Universitext

Universitext

Universitext is a series of textbooks that presents material from a wide variety of mathematical disciplines at master's level and beyond. The books, often well class-tested by their author, may have an informal, personal even experimental approach to their subject matter. Some of the most successful and established books in the series have evolved through several editions, always following the evolution of teaching curricula, into very polished texts.

Thus as research topics trickle down into graduate-level teaching, first textbooks written for new, cutting-edge courses may make their way into *Universitext.*

More information about this series at http://www.springer.com/series/223

Daniel A. Marcus

Number Fields

Second Edition

Typeset in LaTeX by Emanuele Sacco

Springer

Daniel A. Marcus (Deceased)
Columbus, OH
USA

ISSN 0172-5939 ISSN 2191-6675 (electronic)
Universitext
ISBN 978-3-319-90232-6 ISBN 978-3-319-90233-3 (eBook)
https://doi.org/10.1007/978-3-319-90233-3

Library of Congress Control Number: 2018939311

Mathematics Subject Classification (2010): 12-01, 11Rxx, 11Txx

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG part of Springer Nature
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To my parents, Selma and Louis Marcus

Foreword to the Second Edition

What a wonderful book this is! How generous it is in its tempo, its discussions, and in the details it offers. It heads off—rather than merely clears up—the standard confusions and difficulties that beginners often have. It is perceptive in its understanding of exactly which points might prove to be less than smooth sailing for a student, and how it prepares for those obstacles. The substance that it teaches represents a unified arc; nothing extraneous, nothing radically digressive, and everything you need to learn, to have a good grounding in the subject: *Number Fields*.

What makes Marcus' book particularly unusual and compelling is the deft choice of approach to the subject that it takes, requiring such minimal prerequisites; and also the clever balance between text in each chapter and exercises at the end of the chapter: Whole themes are developed in the exercises that fit neatly into the exposition of the book; as if text and exercise are in conversation with each other—the effect being that the student who engages with this text and these exercises is seamlessly drawn into being a collaborator with the author in the exposition of the material.

When I teach this subject, I tend to use Marcus' book as my principal text for all of the above reasons. But, after all, the subject is vast; there are many essentially different approaches to it.[1] A student—even while learning it from one point of view—might profit by being, at the very least, aware of some of the other ways of becoming at home with Number Fields.

There is, for example, the great historical volume *Hilbert's Zahlbericht* published originally in 1897.[2] This hugely influential treatise introduced generations of mathematicians to Number Fields and was studied by many of the major historical

[1] I sometimes ask students to also look at Pierre Samuel's book *Algebraic Theory of Numbers*, Dover (2008), since it does have pretty much the same prerequisites and coverage that Marcus's book has but with a slightly different tone—a tiny bit more formal. No Exercises, though!

[2] The English translation: *The Theory of Algebraic Number Fields*, Springer (1998); see especially the introduction in it written by F. Lemmermeyer and N. Schappacher: `http://www.fen.bilkent.edu.tr/~franz/publ/hil.pdf`.

contributors to the subject, but also has been the target of criticism by André Weil: "More than half of his (i.e., Hilbert's) famous Zahlbericht (viz., parts IV and V) is little more than an account of Kummer's number-theoretical work, with inessential improvements…"[3] One could take this as a suggestion to go back to the works of Kummer—and that would be an enormously illuminating and enjoyable thing to do but not suitable as a *first* introduction to the material. Marcus, however, opens his text (Chap. 1) by visiting Kummer's approach to Fermat's Last Theorem[4] as a way of giving the reader a taste of some of the themes that have served as an inspiration to generations of mathematicians engaged in number theory, and that will be developed further in the book.

André Weil, so critical of Hilbert, had nothing but praise for another classical text—a text quite accessible to students, possibly more so than Hilbert's Zahlbericht—namely, *Lectures on the Theory of Algebraic Numbers* by Erich Hecke.[5] This is the book from which I learned the subject (although there are no exercises in it). To mention André Weil again: "To improve on Hecke in a treatise along classical lines of the theory of algebraic numbers, would be a futile and impossible task."

The flavor of any text in this subject strongly depends on the balance of emphasis it places on *local concepts* in connection with the global objects of study. Does one, for example, treat—or even begin with—local rings and local fields, as they arise as completion and localization rings of integers in global fields? Marcus' text takes a clear position here: It simply focuses on the global. This has advantages: Students who are less equipped with algebraic prerequisites can approach the text more easily; and the instructor can, at appropriate moments, insert some local theory at a level dependent on the background of the students.[6]

---

[3]This is in Weil's introduction to the works of Kummer. See the review published in BAMS: `http://www.ams.org/journals/bull/1977-83-05/S0002-9904-1977-14343-7/S0002-9904-1977-14343-7.pdf`.

[4]This was finally proved by Andrew Wiles in 1994, using methods far beyond those of Kummer.

[5]English translation: Springer (1981).

[6]For texts that deal with the local considerations at the outset and that cover roughly the same material but expect a bit more mathematical experience of its readers, see

- Fröhlich, A., Taylor, M.J.: *Algebraic number theory*. Cambridge University Press (1991)
- Milne, J.S.: *Algebraic number theory*, online course notes. `http://www.jmilne.org/math/CourseNotes/ANT.pdf`.

Excellent "classic" texts having even more focus, at the beginning, on the local aspects—but requiring *much* more background—are

- Cassels, Fröhlich: *Algebraic number theory*, 2nd edn. London Mathematical Society (2010)
- Serre, J.-P.: *Local fields*, Springer (1979).

The many exercises of a computational nature included in the book introduce the reader to a staggeringly important side of our subject—nowadays readily accessible to anyone[7] who might want to numerically experiment with the concepts introduced in this book: discriminants, rings of integers, generators of the group of units, class groups, etc. To have this capability of exploration is enormously helpful to students who wish to be fully at home with the actual phenomena. And there are texts that deal with our subject directly from a computational point of view.[8]

This book offers such a fine approach to our subject and is such a marvelous guide to it, introducing the reader to many modern themes of extreme interest in number theory. For example, *cyclotomic fields*[9]—which Serge Lang once labeled "the backbone of number theory"—is a continuing thread throughout the book, used throughout as a rich source of theory and examples, including some of Kummer's results (in the exercises to Chaps. 1 and 2), the *Kronecker–Weber theorem* (in the exercises to Chap. 4), and *Stickelberger's criterion* (in the exercises to Chap. 2). The Kronecker–Weber theorem, proved at the turn of the nineteenth century, asserts that any number field that is an *abelian*[10] Galois extension of $\mathbb{Q}$, the field of rational numbers, is contained in a cyclotomic field. This result was a precursor of *Class Field Theory*, briefly introduced in Chap. 8, which gives a description and construction of abelian extensions of number fields. Class field theory is itself a precursor of a program—the "Langlands Program"—intensely pursued nowadays, whose goal is to construct a very far-reaching but intimate relationship between algebraic number theory and the representation theory of reductive algebraic groups. This relationship is founded on *zeta functions*, such as those studied in this book from Chap. 7 onwards. The study of zeta functions involves *Analytic Number Theory*, which the reader will get a taste of in Chaps. 6–7. One of the main results is the *class number formula*, shown in Chap. 7, relating the *class number* of a number field to the residue of its Dedekind zeta function at 1. The precise formula requires the concept of *regulator* of a number field, one that naturally belongs to the *Geometry of Numbers*, appearing here in the form of the classical result of Minkowski given in Chap. 5, which is then—as Minkowski did—used to prove fundamental theorems such as Dirichlet's Unit

---

[7] See `http://www.lmfdb.org/NumberField.`

[8] E.g.,

- *A Course in Computational Algebraic Number Theory* by Henri Cohen, Springer (1993)
- *Algebraic Number Theory: A Computational Approach* by William Stein (2012), `http://wstein.org/books/ant/ant.pdf.`

[9] See Chap. 2 for the definition.

[10] Meaning: a Galois extension with an abelian Galois group.

Theorem and the finiteness of the class number. Among the fine array of exercises on class numbers, there is an excursion into *Gauss's class number one problem* in Chap. 5. And the Chebotarev Density Theorem[11] occurs as an exercise in Chap. 8.

But I should end my foreword here and let you begin reading.

Cambridge, Massachusetts
March 2018

Barry Mazur

[11] This theorem gives the precise densities of splitting of primes in a Galois extension—e.g., in a Galois extension of degree n, the "probability" is 1-to-n that a prime of the base will split completely in the extension.

Preface

This book grew out of the lecture notes of a course which I gave at Yale University in the Fall semester, 1972. Exercises were added and the text was rewritten in 1975 and 1976. The first four chapters in their present form were used in a course at Ohio State University in the Fall quarter, 1975.

The first six chapters can be read, in conjunction with Appendices A–C, by anyone who is familiar with the most basic material covered in standard undergraduate courses in linear algebra and abstract algebra. Some complex analysis (meromorphic functions, series and products of functions) is required for Chaps. 7 and 8. Specific references are given.

The level of exposition rises as the book progresses. In Chap. 2, for example, the degree of a field extension is defined, while in Chap. 4 it is assumed that the reader knows Galois theory. The idea is to make it possible for someone with little experience to begin reading the book without difficulty and to be lured into reading further, consulting the appendices for background material when necessary.

I have attempted to present the mathematics in a straightforward "down to earth" manner that would be accessible to the inexperienced reader but hopefully still interesting to the more sophisticated. Thus, I have avoided local methods with no apparent disadvantages except possibly in exercises 20–21 of Chap. 3 and exercises 19–22 of Chap. 4. Even there, I feel that it is worthwhile to have available "direct" proofs such as I present. Any awkwardness therein can be taken by the reader as motivation to learn about localization. At the same time, it is assumed that the reader is reasonably adept at filling in details of arguments. In many places, details are left as exercises, often with elaborate hints. The purpose of this is to make the proofs cleaner and easier to read and to promote involvement on the part of the reader.

Major topics are presented in the exercises: Fractional ideals and the different in Chap. 3, ramification groups and the Kronecker–Weber Theorem in Chap. 4, fundamental units in non-totally real cubic fields in Chap. 5, and cyclotomic class numbers and units in Chap. 7. Many other results appear in step-by-step exercise form. Among these are the determination of the algebraic integers in pure cubic fields (Chap. 2), the proof that prime divisors of the relative different are ramified over the ground field (Chap. 4), and the Frobenius Density Theorem (Chap. 7).

I have taken the liberty to introduce some new terminology ("number ring" for the ring of algebraic integers in a number field), a notational reform ($||I||$ for the index of an ideal I in a number ring, rather than the more cumbersome $\mathrm{N}(I)$), and the concept of polar density, which seems to be the "right" density for sets of primes in a number field. Notice, for example, how easily one obtains Theorem 43 and its corollaries.

Chapter 8 represents a departure from tradition in several ways. The distribution of primes is handled in an abstract context (Theorem 48) and without the complex logarithm. The main facts of class field theory are stated without proof (but, I hope, with ample motivation) and without fractional ideals. Results on the distribution of primes are then derived from these facts. It is hoped that this chapter will be of some help to the reader who goes on to study class field theory.

Columbus, Ohio Daniel A. Marcus
June 1977

Acknowledgements

I thank John Yang for the determination of the algebraic integers in a biquadratic field (exercise 42, Chap. 2) and Dodie Shapiro for the very careful final typing, which is what you see here.

Also, thanks go to my wife Shelley for her unfailing wit and to my son Andrew, age 4, for his cheerful presence.

Contents

Symbols

$\mathbb{Z}$	Integers
$\mathbb{Q}$	Rational numbers
$\mathbb{R}$	Real numbers
$\mathbb{C}$	Complex numbers
$\mathbb{A}$	Algebraic integers in $\mathbb{C}$
$\mathbb{Z}_m$	$= \{0, 1, \ldots, m-1\}$ integers mod m
$\mathbb{Z}_m^*$	$= \{k \in \mathbb{Z}_m : (k, m) = 1\}$ multiplicative group mod m
(m, n)	Greatest common divisor of m and n
$\varphi(m)$	Number of elements in $\mathbb{Z}_m^*$
$\phi(\cdot)$	Frobenius automorphism; Artin map
K, L	Number fields
R, S	Number rings; $R = \mathbb{A} \cap K$, $S = \mathbb{A} \cap L$
P, Q	Prime ideals
I, J	Ideals
$[L : K]$	Degree of L over K
$\|I\|$	Index of I (p. 46)
$\mathrm{Gal}(L\|K)$	Galois group of L over K
$\wedge$	Lattice
ω	Root of unity
ζ	Riemann zeta function
ζ_K	Dedekind zeta function
$\zeta_{K,A}$	See p. 133
$L(s, \chi)$	L-series
$M(s, \chi)$	See p. 162
$\mathrm{N}_K^L(\cdot)$	Norm
$\mathrm{T}_K^L(\cdot)$	Trace
$\mathrm{disc}(\cdot)$	Discriminant
$\mathrm{diff}(\cdot)$	Different
$\mathrm{reg}(\cdot)$	Regulator
$\mathrm{O}(\cdot)$	Big Oh (p. 111)

$i(t), i_C(t)$	Ideal-counting functions (p. 111)
D	Decomposition group
E	Inertia group
V_m	Ramification groups
L_D	Decomposition field
L_E	Inertia field
$\vert$	Divides or lies over
$\vert \cdot \vert$	Absolute value; determinant; number of elements
e_i	Ramification indices
f_i	Inertial degrees
$\left(\frac{p}{q}\right)$	Legendre symbol
$\left(\frac{a}{b}\right)$	Jacobi symbol
$R[x]$	Polynomial ring over R
$R[\alpha]$	Ring generated by α over R
$\subset, \supset$	Containment, not necessarily proper
$\prod$	Product
$\sum$	Sum
$s = x + iy$	Complex variable; $x, y \in \mathbb{R}$
α, β, γ	Algebraic integers
$\overline{\alpha}$	Complex conjugate of α
$\overline{I}$	Ideal class of I
σ, τ	Automorphisms
χ	Character
$\tau(\chi)$, $\tau_k(\chi)$	Gaussian sums
$\hat{G}$	Character group of G
A^{-1}, A^*	See p. 71
$\overset{+}{\sim}, M^{\overset{+}{\sim}}$	See p. 125–126
h	Class number
κ	See p. 111
ρ	See p. 136
f, g	Polynomials
G, H	Groups
G	Ideal class group
H	Hilbert class field
G^+, G_M^+	Ray class groups
H^+, H_M^+	Ray class fields
Π, Π_T	Free abelian semigroups
$\mathbb{S}$	Semigroup in Π or Π_T
$\mathbb{P}$, $\mathbb{P}^+$, $\mathbb{P}_m^+$, $\mathbb{P}_M^+$	Semigroups of principal ideals
$\forall$	For every
$\exists$	There exists