

Graduate Texts in Mathematics 7

Editorial Board

S. Axler F.W. Gehring K.A. Ribet

Graduate Texts in Mathematics

- 1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
- 2 OXTOBY. Measure and Category. 2nd ed.
- 3 SCHAEFER. Topological Vector Spaces. 2nd ed.
- 4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
- 5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
- 6 HUGHES/PIPER. Projective Planes.
- 7 SERRE. A Course in Arithmetic.
- 8 TAKEUTI/ZARING. Axiomatic Set Theory.
- 9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
- 10 COHEN. A Course in Simple Homotopy Theory.
- 11 CONWAY. Functions of One Complex Variable I. 2nd ed.
- 12 BEALS. Advanced Mathematical Analysis.
- 13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
- 14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
- 15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
- 16 WINTER. The Structure of Fields.
- 17 ROSENBLATT. Random Processes. 2nd ed.
- 18 HALMOS. Measure Theory.
- 19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
- 20 HUSEMOLLER. Fibre Bundles. 3rd ed.
- 21 HUMPHREYS. Linear Algebraic Groups.
- 22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
- 23 GREUB. Linear Algebra. 4th ed.
- 24 HOLMES. Geometric Functional Analysis and Its Applications.
- 25 HEWITT/STROMBERG. Real and Abstract Analysis.
- 26 MANES. Algebraic Theories.
- 27 KELLEY. General Topology.
- 28 ZARISKI/SAMUEL. Commutative Algebra. Vol. I.
- 29 ZARISKI/SAMUEL. Commutative Algebra. Vol. II.
- 30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
- 31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
- 32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
- 33 HIRSCH. Differential Topology.
- 34 SPITZER. Principles of Random Walk. 2nd ed.
- 35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
- 36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
- 37 MONK. Mathematical Logic.
- 38 GRAUERT/FRITZSCHE. Several Complex Variables.
- 39 ARVESON. An Invitation to C^* -Algebras.
- 40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
- 41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
- 42 SERRE. Linear Representations of Finite Groups.
- 43 GILLMAN/JERISON. Rings of Continuous Functions.
- 44 KENDIG. Elementary Algebraic Geometry.
- 45 LOËVE. Probability Theory I. 4th ed.
- 46 LOEVE. Probability Theory II. 4th ed.
- 47 MOISE. Geometric Topology in Dimensions 2 and 3.
- 48 SACHS/WU. General Relativity for Mathematicians.
- 49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
- 50 EDWARDS. Fermat's Last Theorem.
- 51 KLINGENBERG. A Course in Differential Geometry.
- 52 HARTSHORNE. Algebraic Geometry.
- 53 MANIN. A Course in Mathematical Logic.
- 54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
- 55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
- 56 MASSEY. Algebraic Topology: An Introduction.
- 57 CROWELL/FOX. Introduction to Knot Theory.
- 58 KOBLITZ. p -adic Numbers, p -adic Analysis, and Zeta-Functions. 2nd ed.
- 59 LANG. Cyclotomic Fields.
- 60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
- 61 WHITEHEAD. Elements of Homotopy Theory.
- 62 KARGAPOLOV/MERLZIAKOV. Fundamentals of the Theory of Groups.
- 63 BOLLOBAS. Graph Theory.
- 64 EDWARDS. Fourier Series. Vol. I 2nd ed.
- 65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.
- 66 WATERHOUSE. Introduction to Affine Group Schemes.
- 67 SERRE. Local Fields.
- 68 WEIDMANN. Linear Operators in Hilbert Spaces.
- 69 LANG. Cyclotomic Fields II.

(continued after index)

J.-P. Serre

A Course in Arithmetic



Springer

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

Editorial Board

S. Axler
Mathematics Department
San Francisco State
University
San Francisco, CA 94132
USA

F.W. Gehring
Mathematics Department
East Hall
University of Michigan
Ann Arbor, MI 48109
USA

K.A. Ribet
Department of Mathematics
University of California
at Berkeley
Berkeley, CA 94720-3840
USA

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 978-0-387-90041-4 ISBN 978-1-4684-9884-4 (eBook)

DOI 10.1007/978-1-4684-9884-4

(pok.) MARC

Printed on acid-free paper.

© 1973 Springer Science+Business Media New York

Originally published by Springer-Verlag New York Inc. in 1973

Softcover reprint of the hardcover 1st edition 1973

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher Springer Science+Business Media, LLC, except for brief excerpts in connection with reviews or scholarly analysis.

Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Printed and bound by R. R. Donnelley and Sons, Harrisonburg, VA

9 8 7 6

ISBN 978-0-387-90041-4

SPIN 10783650

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

Preface	v
---------	---

Part I—Algebraic Methods

<i>Chapter I</i> —Finite fields	3
1—Generalities	3
2—Equations over a finite field	5
3—Quadratic reciprocity law	6
<i>Appendix</i> —Another proof of the quadratic reciprocity law	9
<i>Chapter II</i> — p -adic fields	11
1—The ring \mathbb{Z}_p and the field \mathbb{Q}_p	11
2— p -adic equations	13
3—The multiplicative group of \mathbb{Q}_p	15
<i>Chapter III</i> —Hilbert symbol	19
1—Local properties	19
2—Global properties	23
<i>Chapter IV</i> —Quadratic forms over \mathbb{Q}_p and over \mathbb{Q}	27
1—Quadratic forms	27
2—Quadratic forms over \mathbb{Q}_p	35
3—Quadratic forms over \mathbb{Q}	41
<i>Appendix</i> —Sums of three squares	45
<i>Chapter V</i> —Integral quadratic forms with discriminant ± 1	48
1—Preliminaries	48
2—Statement of results	52
3—Proofs	55

Part II—Analytic Methods

<i>Chapter VI</i> —The theorem on arithmetic progressions	61
1—Characters of finite abelian groups	61
2—Dirichlet series	64
3—Zeta function and L functions	68
4—Density and Dirichlet theorem	73
<i>Chapter VII</i> —Modular forms	77
1—The modular group	77
2—Modular functions	79
3—The space of modular forms	84
4—Expansions at infinity	90
5—Hecke operators	98
6—Theta functions	106

Bibliography	112
Index of Definitions	114
Index of Notations	115

A Course in Arithmetic