J.-P. Serre

A Course in Arithmetic

Springer

Jean-Pierre Serre
Collège de France
75231 Paris Cedex 05
France

Mathematics Subject Classification: 11-01

Title of the French original edition: *Cours d'Arithmétique.*
Publisher: Presses Universitaires de France, Paris, 1970–1977.

Library of Congress Cataloging in Publication Data
Serre, Jean-Pierre.
A course in arithmetic by J.-P. Serre. New York,
Springer-Verlag 1973

viii, 115 p. illus. 25 cm. (Graduate texts in mathematics, 7)
Translation of Cours d'arithmétique.
Bibliography: p. 112–113.

1. Forms, Quadratic. 2. Analytic functions.
I. Title. II. Series.
QA243.S4713 512.9'44 70-190089
ISBN 0-387-90040-3; 0-387-90041-1
(pok.) MARC

Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 (Corrected fifth printing, 1996)

ISBN 0-387-90040-3 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-90040-3 Springer-Verlag Berlin Heidelberg New York SPIN 10549048

Preface

This book is divided into two parts.

The first one is purely algebraic. Its objective is the classification of quadratic forms over the field of rational numbers (Hasse-Minkowski theorem). It is achieved in Chapter IV. The first three chapters contain some preliminaries: quadratic reciprocity law, p-adic fields, Hilbert symbols. Chapter V applies the preceding results to integral quadratic forms of discriminant ± 1. These forms occur in various questions: modular functions, differential topology, finite groups.

The second part (Chapters VI and VII) uses "analytic" methods (holomorphic functions). Chapter VI gives the proof of the "theorem on arithmetic progressions" due to Dirichlet; this theorem is used at a critical point in the first part (Chapter III, no. 2.2). Chapter VII deals with modular forms, and in particular, with theta functions. Some of the quadratic forms of Chapter V reappear here.

The two parts correspond to lectures given in 1962 and 1964 to second year students at the Ecole Normale Supérieure. A redaction of these lectures in the form of duplicated notes, was made by J.-J. Sansuc (Chapters I–IV) and J.-P. Ramis and G. Ruget (Chapters VI–VII). They were very useful to me; I extend here my gratitude to their authors.

J.-P. Serre

Table of Contents

A Course in Arithmetic

Part I

Algebraic Methods

Chapter I

Finite Fields

All fields considered below are supposed commutative.

§1. *Generalities*

1.1. *Finite fields*

Let K be a field. The image of $\mathbf{Z}$ in K is an integral domain, hence isomorphic to $\mathbf{Z}$ or to $\mathbf{Z}/p\mathbf{Z}$, where p is prime; its field of fractions is isomorphic to $\mathbf{Q}$ or to $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$. In the first case, one says that K is of *characteristic zero*; in the second case, that K is of *characteristic p*.

The characteristic of K is denoted by $\mathrm{char}(K)$. If $\mathrm{char}(K) = p \neq 0$, p is also the smallest integer $n>0$ such that $n.1 = 0$.

Lemma.—*If* $\mathrm{char}(K) = p$, *the map* $\sigma\colon x \mapsto x^p$ *is an isomorphism of* K *onto one of its subfields* K^p.

We have $\sigma(xy) = \sigma(x)\sigma(y)$. Moreover, the binomial coefficient $\binom{p}{k}$ is congruent to 0 (mod p) if $0<k<p$. From this it follows that

$$\sigma(x+y) = \sigma(x)+\sigma(y);$$

hence σ is a homomorphism. Furthermore, σ is clearly injective.

Theorem 1.—i) *The characteristic of a finite field K is a prime number $p \neq 0$; if $f = [K:\mathbf{F}_p]$, the number of elements of K is $q = p^f$.*

ii) *Let p be a prime number and let $q = p^f (f \geqq 1)$ be a power of p. Let Ω be an algebraically closed field of characteristic p. There exists a unique subfield $\mathbf{F}_q$ of Ω which has q elements. It is the set of roots of the polynomial $X^q - X$.*

iii) *All finite fields with $q = p^f$ elements are isomorphic to $\mathbf{F}_q$.*

If K is finite, it does not contain the field $\mathbf{Q}$. Hence its characteristic is a prime number p. If f is the degree of the extension $K/\mathbf{F}_p$, it is clear that $\mathrm{Card}(K) = p^f$, and i) follows.

On the other hand, if Ω is algebraically closed of characteristic p, the above lemma shows that the map $x \mapsto x^q$ (where $q = p^f$, $f \geqq 1$) is an automorphism of Ω; indeed, this map is the $f-$th iterate of the automorphism $\sigma\colon x \mapsto x^p$ (note that σ is surjective since Ω is algebraically closed). Therefore, the elements $x \in \Omega$ invariant by $x \mapsto x^q$ form a subfield $\mathbf{F}_q$ of Ω. The derivative of the polynomial $X^q - X$ is

$$qX^{q-1} - 1 = p.p^{f-1}X^{q-1} - 1 = -1$$

and is not zero. This implies (since Ω is algebraically closed) that $X^q - X$ has q distinct roots, hence $\mathrm{Card}(\mathbf{F}_q) = q$. Conversely, if K is a subfield of Ω with q elements, the multiplicative group K^* of nonzero elements in K has $q-1$ elements. Then $x^{q-1} = 1$ if $x \in K^*$ and $x^q = x$ if $x \in K$. This proves that K is contained in $\mathbf{F}_q$. Since $\mathrm{Card}(K) = \mathrm{Card}(\mathbf{F}_q)$ we have $K = \mathbf{F}_q$ which completes the proof of ii).

Assertion iii) follows from ii) and from the fact that all fields with p^f elements can be embedded in Ω since Ω is algebraically closed.

1.2. *The multiplicative group of a finite field*

Let p be a prime number, let f be an integer $\geqq 1$, and let $q = p^f$.

Theorem 2.—*The multiplicative group $\mathbf{F}_q^*$ of a finite field $\mathbf{F}_q$ is cyclic of order $q-1$.*

Proof. If d is an integer $\geqq 1$, recall that $\phi(d)$ denotes the *Euler ϕ-function*, i.e. the number of integers x with $1 \leqq x \leqq d$ which are prime to d (in other words, whose image in $\mathbf{Z}/d\mathbf{Z}$ is a generator of this group). It is clear that the number of generators of a cyclic group of order d is $\phi(d)$.

Lemma 1.—*If n is an integer $\geqq 1$, then $n = \sum_{d|n} \phi(d)$.* (Recall that the notation $d|n$ means that d divides n).

If d divides n, let C_d be the unique subgroup of $\mathbf{Z}/n\mathbf{Z}$ of order d, and let Φ_d be the set of generators of C_d. Since all elements of $\mathbf{Z}/n\mathbf{Z}$ generate one of the C_d, the group $\mathbf{Z}/n\mathbf{Z}$ is the disjoint union of the Φ_d and we have

$$n = \mathrm{Card}(\mathbf{Z}/n\mathbf{Z}) = \sum_{d|n} \mathrm{Card}(\Phi_d) = \sum_{d|n} \phi(d).$$

Lemma 2.—*Let H be a finite group of order n. Suppose that, for all divisors d of n, the set of $x \in H$ such that $x^d = 1$ has at most d elements. Then H is cyclic.*

Let d be a divisor of n. If there exists $x \in H$ of order d, the subgroup $(x) = \{1, x, \ldots, x^{d-1}\}$ generated by x is cyclic of order d; in view of the hypothesis, all elements $y \in H$ such that $y^d = 1$ belong to (x). In particular, all elements of H of order d are generators of (x) and these are in number $\phi(d)$. Hence, the number of elements of H of order d is 0 or $\phi(d)$. If it were zero for a value of d, the formula $n = \sum_{d|n} \phi(d)$ would show that the number of elements in H is $<n$, contrary to hypothesis. In particular, there exists an element $x \in H$ of order n and H coincides with the cyclic group (x).

Theorem 2 follows from lemma 2 applied to $H = \mathbf{F}_q^*$ and $n = q-1$; it is indeed obvious that the equation $x^d = 1$, which has degree d, has at most d solutions in $\mathbf{F}_q$.

Remark. The above proof shows more generally that all finite subgroups of the multiplicative group of a field are cyclic.