Algebraic Geometry in Coding Theory and Cryptography

HARALD NIEDERREITER
AND
CHAOPING XING

Algebraic Geometry in Coding Theory and Cryptography

HARALD NIEDERREITER
AND CHAOPING XING

PRINCETON UNIVERSITY PRESS
PRINCETON AND OXFORD

Published by Princeton University Press, 41 William Street,
Princeton, New Jersey 08540
In the United Kingdom: Princeton University Press, 6 Oxford Street,
Woodstock, Oxfordshire OX20 1TW

Library of Congress Cataloging-in-Publication Data

Niederreiter, Harald, 1944–
Algebraic geometry in coding theory and cryptography / Harald
Niederreiter and Chaoping Xing.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-691-10288-7 (hardcover : alk. paper)
1. Coding theory. 2. Cryptography. 3. Geometry, Algebraic.
I. Xing, Chaoping, 1963– II. Title.
QA268.N54 2009
003'. 54—dc22 2008056156

British Library Cataloging-in-Publication Data is available

This book has been composed in Times
Printed on acid-free paper. ∞
press.princeton.edu

Typeset by S R Nova Pvt Ltd, Bangalore, India
Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Algebraic Geometry in Coding Theory and Cryptography

For Gerlinde, spirited and indomitable companion on that great trek called life

To my wife Youqun Shi and my children Zhengrong and Menghong

Preface

Algebraic geometry has found fascinating applications to coding theory and cryptography in the last few decades. This book aims to provide the necessary theoretical background for reading the contemporary literature on these applications. An aspect that we emphasize, as it is very useful for the applications, is the interplay between nonsingular projective curves over finite fields and global function fields. This correspondence is well known and frequently employed by researchers, but nevertheless it is difficult to find detailed proofs of the basic facts about this correspondence in the expository literature. One contribution of our book is to fill this gap by giving complete proofs of these results.

We also want to offer the reader a taste of the applications of algebraic geometry, and in particular of algebraic curves over finite fields, to coding theory and cryptography. Several books, among them our earlier book *Rational Points on Curves over Finite Fields: Theory and Applications*, have already treated such applications. Accordingly, besides presenting standard topics such as classical algebraic-geometry codes, we have also selected material that cannot be found in other books, partly because it is of recent origin.

As a reflection of the above aims, the book splits into two parts. The first part, consisting of Chapters 1 to 4, develops the theory of algebraic varieties, of algebraic curves, and of their function fields, with the emphasis gradually shifting to global function fields. The second part consists of Chapters 5 and 6 and describes applications to coding theory and cryptography, respectively. The book is written at the level of advanced undergraduates and first-year graduate students with a good background in algebra.

We are grateful to our former Ph.D. students David Mayor and Ayineedi Venkateswarlu for their help with typesetting and proofreading. We also thank Princeton University Press for the invitation to write this book.

Singapore, November 2007

HARALD NIEDERREITER
CHAOPING XING

Contents

1 Finite Fields and Function Fields

In the first part of this chapter, we describe the basic results on finite fields, which are our ground fields in the later chapters on applications. The second part is devoted to the study of function fields.

Section 1.1 presents some fundamental results on finite fields, such as the existence and uniqueness of finite fields and the fact that the multiplicative group of a finite field is cyclic. The algebraic closure of a finite field and its Galois group are discussed in Section 1.2. In Section 1.3, we study conjugates of an element and roots of irreducible polynomials and determine the number of monic irreducible polynomials of given degree over a finite field. In Section 1.4, we consider traces and norms relative to finite extensions of finite fields.

A function field governs the abstract algebraic aspects of an algebraic curve. Before proceeding to the geometric aspects of algebraic curves in the next chapters, we present the basic facts on function fields. In particular, we concentrate on algebraic function fields of one variable and their extensions including constant field extensions. This material is covered in Sections 1.5, 1.6, and 1.7.

One of the features in this chapter is that we treat finite fields using the Galois action. This is essential because the Galois action plays a key role in the study of algebraic curves over finite fields. For comprehensive treatments of finite fields, we refer to the books by Lidl and Niederreiter [71, 72].

1.1 Structure of Finite Fields

For a prime number p, the residue class ring $\mathbb{Z}/p\mathbb{Z}$ of the ring $\mathbb{Z}$ of integers forms a field. We also denote $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$. It is a prime field in the sense that there are no proper subfields of $\mathbb{F}_p$. There are exactly p elements in $\mathbb{F}_p$. In general, a field is called a *finite field* if it contains only a finite number of elements.

Proposition 1.1.1. Let k be a finite field with q elements. Then:

(i) there exists a prime p such that $\mathbb{F}_p \subseteq k$;
(ii) $q = p^n$ for some integer $n \geq 1$;
(iii) $\alpha^q = \alpha$ for all $\alpha \in k$.

Proof.

(i) Since k has only $q < \infty$ elements, the characteristic of k must be a prime p. Thus, $\mathbb{F}_p$ is the prime subfield of k.

(ii) We consider k as a vector space over $\mathbb{F}_p$. Since k is finite, the dimension $n := \dim_{\mathbb{F}_p}(k)$ is also finite. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of k over $\mathbb{F}_p$. Then each element of k can be uniquely represented in the form $a_1\alpha_1 + \cdots + a_n\alpha_n$ with $a_1, \ldots, a_n \in \mathbb{F}_p$. Thus, $q = p^n$.

(iii) It is trivial that $\alpha^q = \alpha$ if $\alpha = 0$. Assume that α is a nonzero element of k. Since all nonzero elements of k form a multiplicative group k^* of order $q - 1$, we have $\alpha^{q-1} = 1$, and so $\alpha^q = \alpha$. □

Using the above proposition, we can show the most fundamental result concerning the existence and uniqueness of finite fields.

Theorem 1.1.2. For every prime p and every integer $n \geq 1$, there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of the polynomial $x^q - x$ over $\mathbb{F}_p$.

Proof. (Existence) Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$ and let $k \subseteq \overline{\mathbb{F}_p}$ be the splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. Let R be the set of all roots of $x^{p^n} - x$ in k. Then R has exactly p^n elements since the derivative of the polynomial $x^{p^n} - x$ is $p^n x^{p^n-1} - 1 = -1$. It is easy to verify that R contains $\mathbb{F}_p$ and R forms a subfield of $\overline{\mathbb{F}_p}$ (note that $(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$ for any $\alpha, \beta \in \overline{\mathbb{F}_p}$ and any integer $m \geq 1$). Thus, R is exactly the splitting field k, that is, k is a finite field with p^n elements.

(Uniqueness) Let $k \subseteq \overline{\mathbb{F}_p}$ be a finite field with q elements. By Proposition 1.1.1(iii), all elements of k are roots of the polynomial $x^q - x$. Thus, k is the splitting field of the polynomial of $x^q - x$ over $\mathbb{F}_p$. This proves the uniqueness. □

The above theorem shows that for given $q = p^n$, the finite field with q elements is unique in a fixed algebraic closure $\overline{\mathbb{F}_p}$. We denote this finite field by $\mathbb{F}_q$ and call it *the* finite field of order q (or with q elements). It follows from the proof of the above theorem that $\mathbb{F}_q$ is the splitting field of the polynomial $x^q - x$ over $\mathbb{F}_p$, and so $\mathbb{F}_q/\mathbb{F}_p$ is a Galois extension of degree n. The following result yields the structure of the Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Lemma 1.1.3. The Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ with $q = p^n$ is a cyclic group of order n with generator $\sigma : \alpha \mapsto \alpha^p$.

Proof. It is clear that σ is an automorphism in $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Suppose that σ^m is the identity for some $m \geq 1$. Then $\sigma^m(\alpha) = \alpha$, that is, $\alpha^{p^m} - \alpha = 0$, for all $\alpha \in \mathbb{F}_q$. Thus, $x^{p^m} - x$ has at least $q = p^n$ roots. Therefore, $p^m \geq p^n$, that is, $m \geq n$. Hence, the order of σ is equal to n since $|\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = n$. □

Lemma 1.1.4. The field $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if m divides n.

Proof. If m divides n, then there exists a subgroup H of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ with $|H| = n/m$ since $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a cyclic group of order n by Lemma 1.1.3. Let k be the subfield of $\mathbb{F}_{p^n}/\mathbb{F}_p$ fixed by H. Then $[k : \mathbb{F}_p] = m$. Thus, $k = \mathbb{F}_{p^m}$ by the uniqueness of finite fields.

Conversely, let $\mathbb{F}_{p^m}$ be a subfield of $\mathbb{F}_{p^n}$. Then the degree $m = [\mathbb{F}_{p^m} : \mathbb{F}_p]$ divides the degree $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$. □

Theorem 1.1.5. Let q be a prime power. Then:

(i) $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^n}$ for every integer $n \geq 1$.
(ii) $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a cyclic group of order n with generator $\sigma : \alpha \mapsto \alpha^q$.
(iii) $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n}$ if and only if m divides n.

Proof.

(i) Let $q = p^s$ for some prime p and integer $s \geq 1$. Then by Lemma 1.1.4, $\mathbb{F}_q = \mathbb{F}_{p^s} \subseteq \mathbb{F}_{p^{ns}} = \mathbb{F}_{q^n}$.
(ii) Using exactly the same arguments as in the proof of Lemma 1.1.3 but replacing p by q, we obtain the proof of (ii).
(iii) By Lemma 1.1.4, $\mathbb{F}_{q^m} = \mathbb{F}_{p^{ms}}$ is a subfield of $\mathbb{F}_{q^n} = \mathbb{F}_{p^{ns}}$ if and only if ms divides ns. This is equivalent to m dividing n. □

We end this section by determining the structure of the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of a finite field $\mathbb{F}_q$.

Proposition 1.1.6. The multiplicative group $\mathbb{F}_q^*$ is cyclic.

Proof. Let $t \leq q-1$ be the largest order of an element of the group $\mathbb{F}_q^*$. By the structure theorem for finite abelian groups, the order of any element of $\mathbb{F}_q^*$ divides t. It follows that every element of $\mathbb{F}_q^*$ is a root of the polynomial $x^t - 1$, hence, $t \geq q-1$, and so $t = q-1$. □

Definition 1.1.7. A generator of the cyclic group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

Let γ be a generator of $\mathbb{F}_q^*$. Then γ^n is also a generator of $\mathbb{F}_q^*$ if and only if $\gcd(n, q-1) = 1$. Thus, we have the following result.

Corollary 1.1.8. There are exactly $\phi(q-1)$ primitive elements of $\mathbb{F}_q$, where ϕ is the Euler totient function.

1.2 Algebraic Closure of Finite Fields

Let p be the characteristic of $\mathbb{F}_q$. It is clear that the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$ is the same as $\overline{\mathbb{F}_p}$.

Theorem 1.2.1. The algebraic closure of $\mathbb{F}_q$ is the union $\cup_{n=1}^{\infty} \mathbb{F}_{q^n}$.

Proof. Put $U := \cup_{n=1}^{\infty} \mathbb{F}_{q^n}$. It is clear that U is a subset of $\overline{\mathbb{F}_q}$ since $\mathbb{F}_{q^n}$ is a subset of $\overline{\mathbb{F}_p}$. It is also easy to verify that U forms a field.

Let $f(x) = \sum_{i=0}^{s} \lambda_i x^i$ be a nonconstant polynomial over U. Then for $0 \leq i \leq s$ we have $\lambda_i \in \mathbb{F}_{q^{m_i}}$ for some $m_i \geq 1$. Hence, by Theorem 1.1.5(iii), $f(x)$ is a polynomial over $\mathbb{F}_{q^m}$, where $m = \prod_{i=0}^{s} m_i$. Let α be a root of $f(x)$. Then $\mathbb{F}_{q^m}(\alpha)$ is an algebraic extension of $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^m}(\alpha)$ is a finite-dimensional vector space over $\mathbb{F}_{q^m}$. Hence, $\mathbb{F}_{q^m}(\alpha)$ is also a finite field containing $\mathbb{F}_q$. Let r be the degree of $\mathbb{F}_{q^m}(\alpha)$ over $\mathbb{F}_{q^m}$. Then $\mathbb{F}_{q^m}(\alpha)$ contains exactly q^{rm} elements, that is, $\mathbb{F}_{q^m}(\alpha) = \mathbb{F}_{q^{rm}}$. So α is an element of U. This shows that U is the algebraic closure $\overline{\mathbb{F}_q}$. □

We are going to devote the rest of this section to the study of the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. We start from the definition of the inverse limit for finite groups. For a detailed discussion of inverse limits of groups, we refer to the book by Wilson [130].

A *directed set* is a nonempty partially ordered set I such that for all $i_1, i_2 \in I$, there is an element $j \in I$ for which $i_1 \leq j$ and $i_2 \leq j$.

Definition 1.2.2. An *inverse system* $\{G_i, \varphi_{ij}\}$ of finite groups indexed by a directed set I consists of a family $\{G_i : i \in I\}$ of finite groups and a family $\{\varphi_{ij} \in \mathrm{Hom}(G_j, G_i) : i, j \in I,\ i \leq j\}$ of maps such that φ_{ii} is the identity on G_i for each i and $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$ whenever $i \leq j \leq k$. Here, $\mathrm{Hom}(G_j, G_i)$ denotes the set of group homomorphisms from G_j to G_i.

For an inverse system $\{G_i, \varphi_{ij}\}$ of finite groups indexed by a directed set I, we form the Cartesian product $\prod_{i \in I} G_i$, viewed as a product group. We consider the subset of $\prod_{i \in I} G_i$ given by

$$D := \left\{ (x_i) \in \prod_{i \in I} G_i : \varphi_{ij}(x_j) = x_i \quad \text{for all } i, j \in I \quad \text{with } i \leq j \right\}.$$

It is easy to check that D forms a subgroup of $\prod_{i \in I} G_i$. We call D the *inverse limit* of $\{G_i, \varphi_{ij}\}$, denoted by $\lim_{\leftarrow} G_i$.

Example 1.2.3. Define a partial order in the set $\mathbb{N}$ of positive integers as follows: for $m, n \in \mathbb{N}$, let $m \leq n$ if and only if m divides n. For each positive integer i, let G_i be the cyclic group $\mathbb{Z}/i\mathbb{Z}$, and for each pair $(i, j) \in \mathbb{N}^2$ with $i \mid j$, define $\varphi_{ij} : \overline{n} \in G_j \mapsto \overline{n} \in G_i$, with the bar indicating the formation of a residue class. Then it is easy to verify that the family $\{\mathbb{Z}/i\mathbb{Z}, \varphi_{ij}\}$ forms an inverse system of finite groups indexed by $\mathbb{N}$. The inverse limit $\lim_{\leftarrow} \mathbb{Z}/i\mathbb{Z}$ is denoted by $\hat{\mathbb{Z}}$.

Example 1.2.4. Now let $\mathbb{F}_q$ be the finite field with q elements. We consider the family of Galois groups $G_i := \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ of $\mathbb{F}_{q^i}$ over $\mathbb{F}_q$ for each $i \in \mathbb{N}$. We define a partial order in $\mathbb{N}$ as in Example 1.2.3. For each pair $(i, j) \in \mathbb{N}^2$ with $i \mid j$, define the homomorphism φ_{ij}: $\sigma_j \in \mathrm{Gal}(\mathbb{F}_{q^j}/\mathbb{F}_q) \mapsto \sigma_j|_{\mathbb{F}_{q^i}} \in \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$, where $\sigma_j|_{\mathbb{F}_{q^i}}$ stands for the restriction of σ_j to $\mathbb{F}_{q^i}$. Then $\{\mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q), \varphi_{ij}\}$ forms an inverse system of finite groups indexed by $\mathbb{N}$.

Theorem 1.2.5. We have

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \simeq \lim_{\leftarrow} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q).$$

Proof. For each $i \in \mathbb{N}$, we have a homomorphism $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ obtained by restriction. These together yield a homomorphism

$$\theta : \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \prod_{i\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q).$$

It is clear that the image of θ is contained in $\varprojlim \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$. We show in the following that θ is an isomorphism onto $\varprojlim \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$.

If $\sigma \neq 1$ is in $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, then there exists an element $x \in \overline{\mathbb{F}_q}$ such that $\sigma(x) \neq x$. By Theorem 1.2.1, x belongs to $\mathbb{F}_{q^n}$ for some $n \in \mathbb{N}$. Now the image of σ in $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ maps x to $\sigma(x)$, and thus $\theta(\sigma)$ is not the identity. Hence, θ is injective.

Take (σ_i) in $\varprojlim \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$. If $x \in \overline{\mathbb{F}_q}$ and we set $\sigma(x) = \sigma_i(x)$, where $x \in \mathbb{F}_{q^i}$, then this is an unambiguous definition of a map $\sigma : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$. It is easy to check that σ is an element of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Since $\theta(\sigma) = (\sigma_i)$, $\varprojlim \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ is the image of θ. □

Corollary 1.2.6. We have

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \simeq \hat{\mathbb{Z}}.$$

Proof. For each $i \in \mathbb{N}$, we can identify the group $\mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ with $\mathbb{Z}/i\mathbb{Z}$ by Theorem 1.1.5(ii). Under this identification, the family of homomorphisms in Example 1.2.4 coincides with that in Example 1.2.3. Thus, the desired result follows from Theorem 1.2.5. □

It is another direct consequence of Theorem 1.2.5 that the restrictions of all automorphisms in $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ to $\mathbb{F}_{q^m}$ give all automorphisms in $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, that is, we obtain the following result.

Corollary 1.2.7. For every integer $m \geq 1$, we have

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \{\sigma|_{\mathbb{F}_{q^m}} : \sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)\}.$$

For each $i \in \mathbb{N}$, let $\pi_i \in \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$ be the automorphism $\pi_i : x \mapsto x^q$. Then the element (π_i) is in $\varprojlim \mathrm{Gal}(\mathbb{F}_{q^i}/\mathbb{F}_q)$. This yields an automorphism in $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. We call it the *Frobenius (automorphism)* of $\overline{\mathbb{F}_q}/\mathbb{F}_q$, denoted by π. It is clear that $\pi(x) = x^q$ for all $x \in \overline{\mathbb{F}_q}$ and that the restriction of π to $\mathbb{F}_{q^i}$ is π_i, the *Frobenius (automorphism)* of $\mathbb{F}_{q^i}/\mathbb{F}_q$.

1.3 Irreducible Polynomials

Let $\alpha \in \overline{\mathbb{F}_q}$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. The element $\sigma(\alpha)$ is called a *conjugate* of α with respect to $\mathbb{F}_q$.

Lemma 1.3.1. The set of conjugates of an element $\alpha \in \overline{\mathbb{F}_q}$ with respect to $\mathbb{F}_q$ is equal to $\{\pi^i(\alpha) : i = 0, 1, 2, \ldots\}$, where $\pi \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is the Frobenius automorphism.

Proof. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. There exists an integer $m \geq 1$ such that α is an element of $\mathbb{F}_{q^m}$. Then the restrictions $\sigma|_{\mathbb{F}_{q^m}}$ and $\pi|_{\mathbb{F}_{q^m}}$ are both elements of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Moreover, $\pi|_{\mathbb{F}_{q^m}}$ is a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Thus, $\sigma|_{\mathbb{F}_{q^m}} = (\pi|_{\mathbb{F}_{q^m}})^i$ for some $i \geq 0$. Hence, $\sigma(\alpha) = \sigma|_{\mathbb{F}_{q^m}}(\alpha) = (\pi|_{\mathbb{F}_{q^m}})^i(\alpha) = \pi^i(\alpha)$. □

Proposition 1.3.2. All distinct conjugates of an element $\alpha \in \overline{\mathbb{F}_q}$ with respect to $\mathbb{F}_q$ are $\alpha, \pi(\alpha), \ldots, \pi^{m-1}(\alpha)$, where m is the least positive integer such that $\mathbb{F}_{q^m}$ contains α, that is, m is such that $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$.

Proof. The restriction $\pi|_{\mathbb{F}_{q^m}}$ of π to $\mathbb{F}_{q^m}$ has order m since it is a generator of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Hence, $\pi^m(\alpha) = (\pi|_{\mathbb{F}_{q^m}})^m(\alpha) = \alpha$. This implies that $\alpha, \pi(\alpha), \ldots, \pi^{m-1}(\alpha)$ yield all conjugates of α. It remains to show that they are pairwise distinct. Suppose that $\pi^n(\alpha) = \alpha$ for some $n \geq 1$. Then it is clear that $\pi^n(\beta) = \beta$ for all $\beta \in \mathbb{F}_q(\alpha)$, that is, $\beta^{q^n} - \beta = 0$ for all elements $\beta \in \mathbb{F}_{q^m}$. Thus, the polynomial $x^{q^n} - x$ has at least q^m roots. Hence, $n \geq m$. This implies that $\alpha, \pi(\alpha), \ldots, \pi^{m-1}(\alpha)$ are pairwise distinct. □

Corollary 1.3.3. All distinct conjugates of an element $\alpha \in \overline{\mathbb{F}_q}$ with respect to $\mathbb{F}_q$ are $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$, where m is the least positive integer such that $\mathbb{F}_{q^m}$ contains α, that is, m is such that $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$.

Proof. This follows from Proposition 1.3.2 and the fact that $\pi(\alpha) = \alpha^q$. □

By field theory, all conjugates of α with respect to $\mathbb{F}_q$ form the set of all roots of the minimal polynomial of α over $\mathbb{F}_q$. Hence, we get the following result.

Corollary 1.3.4. Let f be an irreducible polynomial over $\mathbb{F}_q$ of degree m and let $\alpha \in \overline{\mathbb{F}_q}$ be a root of f. Then $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are all distinct roots of f, and moreover $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$.

From the above result we obtain that all roots of an irreducible polynomial f over $\mathbb{F}_q$ are simple and that $\mathbb{F}_{q^m}$ is the splitting field of f over $\mathbb{F}_q$, where $m = \deg(f)$.

Lemma 1.3.5. A monic irreducible polynomial $f(x)$ of degree m over $\mathbb{F}_q$ divides $x^{q^n} - x$ if and only if m divides n.

Proof. Let $\alpha \in \overline{\mathbb{F}_q}$ be a root of $f(x)$. Then we have $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$ by Corollary 1.3.4. If m divides n, then $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n}$ by Theorem 1.1.5(iii). From Proposition 1.1.1(iii) we get $\beta^{q^n} - \beta = 0$ for all $\beta \in \mathbb{F}_{q^n}$. In particular, $\alpha^{q^n} - \alpha = 0$. Hence, the minimal polynomial $f(x)$ of α over $\mathbb{F}_q$ divides $x^{q^n} - x$.

If $f(x)$ divides $x^{q^n} - x$, then $\alpha^{q^n} - \alpha = 0$. Hence, $\alpha \in \mathbb{F}_{q^n}$ by the existence part of the proof of Theorem 1.1.2. Now $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$ and our desired result follows from Theorem 1.1.5(iii). □

Since $x^{q^n} - x$ has no multiple roots, we know from Lemma 1.3.5 that the product of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n is equal to $x^{q^n} - x$. From this we obtain the number of monic irreducible polynomials over $\mathbb{F}_q$ of given degree, as stated in the following theorem.

Theorem 1.3.6. Let $I_q(n)$ be the number of monic irreducible polynomials over $\mathbb{F}_q$ of fixed degree $n \geq 1$. Then

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},$$

where the sum is over all positive integers d dividing n and μ is the Möbius function on $\mathbb{N}$ defined by

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1, \\ (-1)^r & \text{if } d \text{ is the product of } r \text{ distinct primes}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Since the product of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n is equal to $x^{q^n} - x$, we obtain the identity

$$q^n = \sum_{d|n} d I_q(d)$$

by comparing degrees. Applying the Möbius inversion formula (e.g., see [72, p. 92]), we get the desired result. □

1.4 Trace and Norm

In this section, we discuss two maps from the field $\mathbb{F}_{q^m}$ to the field $\mathbb{F}_q$: trace and norm.

Definition 1.4.1. The *trace* map $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ is defined to be

$$\sum_{\sigma \in G} \sigma,$$

where $G := \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, that is, for any $\alpha \in \mathbb{F}_{q^m}$, we put

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha).$$

If there is no confusion, we simply denote the map by Tr.

For any $\tau \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $\alpha \in \mathbb{F}_{q^m}$, we have

$$\tau(\mathrm{Tr}(\alpha)) = \tau\left(\sum_{\sigma \in G} \sigma(\alpha)\right) = \sum_{\sigma \in G} (\tau\sigma)(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) = \mathrm{Tr}(\alpha).$$

Thus indeed, Tr is a map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Furthermore, the trace map has the following properties.

Proposition 1.4.2.

(i) $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$ for all $\alpha, \beta \in \mathbb{F}_{q^m}$.
(ii) $\mathrm{Tr}(a\alpha) = a\mathrm{Tr}(\alpha)$ for all $\alpha \in \mathbb{F}_{q^m}$ and $a \in \mathbb{F}_q$.