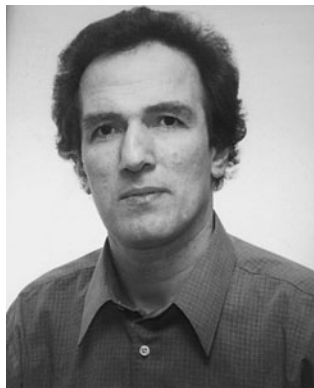


Cambridge University Press
978-0-521-83250-2 - Introductory Algebraic Number Theory
Şaban Alaca and Kenneth S. Williams
Frontmatter
[More information](#)

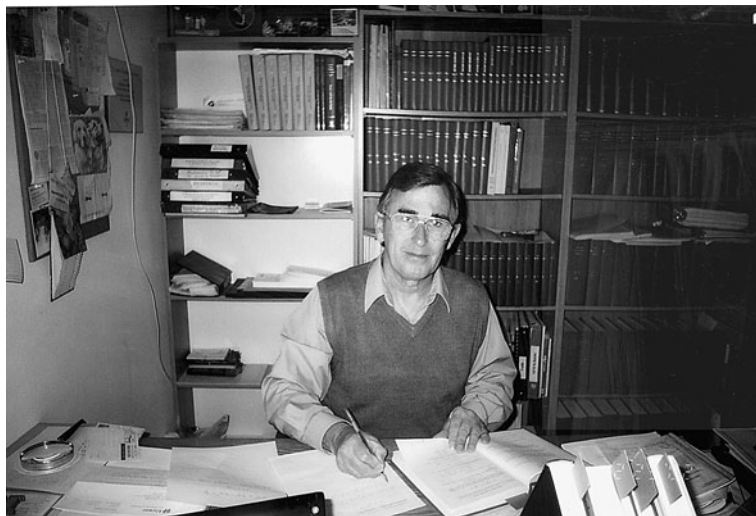
INTRODUCTORY ALGEBRAIC NUMBER THEORY

Algebraic number theory is a subject that came into being through the attempts of mathematicians to try to prove Fermat's last theorem and that now has a wealth of applications to Diophantine equations, cryptography, factoring, primality testing, and public-key cryptosystems.

This book provides an introduction to the subject suitable for senior undergraduate and beginning graduate students in mathematics. The material is presented in a straightforward, clear, and elementary fashion, and the approach is hands on, with an explicit computational flavor. Prerequisites are kept to a minimum, and numerous examples illustrating the material occur throughout the text. References to suggested readings and to the biographies of mathematicians who have contributed to the development of algebraic number theory are given at the end of each chapter. There are more than 320 exercises, an extensive index, and helpful location guides to theorems and lemmas in the text.



Şaban Alaca is Lecturer in Mathematics at Carleton University, where he has been honored by three teaching awards: Faculty of Science Teaching Award, Professional Achievement Award, and Students Choice Award. His main research interest is in algebraic number theory.



Kenneth S. Williams is Professor Emeritus and Distinguished Research Professor of Mathematics at Carleton University. Dr. Williams has published more than 240 research papers in number theory, linear algebra, algebra, and analysis. This is his seventh book.

Cambridge University Press
978-0-521-83250-2 - Introductory Algebraic Number Theory
Şaban Alaca and Kenneth S. Williams
Frontmatter
[More information](#)

Cambridge University Press
978-0-521-83250-2 - Introductory Algebraic Number Theory
Şaban Alaca and Kenneth S. Williams
Frontmatter
[More information](#)

INTRODUCTORY ALGEBRAIC NUMBER THEORY

ŞABAN ALACA

Carleton University, Ottawa

KENNETH S. WILLIAMS

Carleton University, Ottawa



Cambridge University Press
 978-0-521-83250-2 - Introductory Algebraic Number Theory
 Şaban Alaca and Kenneth S. Williams
 Frontmatter
[More information](#)

CAMBRIDGE
 UNIVERSITY PRESS

32 Avenue of the Americas, New York NY 10013-2473, USA

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org

Information on this title: www.cambridge.org/9780521832502

© Şaban Alaca and Kenneth S. Williams 2004

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2004

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data

Alaca, Şaban, 1964–

Introductory algebraic number theory / Şaban Alaca, Kenneth S. Williams.

p. cm.

Includes bibliographical references and index.

ISBN 0-521-83250-0 (hb.) – ISBN 0-521-54011-9 (pbk.)

1. Algebraic number theory. I. Williams, Kenneth S. II. Title.

QA247 .A43 2003

512'.74 – dc21 2003051243

ISBN 978-0-521-83250-2 Hardback

ISBN 978-0-521-54011-7 Paperback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Cambridge University Press
978-0-521-83250-2 - Introductory Algebraic Number Theory
Şaban Alaca and Kenneth S. Williams
Frontmatter
[More information](#)

To our wives
Ayşe and Carole

Cambridge University Press
978-0-521-83250-2 - Introductory Algebraic Number Theory
Şaban Alaca and Kenneth S. Williams
Frontmatter
[More information](#)

Contents

<i>List of Tables</i>	<i>page</i> xi
<i>Notation</i>	xiii
<i>Introduction</i>	xv
1 Integral Domains	1
1.1 Integral Domains	1
1.2 Irreducibles and Primes	5
1.3 Ideals	8
1.4 Principal Ideal Domains	10
1.5 Maximal Ideals and Prime Ideals	16
1.6 Sums and Products of Ideals	21
Exercises	23
Suggested Reading	25
Biographies	25
2 Euclidean Domains	27
2.1 Euclidean Domains	27
2.2 Examples of Euclidean Domains	30
2.3 Examples of Domains That are Not Euclidean	37
2.4 Almost Euclidean Domains	46
2.5 Representing Primes by Binary Quadratic Forms	47
Exercises	49
Suggested Reading	51
Biographies	53
3 Noetherian Domains	54
3.1 Noetherian Domains	54
3.2 Factorization Domains	57
3.3 Unique Factorization Domains	60
3.4 Modules	64
3.5 Noetherian Modules	67
Exercises	71

	Suggested Reading	72
	Biographies	73
4	Elements Integral over a Domain	74
4.1	Elements Integral over a Domain	74
4.2	Integral Closure	81
	Exercises	86
	Suggested Reading	87
	Biographies	87
5	Algebraic Extensions of a Field	88
5.1	Minimal Polynomial of an Element Algebraic over a Field	88
5.2	Conjugates of α over K	90
5.3	Conjugates of an Algebraic Integer	91
5.4	Algebraic Integers in a Quadratic Field	94
5.5	Simple Extensions	98
5.6	Multiple Extensions	102
	Exercises	106
	Suggested Reading	108
	Biographies	108
6	Algebraic Number Fields	109
6.1	Algebraic Number Fields	109
6.2	Conjugate Fields of an Algebraic Number Field	112
6.3	The Field Polynomial of an Element of an Algebraic Number Field	116
6.4	The Discriminant of a Set of Elements in an Algebraic Number Field	123
6.5	Basis of an Ideal	129
6.6	Prime Ideals in Rings of Integers	137
	Exercises	138
	Suggested Reading	140
	Biographies	140
7	Integral Bases	141
7.1	Integral Basis of an Algebraic Number Field	141
7.2	Minimal Integers	160
7.3	Some Integral Bases in Cubic Fields	170
7.4	Index and Minimal Index of an Algebraic Number Field	178
7.5	Integral Basis of a Cyclotomic Field	186
	Exercises	189
	Suggested Reading	191
	Biographies	193
8	Dedekind Domains	194
8.1	Dedekind Domains	194
8.2	Ideals in a Dedekind Domain	195

<i>Contents</i>		ix
8.3	Factorization into Prime Ideals	200
8.4	Order of an Ideal with Respect to a Prime Ideal	206
8.5	Generators of Ideals in a Dedekind Domain	215
	Exercises	216
	Suggested Reading	217
9	Norms of Ideals	218
9.1	Norm of an Integral Ideal	218
9.2	Norm and Trace of an Element	222
9.3	Norm of a Product of Ideals	228
9.4	Norm of a Fractional Ideal	231
	Exercises	233
	Suggested Reading	234
	Biographies	235
10	Factoring Primes in a Number Field	236
10.1	Norm of a Prime Ideal	236
10.2	Factoring Primes in a Quadratic Field	241
10.3	Factoring Primes in a Monogenic Number Field	249
10.4	Some Factorizations in Cubic Fields	253
10.5	Factoring Primes in an Arbitrary Number Field	257
10.6	Factoring Primes in a Cyclotomic Field	260
	Exercises	261
	Suggested Reading	262
11	Units in Real Quadratic Fields	264
11.1	The Units of $\mathbb{Z} + \mathbb{Z}\sqrt{2}$	264
11.2	The Equation $x^2 - my^2 = 1$	267
11.3	Units of Norm 1	271
11.4	Units of Norm -1	275
11.5	The Fundamental Unit	278
11.6	Calculating the Fundamental Unit	286
11.7	The Equation $x^2 - my^2 = N$	294
	Exercises	297
	Suggested Reading	298
	Biographies	298
12	The Ideal Class Group	299
12.1	Ideal Class Group	299
12.2	Minkowski's Translate Theorem	300
12.3	Minkowski's Convex Body Theorem	305
12.4	Minkowski's Linear Forms Theorem	306
12.5	Finiteness of the Ideal Class Group	311
12.6	Algorithm to Determine the Ideal Class Group	314
12.7	Applications to Binary Quadratic Forms	331
	Exercises	341

x	<i>Contents</i>	
	Suggested Reading	343
	Biographies	343
13	Dirichlet's Unit Theorem	344
13.1	Valuations of an Element of a Number Field	344
13.2	Properties of Valuations	346
13.3	Proof of Dirichlet's Unit Theorem	359
13.4	Fundamental System of Units	361
13.5	Roots of Unity	363
13.6	Fundamental Units in Cubic Fields	369
13.7	Regulator	378
	Exercises	382
	Suggested Reading	383
	Biographies	384
14	Applications to Diophantine Equations	385
14.1	Insolvability of $y^2 = x^3 + k$ Using Congruence Considerations	385
14.2	Solving $y^2 = x^3 + k$ Using Algebraic Numbers	389
14.3	The Diophantine Equation	
	$y(y + 1) = x(x + 1)(x + 2)$	401
	Exercises	410
	Suggested Reading	411
	Biographies	411
	<i>List of Definitions</i>	413
	<i>Location of Theorems</i>	417
	<i>Location of Lemmas</i>	421
	<i>Bibliography</i>	423
	<i>Index</i>	425

List of Tables

1	Integral bases and discriminants for $\mathbb{Q}(\sqrt[3]{k})$, $2 \leq k \leq 20$, k cubefree.	page 177
2	Integral bases and discriminants for $\mathbb{Q}(\sqrt[4]{k})$, $x^4 - k$ irreducible in $\mathbb{Q}[x]$, $2 \leq k \leq 10$.	177
3	Integral bases and discriminants for $\mathbb{Q}(\sqrt[4]{-k})$, $x^4 + k$ irreducible in $\mathbb{Q}[x]$, $1 \leq k \leq 10$.	178
4	Fundamental units of $O_{\mathbb{Q}(\sqrt{m})}$, $2 \leq m < 40$, m squarefree.	280
5	Nontrivial ideal class groups $H(\mathbb{Q}(\sqrt{k}))$, $-30 < k < 0$, k squarefree.	322
6	Nontrivial ideal class groups $H(\mathbb{Q}(\sqrt{k}))$, $2 \leq k < 100$, k squarefree.	323
7	Class numbers of imaginary quadratic fields $K = \mathbb{Q}(\sqrt{k})$, $-195 \leq k < 0$, k squarefree.	325
8	Class numbers of real quadratic fields $K = \mathbb{Q}(\sqrt{k})$, $0 < k \leq 197$, k squarefree.	326
9	Class numbers of $\mathbb{Q}(\sqrt[3]{k})$, $2 \leq k \leq 101$, k cubefree.	329
10	Class numbers of cyclotomic fields K_m , $3 \leq m \leq 45$, $m \not\equiv 2 \pmod{4}$.	331
11	Fundamental unit (> 1) of $\mathbb{Q}(\sqrt[3]{m})$ for a few values of $m \in \mathbb{N}$.	375
12	Fundamental unit of cubic fields K with exactly one real embedding and $-268 \leq d(K) < 0$.	376
13	Units of totally real cubic fields K with $0 < d(K) \leq 1101$.	377
14	Fundamental unit of some pure quartic fields $\mathbb{Q}(\sqrt[4]{-m})$.	378
15	Solutions $(x, y) \in \mathbb{Z}^2$ of $y^2 = x^3 + k$, $-20 \leq k < 0$.	402
16	Solutions $(x, y) \in \mathbb{Z}^2$ of $y^2 = x^3 + k$, $0 < k \leq 20$.	403

Cambridge University Press
978-0-521-83250-2 - Introductory Algebraic Number Theory
Şaban Alaca and Kenneth S. Williams
Frontmatter
[More information](#)

Notation

$\mathbb{N} = \{1, 2, 3, \dots\}$

$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$

\mathbb{Q} = field of rational numbers

\mathbb{R} = field of real numbers

\mathbb{C} = field of complex numbers

ϕ = empty set

$\left(\frac{m}{p}\right)$ = Legendre symbol = $\begin{cases} 1, & \text{if } p \nmid m \text{ and } x^2 \equiv m \pmod{p} \text{ is solvable,} \\ -1, & \text{if } p \nmid m \text{ and } x^2 \equiv m \pmod{p} \text{ is insolvable,} \\ 0, & \text{if } p \mid m, \end{cases}$

where $m \in \mathbb{Z}$ and p is a prime

$[x]$ = greatest integer less than or equal to the real number x

$\binom{m}{n}$ = binomial coefficient = $\frac{m!}{(m-n)!n!}$, where m and n are integers such that $0 \leq n \leq m$

If A is a set containing 0 then $A^* = A \setminus \{0\}$

\mathbb{Z}_n = cyclic group of order n

$\text{card}(S)$ = cardinality of the set S

O_n = $n \times n$ zero matrix

I_n = $n \times n$ identity matrix

$O_{r,s}$ = $r \times s$ zero matrix

Cambridge University Press
978-0-521-83250-2 - Introductory Algebraic Number Theory
Şaban Alaca and Kenneth S. Williams
Frontmatter
[More information](#)

Introduction

This book is intended as an introductory text for senior undergraduate and beginning graduate students wishing to learn the fundamentals of algebraic number theory. It is based upon a course in algebraic number theory given by the second author at Carleton University for more than thirty years. Keeping in mind that this is an introductory text, the authors have strived to present the material in as straightforward, clear, and elementary fashion as possible. Throughout the text many numerical examples are given to illustrate the theory. Each chapter closes with a set of exercises on the material covered in the chapter, as well as some suggested further reading. References cited in each chapter are listed under suggested reading. Biographical references for some of the mathematicians mentioned in the text are also given at the end of each chapter. For the convenience of the reader, the book concludes with page references for the definitions, theorems, and lemmas in the text. In addition an extensive bibliography of books on algebraic number theory is provided.

The main aim of the book is to present to the reader a detailed self-contained development of the classical theory of algebraic numbers. This theory is one of the crowning achievements of nineteenth-century mathematics. It came into being through the attempts of mathematicians of that century to prove Fermat's last theorem, namely, that the equation $x^n + y^n = z^n$ has no solutions in nonzero integers x, y, z , where n is an integer ≥ 3 . A wonderful achievement of the twentieth century was the proof of Fermat's last theorem by Andrew Wiles of Princeton University. Although the proof of Fermat's last theorem is beyond the scope of this book, we will show how algebraic number theory can be used to find the solutions in integers (if any) of other equations.

The contents of the book are divided into fourteen chapters. Chapter 1 serves as an introduction to the basic properties of integral domains. Chapters 2 and 3 are devoted to Euclidean domains and Noetherian domains respectively. In Chapter 4 the reader is introduced to algebraic numbers and algebraic integers. Algebraic number fields are introduced in Chapter 6 after a discussion of algebraic extensions of fields in Chapter 5. Chapter 7 is devoted to the study of integral bases. Minimal integers are introduced as a tool for finding integral bases and many numerical

examples are given. Chapter 8 is concerned with Dedekind domains. The ring of integers of an algebraic number field is the prototype of a Dedekind domain. Chapters 9 and 10 discuss the factorization of ideals into prime ideals. The structure of the unit group of a real quadratic field is determined in Chapter 11. In Chapter 12 the classic theorems of Minkowski in the geometry of numbers are proved and are used to show that the ideal class group is finite. Dirichlet's determination of the units in an arbitrary algebraic number field is presented in Chapter 13 using the approach given by van der Waerden. Finally, in Chapter 14, the algebraic number-theoretic tools developed in earlier chapters are used to discuss the solvability of certain equations in integers.

The prerequisites for this book are a basic course in linear algebra (systems of linear equations, vector spaces over a field), a basic course in modern algebra (groups, rings, and fields including Eisenstein's irreducibility criterion), and a basic course in elementary number theory (the Legendre symbol, quadratic residues, and the law of quadratic reciprocity.) No Galois theory is needed.

A possible outline for a one-semester course (three hours of lectures per week for twelve weeks) together with an approximate breakdown of lecture time is as follows:

Chapter 1 (excluding Theorem 1.2.2)	2 hours
Chapter 2 (excluding Sections 2.3, 2.4)	2 hours
Chapter 3	3 hours
Chapter 4	3 hours
Chapter 5	3 hours
Chapter 6	5 hours
Chapter 7 (Section 7.1 only)	3 hours
Chapter 8	3 hours
Chapter 9	3 hours
Chapter 10 (excluding Sections 10.4, 10.5, 10.6)	2 hours
Chapter 11	3 hours
Chapter 12 (excluding Section 12.7)	2 hours
Chapter 14 (Section 14.2 only)	2 hours

It is planned to provide solutions to selected questions, as well as corrections to any errors, on the website

<http://mathstat.carleton.ca/~williams/books.html>

or

<http://www.math.carleton.ca/~williams/books.html>.

The authors would like to thank their colleagues John D. Dixon, James G. Huard, Pierre Kaplan, Blair K. Spearman, and P. Gary Walsh for helpful suggestions in connection with the writing of this book. The second author would like to thank the many students who have taken the course Mathematics 70.436*/70.536 Algebraic Number Theory with him at Carleton University over the years. Special thanks go

Cambridge University Press
978-0-521-83250-2 - Introductory Algebraic Number Theory
Şaban Alaca and Kenneth S. Williams
Frontmatter
[More information](#)

Introduction

xvii

to the class of 2000–1 (Yaroslav Bezverkhnayev, Joanne Charlebois, Colette Haley, Mathieu Lemire, Rima Rahal, Fabien Roche, Tom Wiley, and Benjamin Young) for their suggestions for improvement to the preliminary draft of this book used in class. Finally, the authors would like to thank Austin Behne for his help in translating van der Waerden's paper on Dirichlet's unit theorem from German into English.