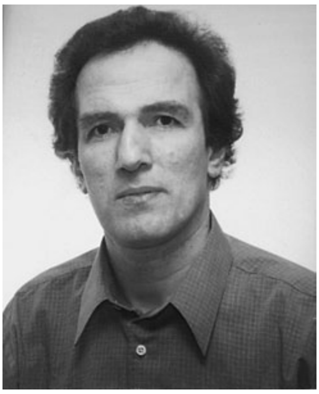
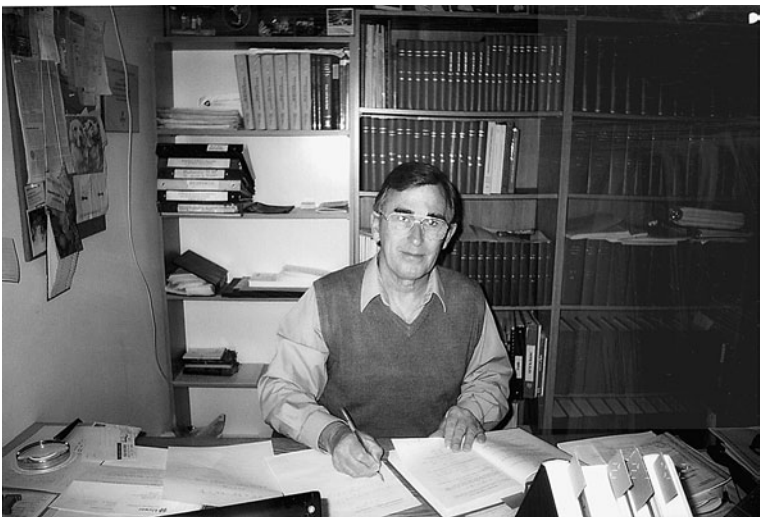
INTRODUCTORY ALGEBRAIC NUMBER THEORY

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

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE
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

© in this web service Cambridge University Press www.cambridge.org

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, Saban, 1964–
Introductory algebraic number theory / Saban 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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

Contents

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

© in this web service Cambridge University Press www.cambridge.org

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

List of Tables

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

Notation

$\mathbb{N} = \{1, 2, 3, \ldots\}$
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
$\mathbb{Q}$ = field of rational numbers
$\mathbb{R}$ = field of real numbers
$\mathbb{C}$ = field of complex numbers
ϕ = empty set

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

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 = $\dfrac{m!}{(m-n)!n!}$, where m and n are integers such that $0 \le n \le m$

If A is a set containing 0 then $A^* = A \setminus \{0\}$
$\mathbb{Z}_n$ = cyclic group of order n
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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

© in this web service Cambridge University Press www.cambridge.org

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

to the class of 2000–1 (Yaroslav Bezverkhnyev, 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.

© in this web service Cambridge University Press www.cambridge.org