over a ground field, and $\mathfrak{X}, \mathfrak{Y}, \ldots$ will be algebraic functions, i.e., they will be algebraically dependent on some of $X, Y, \ldots$. Thus $f(X_1, \ldots, X_n)$ is a polynomial, and $f(x_1, \ldots, x_n)$ is the value of this polynomial at $(x_1, \ldots, x_n)$.

$F(x)$ or $F(X)$ or $F(X,Y)$ or $F(X,\mathfrak{Y})$, or similar, will be the field obtained by adjoining x or X or X,Y or $X,\mathfrak{Y}$ to a ground field F . Thus $F(X)$ is the field of rational functions in a variable X with coefficients in F . $R[X]$ denotes the ring of polynomials in X with coefficients in the ring R .

If a,b are in Z, we write $a|b$ (or $a \nmid b$) if a does (or does not) divide b. Occasionally we shall write $d|q-1$ instead of the more proper notation $d|(q-1)$. Again, we shall write $f(X)|g(X)$ if the polynomial $f(X)$ divides $g(X)$. Further $(f(X))$ (or $(f(X),g(X))$) will be the ideal generated by $f(X)$ (or by $f(X)$ and $g(X)$).

$|\omega|$ denotes the number of elements of a finite set ω. Given sets $A \subseteq B$, the set theoretic difference is denoted by $B \sim A$.

Table of Contents