Graduate Texts in Mathematics 121

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFFER. Topological Vector Spaces.
4 HILTON/STAMMBACH. A Course in Homological Algebra.
5 MAC LANE. Categories for the Working Mathematician.
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. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules.
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., revised.
20 HUSEMOLLER. Fibre Bundles. 2nd 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 WERMER. Banach Algebras and Several Complex Variables. 2nd 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 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.

Serge Lang

Cyclotomic Fields I and II

Combined Second Edition

With an Appendix by Karl Rubin

Springer Science+Business Media, LLC

Serge Lang
Department of Mathematics
Yale University
New Haven, CT 06520
U.S.A.

Mathematical Subject Classifications (1980): 12A35, 12B30, 12C20, 14G20

Library of Congress Cataloging-in-Publication Data
Lang, Serge, 1927-
Cyclotomic fields I and II (Combined Second Edition)/Serge Lang
p. cm. -- (Graduate texts in mathematics; 121)
Bibliography: p.
Includes index.
ISBN 0-387-96671-4

1. Fields, Algebraic. 2. Cyclotomy. I. Title. II. Series
QA247.L33 1990
512'.3--dc19 87-35616

This book is a combined edition of the books previously published as *Cyclotomic Fields* and *Cyclotomic Fields II*, by Springer Science+Business Media, LLC, in 1978 and 1980, respectively. It contains an additional appendix by Karl Rubin.

9 8 7 6 5 4 3 2 1

ISBN 978-1-4612-6972-4 ISBN 978-1-4612-0987-4 (eBook)
DOI 10.1007/978-1-4612-0987-4

Contents

APPENDIX BY KARL RUBIN

Notation

$\mathbf{Z}(N)$ = integers mod $N = \mathbf{Z}/N\mathbf{Z}$.

If A is an abelian group, we usually denoted by A_N the elements $x \in A$ such that $Nx = 0$. Thus for a prime p, we denote by A_p the elements of order p. However, we also use p in this position for indexing purposes, so we rely to some extent on the context to make the intent clear. In his book, Shimura uses $A[p]$ for the kernel of p, and more generally, if A is a module over a ring, uses $A[\mathfrak{a}]$ for the kernel of an ideal $\mathfrak{a}$ in A. The brackets are used also in other contexts, like operators, as in Lubin–Tate theory. There is a dearth of symbols and positions, so some duplication is hard to avoid.

We let $A(N) = A/NA$. We let $A^{(p)}$ be the subgroup of A consisting of all elements annihilated by a power of p.

Introduction

Kummer's work on cyclotomic fields paved the way for the development of algebraic number theory in general by Dedekind, Weber, Hensel, Hilbert, Takagi, Artin and others. However, the success of this general theory has tended to obscure special facts proved by Kummer about cyclotomic fields which lie deeper than the general theory. For a long period in the 20th century this aspect of Kummer's work seems to have been largely forgotten, except for a few papers, among which are those by Pollaczek [Po], Artin–Hasse [A–H] and Vandiver [Va].

In the mid 1950's, the theory of cyclotomic fields was taken up again by Iwasawa and Leopoldt. Iwasawa viewed cyclotomic fields as being analogues for number fields of the constant field extensions of algebraic geometry, and wrote a great sequence of papers investigating towers of cyclotomic fields, and more generally, Galois extensions of number fields whose Galois group is isomorphic to the additive group of p-adic integers. Leopoldt concentrated on a fixed cyclotomic field, and established various p-adic analogues of the classical complex analytic class number formulas. In particular, this led him to introduce, with Kubota, p-adic analogues of the complex L-functions attached to cyclotomic extensions of the rationals. Finally, in the late 1960's, Iwasawa [Iw 11] made the fundamental discovery that there was a close connection between his work on towers of cyclotomic fields and these p-adic L-functions of Leopoldt–Kubota.

The classical results of Kummer, Stickelberger, and the Iwasawa–Leopoldt theories have been complemented by, and received new significance from the following directions:

1. The analogues for abelian extensions of imaginary quadratic fields in the context of complex multiplication by Novikov, Robert, and Coates–Wiles. Especially the latter, leading to a major result in the direction of the

Birch–Swinnerton-Dyer conjecture, new insight into the explicit reciprocity laws, and a refinement of the Kummer–Takagi theory of units to all levels.

2. The development by Coates, Coates–Sinnott and Lichtenbaum of an analogous theory in the context of K-theory.

3. The development by Kubert–Lang of an analogous theory for the units and cuspidal divisor class group of the modular function field.

4. The introduction of modular forms by Ribet in proving the converse of Herbrand's theorem. The connection between cyclotomic theory and modular forms reached a culmination in the work of Mazur–Wiles, who proved the "main conjecture". This is one of the greatest achievements of the modern period of mathematics.

5. The connection between values of zeta functions at negative integers and the constant terms of modular forms starting with Klingen and Siegel, and highly developed to congruence properties of these constant terms by Serre, for instance, leading to the existence of the p-adic L-function for arbitrary totally real fields.

6. The construction of p-adic zeta functions in various contexts of elliptic curves and modular forms by Katz, Manin, Mazur, Vishik.

7. The connection with rings of endomorphisms of abelian varieties or curves, involving complex multiplication (Shimura–Taniyama) and/or the Fermat curve (Davenport–Hasse–Weil and more recently Gross–Rohrlich).

My two volumes on Cyclotomic Fields provided a systematic introduction to the basic theory. No such introduction existed when they first came out. Since then, Washington's book has appeared, covering some of the material but emphasizing different things. As my books went out of print, Springer-Verlag and I decided to continue making them available in a single volume for the convenience of readers. No changes have been made except for some corrections, for which I am indebted to Larry Washington, Neal Koblitz, and others. Thus the book is kept essentially purely cyclotomic, and as elementary as possible, although in a couple of places we use class field theory. No connection is made with modular forms. This would require an entire book by itself. However, in a major development, a purely cyclotomic proof of the "main conjecture", the Mazur–Wiles theorem, has been found, and I am very much indebted to Karl Rubin for having given me an appendix containing a self-contained proof, based on work of Thaine, Kolyvagin and Rubin himself. For details of the history, see Rubin's own introduction to his appendix.

My survey article [L 5] provides another type of introduction to cyclotomic theory. First, at the beginning in §2 it gives a quick and efficient summary of main results, stripped of their proofs which necessarily add bulk. Second, this article is also useful to get a perspective on cyclotomic fields in connection with other topics, for instance having to do with modular curves and elliptic curves. In that survey, I emphasize questions about class groups and unit groups in a broader context than cyclotomic fields. Specifically, in Theorem 4.2 of [L 5] I state how Mazur–

Wiles construct certain class fields (abelian unramified extensions) of cyclotomic fields by means of torsion points on the Jacobians of modular curves. The existence of class fields of certain degrees is predicted abstractly by the pure cyclotomic theory, but the explicit description of the irrationalities generating such class fields provides an additional basic structure. In that sense, the purely cyclotomic proof of the "main conjecture", and even the "main conjecture" itself, do not supersede and are not substitutes for the Mazur–Wiles theory.

The first seven chapters of the present book, together with Chapters 10, 11, 12 and 13 and Rubin's appendix develop systematically the basic structure of units and ideal class groups in cyclotomic fields, or possibly Galois extensions whose Galois group is isomorphic to the group of p-adic integers. We look at the ideal class group in fields such as $\mathbf{Q}(\mu_{p^n})$ where μ_{p^n} is the group of p^n-th roots of unity. We decompose these groups, as well as their projective limits, into eigenspaces for characters of $(\mathbf{Z}/p\mathbf{Z})^*$, and we attempt to describe as precisely as possible the structure of these eigenspaces. For instance, let h_p denote the class number of $\mathbf{Q}(\mu_p)$. There is already a natural decomposition $h_p = h_p^+ h_p^-$, where h_p^+ is the order of the $(+1)$-eigenspace, and h_p^- is the order of the (-1)-eigenspace for complex conjugation, and similarly for p^n instead of p. Part of the problem is to determine as accurately as possible the p-divisibility of h_p^+ and h_p^-, and also asymptotically for p^n instead of p when $n \to \infty$.

A number of chapters are logically independent of each other. For instance, readers might want to read Chapter 10 on measures and Iwasawa power series immediately after Chapter 4, since the ideas of Chapter 10 are continuations of those of Chapter 4. This leads naturally into the Ferrero–Washington theorems, proving Iwasawa's conjecture that the p-primary part of the ideal class group in the cyclotomic $\mathbf{Z}_p$-extension of a cyclotomic field grows linearly rather than exponentially. This is first done for the minus part (the minus referring, as usual, to the eigenspace for complex conjugation), and then it follows for the plus part because of results bounding the plus part in terms of the minus part. Kummer had already proved such results. Another proof for the Ferrero–Washington theorem was subsequently given by Sinnott [Sin 2].

The first seven chapters suffice for the proof of the "main conjecture" in Rubin's appendix, which does not use the Ferrero–Washington theorem. However, using that theorem in addition gives a clearer picture of the projective limit of the ideal class groups as module over the projective limit of the group rings $\mathbf{Z}_p[G_n]$, where G_n is the Galois group of $\mathbf{Q}(\mu_{p^n})$ over $\mathbf{Q}(\mu_p)$, and therefore also as module over $\mathbf{Z}_p$. This module plays a role analogous to the Jacobian in the theory of curves. The Ferrero–Washington theorem states that up to a finite torsion group, this module is free of finite rank over $\mathbf{Z}_p$. The "main conjecture" gives some description of the characteristic polynomial of a generator for the Galois group playing an analogous role to the Frobenius endomorphism in the theory

of curves. Questions then arise whether these characteristic polynomials behave in ways similar to those in the theory of curves over finite fields. These questions pertain both to the nature of these polynomials, e.g. their coefficients and their roots (Riemann type hypotheses); and also concerning the behavior of these polynomials for varying p. Cf. [L 5], p. 274.

After dealing mostly with ideal class groups and units, we turn to a more systematic study of Gauss sums. We do what amounts to "Dwork theory", to derive the Gross–Koblitz formula expressing Gauss sums in terms of the p-adic gamma function. This lifts Stickelberger's theorem p-adically. Half of the proof relies on a course of Katz, who had first obtained Gauss sums as limits of certain factorials, and thought of using Washnitzer–Monsky cohomology to prove the Gross–Koblitz formula.

Finally, we apply these latter results to the Ferrero–Greenberg theorem, showing that $L_p'(0, \chi) \neq 0$ under the appropriate conditions. We take this opportunity to introduce a technique of Washington, who defined the p-adic analogues of the Hurwitz partial zeta functions, in a way making it possible to parallel the treatment from the complex case to the p-adic case, but in a much more efficient way.

Some basic conjectures remain open, notably the Kummer–Vandiver conjecture that h_p^+ is prime to p. The history of that conjecture is interesting. Kummer made it in no uncertain terms in a letter to Kronecker dated 28 December 1849. Kummer first tells Kronecker off for not understanding properly what he had previously written about cyclotomic fields and Fermat's equation, by stating "so liegt hierin ein grosser Irrthum deinerseits ..."; and then he goes on (Collected Works, Vol. 1, p. 84):

> Deine auf dieser falschen Ansicht berühenden Folgerungen fallen somit von selbst weg. Ich gedenke vielmehr den Beweis des Fermatschen Satzes auf folgendes zu grunden:
> 1. Auf den noch zu beweisenden Satz, dass es für die Ausnahmszahlen λ stets Einheiten giebt, welche ganzen Zahlen congruent sind für den Modul λ, ohne darum λte Potenzen anderer Einheiten zu sein, oder was dasselbe ist, dass hier niemals D/Δ durch λ theilbar wird.

In our notation: $\lambda = p$ and $D/\Delta = h_p^+$. Kummer wrote D/Δ as a quotient of regulators, expressing the index of the cyclotomic units in the group of all units. This index happens to coincide with h_p^+ (cf. Theorem 5.1 of Chapter 3). Thus Kummer rather expected to prove the conjecture. According to Barry Mazur, who reviewed Kummer's complete works when they were published by Springer-Verlag, Kummer never mentioned the conjecture in a published paper, but he mentioned it once more in another letter to Kronecker on 24 April 1853 (loc cit p. 93):

> Hierein hängt auch zusammen, dass eines meiner Haupresultate auf welches ich seit einem Vierteljahre gebaut hatte, dass der zweite Faktor der Klassen-

> zahl D/Δ niemals durch λ theilbar ist, falsch ist oder wenigstens unbewiesen ... Ich werde also vorlaufig hauptsachlich meinen Fleiss nur auf die Weiterführung der Theorie der complexen Zahlen wenden, und dann sehen ob etwas daraus entsteht, was auch uber jene Aufgabe Licht verbreitet.

So the situation was less clear than Kummer thought at first. Much later, Vandiver made the same conjecture, and wrote [Va 1]:

> ... However, about twenty-five years ago I conjectured that this number was never divisible by l [referring to h^+]. Later on, when I discovered how closely the question was related to Fermat's Last Theorem, I began to have my doubts, recalling how often conjectures concerning the theorem turned out to be incorrect. When I visited Furtwängler in Vienna in 1928, he mentioned that he had conjectured the same thing before I had brought up any such topic with him. As he had probably more experience with algebraic numbers than any mathematician of his generation, I felt a little more confident ....

On the other hand, many years ago, Feit was unable to understand a step in Vandiver's "proof" that $p \nmid h^+$ implies the first case of Fermat's Last Theorem, and stimulated by this, Iwasawa found a precise gap which is such that there is no proof.

The Iwasawa–Leopoldt conjecture that the p-primary part of C^- is cyclic over the group ring, and is therefore isomorphic to the group ring modulo the Stickelberger ideal, also remains open. For prime level, Leopoldt and Iwasawa have shown that this is a consequence of the Kummer–Vandiver conjecture. Cf. Chapter IV, §4.

Much of the cyclotomic theory extends to totally real number fields, as theorems or conjecturally. We do not touch on this aspect of the question. Cf. Coates' survey paper [Co 3], and especially Shintani [Sh].

Coates, Ribet, and Rohrlich had read the original manuscript and had made a large number of suggestions for improvement. I thank them again, as well as Koblitz and Washington, for their suggestions and corrections.

New Haven, 1989 SERGE LANG