Graduate Texts in Mathematics

Lawrence C. Washington

Introduction to Cyclotomic Fields

Second Edition

割圆域导论 第2版

Springer

世界图书出版公司
www.wpcbj.com.cn

Graduate Texts in Mathematics

Lawrence C. Washington

Introduction to Cyclotomic Fields

Second Edition

Springer

Lawrence C. Washington

Introduction to Cyclotomic Fields

Second Edition

Springer

图书在版编目（CIP）数据

割圆域导论：第2版：英文/(美)华盛顿著. —北京：世界图书出版公司北京公司，2014.7

ISBN 978-7-5100-7785-2

Ⅰ.①割… Ⅱ.①华… Ⅲ.①数论—教材—英文 Ⅳ.①O156

中国版本图书馆CIP数据核字（2014）第057743号

书　　名：	Introduction to Cyclotomic Fields 2nd ed.
作　　者：	Lawrence C. Washington
中 译 名：	割圆域导论 第2版
责任编辑：	高蓉　刘慧
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河市国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街137号 100010）
联系电话：	010-64021602，010-64015659
电子信箱：	kjb@wpcbj.com.cn
开　　本：	24开
印　　张：	21.5
版　　次：	2014年7月
版权登记：	图字：01-2013-6777
书　　号：	978-7-5100-7785-2　　定　　价：79.00元

Graduate Texts in Mathematics 83

Springer
New York
Berlin
Heidelberg
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

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 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. 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

(continued after index)

Lawrence C. Washington
Mathematics Department
University of Maryland
College Park, MD 20742
USA

Mathematics Subject Classification (1991): 11Rxx, 11-01

With nine illustrations.

Library of Congress Cataloging-in-Publication Data
Washington, Lawrence C.
Introduction to cyclotomic fields / Lawrence C. Washington. — 2nd ed.
p. cm. — (Graduate texts in mathematics ; 83)
Includes bibliographical references and index.
ISBN 0-387-94762-0 (hardcover : alk. paper)
1. Algebraic fields. 2. Cyclotomy. I. Title. II. Series.
QA247.W35 1996
512'.74—dc20 96-13169

To My Parents

Preface to the Second Edition

Since the publication of the first edition, several remarkable developments have taken place. The work of Thaine, Kolyvagin, and Rubin has produced fairly elementary proofs of Ribet's converse of Herbrand's theorem and of the Main Conjecture. The original proofs of both of these results used delicate techniques from algebraic geometry and were inaccessible to many readers. Also, Sinnott discovered a beautiful proof of the vanishing of Iwasawa's μ-invariant that is much simpler than the one given in Chapter 7. Finally, Fermat's Last Theorem was proved by Wiles, using work of Frey, Ribet, Serre, Mazur, Langlands–Tunnell, Taylor–Wiles, and others. Although the proof, which is based on modular forms and elliptic curves, is much different from the cyclotomic approaches described in this book, several of the ingredients were inspired by ideas from cyclotomic fields and Iwasawa theory.

The present edition includes two new chapters covering some of these developments. Chapter 15 treats the work of Thaine, Kolyvagin, and Rubin, culminating in a proof of the Main Conjecture for the pth cyclotomic field. Chapter 16 includes Sinnott's proof that $\mu = 0$ and his elementary proof of the corresponding result on the ℓ-part of the class number in a $\mathbb{Z}_p$-extension. Since the application of Jacobi sums to primality testing was too beautiful to omit, I have also included it in this chapter.

The first 14 chapters have been left essentially unchanged, except for corrections and updates. The proof of Fermat's Last Theorem, which is far beyond the scope of the present book, makes certain results of these chapters obsolete. However, I decided to let them remain, for they are interesting not only from an historical viewpoint but also as applications of various techniques. Moreover, some of the results of Chapter 9 apply to Vandiver's conjecture, one of the major unresolved questions in the field. For aesthetic reasons, it might have been appropriate to put the new Chapter 15 immedi-

ately after Chapter 13. However, I opted for the more practical route of placing it after the Kronecker–Weber theorem, thus ensuring that all numbering from the first edition is compatible with the second.

Other changes from the first edition include updating the bibliography and the addition of a table of class numbers of real cyclotomic fields due to Schoof.

Many people have sent me detailed lists of corrections and suggestions or have contributed in other ways to this edition. In particular, I would like to thank Brian Conrad, Keith Conrad, Li Guo, Mikihito Hirabayashi, Jim Kraft, Tauno Metsänkylä, Ken Ribet, Yuan-Yuan Shen, Peter Stevenhagen, Patrick Washington, and Susan Zengerle.

Lawrence C. Washington

Preface to the First Edition

This book grew out of lectures given at the University of Maryland in 1979/1980. The purpose was to give a treatment of p-adic L-functions and cyclotomic fields, including Iwasawa's theory of $\mathbb{Z}_p$-extensions, which was accessible to mathematicians of varying backgrounds.

The reader is assumed to have had at least one semester of algebraic number theory (though one of my students took such a course concurrently). In particular, the following terms should be familiar: Dedekind domain, class number, discriminant, units, ramification, local field. Occasionally one needs the fact that ramification can be computed locally. However, one who has a good background in algebra should be able to survive by talking to the local algebraic number theorist. I have not assumed class field theory; the basic facts are summarized in an appendix. For most of the book, one only needs the fact that the Galois group of the maximal unramified abelian extension is isomorphic to the ideal class group, and variants of this statement.

The chapters are intended to be read consecutively, but it should be possible to vary the order considerably. The first four chapters are basic. After that, the reader willing to believe occasional facts could probably read the remaining chapters randomly. For example, the reader might skip directly to Chapter 13 to learn about $\mathbb{Z}_p$-extensions. The last chapter, on the Kronecker–Weber theorem, can be read after Chapter 2.

The notations used in the book are fairly standard; $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_p$, and $\mathbb{Q}_p$ denote the integers, the rationals, the p-adic integers, and the p-adic rationals, respectively. If A is a ring (commutative with identity), then $A^\times$ denotes its group of units. At Serge Lang's urging I have let the first Bernoulli number be $B_1 = -\frac{1}{2}$ rather than $+\frac{1}{2}$. This disagrees with Iwasawa [23] and several of my papers, but conforms to what is becoming standard usage.

Throughout the preparation of this book I have found Serge Lang's two volumes on cyclotomic fields very helpful. The reader is urged to look at them for different viewpoints on several of the topics discussed in the present volume and for a different selection of topics. The second half of his second volume gives a nice self-contained (independent of the remaining one and a half volumes) proof of the Gross–Koblitz relation between Gauss sums and the p-adic gamma function, and the related formula of Ferrero and Greenberg for the derivative of the p-adic L-function at 0, neither of which I have included here. I have also omitted a discussion of explicit reciprocity laws. For these the reader can consult Lang [4], Hasse [2], Henniart, Ireland–Rosen, Tate [3], or Wiles [1].

Perhaps it is worthwhile to give a very brief history of cyclotomic fields. The subject got its real start in the 1840s and 1850s with Kummer's work on Fermat's Last Theorem and reciprocity laws. The basic foundations laid by Kummer remained the main part of the theory for around a century. Then in 1958, Iwasawa introduced his theory of $\mathbb{Z}_p$-extensions, and a few years later Kubota and Leopoldt invented p-adic L-functions. In a major paper (Iwasawa [18]), Iwasawa interpreted these p-adic L-functions in terms of $\mathbb{Z}_p$-extensions. In 1979, Mazur and Wiles proved the Main Conjecture, showing that p-adic L-functions are essentially the characteristic power series of certain Galois actions arising in the theory of $\mathbb{Z}_p$-extensions.

What remains? Most of the universally accepted conjectures, in particular those derived from analogy with function fields, have been proved, at least for abelian extensions of $\mathbb{Q}$. Many of the conjectures that remain are probably better classified as "open questions," since the evidence for them is not very overwhelming, and there do not seem to be any compelling reasons to believe or not to believe them. The most notable are Vandiver's conjecture, the weaker statement that the p-Sylow subgroup of the ideal class group of the pth cyclotomic field is cyclic over the group ring of the Galois group, and the question of whether or not $\lambda = 0$ for totally real fields. In other words, we know a lot about imaginary things, but it is not clear what to expect in the real case. Whether or not there exists a fruitful theory remains to be seen.

Other possible directions for future developments could be a theory of $\hat{\mathbb{Z}}$-extensions ($\hat{\mathbb{Z}} = \prod \mathbb{Z}_p$; some progress has recently been made by Friedman [1]), and the analogues of Iwasawa's theory in the elliptic case (Coates–Wiles [4]).

I would like to thank Gary Cornell for much help and many excellent suggestions during the writing of this book. I would also like to thank John Coates for many helpful conversations concerning Chapter 13. This chapter also profited greatly from the beautiful courses of my teacher, Kenkichi Iwasawa, at Princeton University. Finally, I would like to thank N.S.F. and the Sloan Foundation for their financial support and I.H.E.S. and the University of Maryland for their academic support during the writing of this book.

Lawrence C. Washington

Contents

CHAPTER 1

Fermat's Last Theorem

We start with a special case of Fermat's Last Theorem, since not only was it the motivation for much work on cyclotomic fields but also it provides a sampling of the various topics we shall discuss later.

Theorem 1.1. *Suppose p is an odd prime and p does not divide the class number of the field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity. Then*

$$x^p + y^p = z^p, \qquad (xyz, p) = 1$$

has no solutions in rational integers.

Remark. The case where p does not divide x, y, and z is called the first case of Fermat's Last Theorem, and is in general easier to treat than the second case, where p divides one of x, y, z. We shall prove the above theorem in the second case later, again with the assumption on the class number.

Factoring the above equation as

$$\prod_{i=0}^{p-1} (x + \zeta_p^i y) = z^p,$$

we find we are naturally led to consider the ring $\mathbb{Z}[\zeta_p]$. We first need some basic results on this ring. Throughout the remainder of this chapter, we let $\zeta = \zeta_p$.

Proposition 1.2. *$\mathbb{Z}[\zeta]$ is the ring of algebraic integers in the field $\mathbb{Q}(\zeta)$. Therefore $\mathbb{Z}[\zeta]$ is a Dedekind domain (so we have unique factorization into prime ideals, etc.).*