Undergraduate Texts in Mathematics

Springer Science+Business Media, LLC

Undergraduate Texts in Mathematics

Anglin: Mathematics: A Concise History and Philosophy.
Readings in Mathematics.
Anglin/Lambek: The Heritage of Thales.
Readings in Mathematics.
Apostol: Introduction to Analytic Number Theory. Second edition.
Armstrong: Basic Topology.
Armstrong: Groups and Symmetry.
Axler: Linear Algebra Done Right.
Beardon: Limits: A New Approach to Real Analysis.
Bak/Newman: Complex Analysis. Second edition.
Banchoff/Wermer: Linear Algebra Through Geometry. Second edition.
Berberian: A First Course in Real Analysis.
Brémaud: An Introduction to Probabilistic Modeling.
Bressoud: Factorization and Primality Testing.
Bressoud: Second Year Calculus.
Readings in Mathematics.
Brickman: Mathematical Introduction to Linear Programming and Game Theory.
Browder: Mathematical Analysis: An Introduction.
Buskes/van Rooij: Topological Spaces: From Distance to Neighborhood.
Cederberg: A Course in Modern Geometries.
Childs: A Concrete Introduction to Higher Algebra. Second edition.
Chung: Elementary Probability Theory with Stochastic Processes. Third edition.
Cox/Little/O'Shea: Ideals, Varieties, and Algorithms. Second edition.
Croom: Basic Concepts of Algebraic Topology.
Curtis: Linear Algebra: An Introductory Approach. Fourth edition.
Devlin: The Joy of Sets: Fundamentals of Contemporary Set Theory. Second edition.
Dixmier: General Topology.
Driver: Why Math?
Ebbinghaus/Flum/Thomas: Mathematical Logic. Second edition.
Edgar: Measure, Topology, and Fractal Geometry.
Elaydi: Introduction to Difference Equations.
Exner: An Accompaniment to Higher Mathematics.
Fine/Rosenberger: The Fundamental Theory of Algebra.
Fischer: Intermediate Real Analysis.
Flanigan/Kazdan: Calculus Two: Linear and Nonlinear Functions. Second edition.
Fleming: Functions of Several Variables. Second edition.
Foulds: Combinatorial Optimization for Undergraduates.
Foulds: Optimization Techniques: An Introduction.
Franklin: Methods of Mathematical Economics.
Gordon: Discrete Probability.
Hairer/Wanner: Analysis by Its History.
Readings in Mathematics.
Halmos: Finite-Dimensional Vector Spaces. Second edition.
Halmos: Naive Set Theory.
Hämmerlin/Hoffmann: Numerical Mathematics.
Readings in Mathematics.
Hijab: Introduction to Calculus and Classical Analysis.
Hilton/Holton/Pedersen: Mathematical Reflections: In a Room with Many Mirrors.
Iooss/Joseph: Elementary Stability and Bifurcation Theory. Second edition.
Isaac: The Pleasures of Probability.
Readings in Mathematics.

(continued after index)

Rudolf Lidl Günter Pilz

Applied Abstract Algebra

Second Edition

With 112 illustrations

Springer

Rudolf Lidl
DVC Office
University of Tasmania
Launceston, Tasmania 7250
Australia

Günter Pilz
Institut für Mathematik
Universität Linz
A-4040 Linz
Austria

Mathematics Subject Classification (1991): 05-01, 06-01, 08-01, 12-01, 13-01, 16-01, 20-01, 68-01, 93-01

Library of Congress Cataloging-in-Publication Data
Lidl, Rudolf.
Applied abstract algebra / Rudolf Lidl, Günter Pilz. — 2nd ed.
p. cm. — (Undergraduate texts in mathematics)
Includes bibliographical references and index.
1. Algebra, Abstract. I. Pilz, Günter, 1945- . II. Title.
III. Series.
QA162.L53 1997 97-22883
512'.02—dc21

Printed on acid-free paper.

Originally published by Springer-Verlag New York in 1998.
Softcover reprint of the hardcover 2nd edition 1998

Production managed by Steven Pisano; manufacturing supervised by Joe Quatela.
Photocomposed by Integre Technical Publishing Co., Inc., Albuquerque, NM.

9 8 7 6 5 4 3 2 1

ISBN 978-1-4419-3117-7 ISBN 978-1-4757-2941-2 (eBook)
DOI 10.1007/978-1-4757-2941-2

To Pamela and Gerti

Preface

Algebra is beautiful. It is so beautiful that many people forget that algebra can be very useful as well. It is still the case that students who have studied mathematics quite often enter graduate studies or enter employment without much knowledge of the applicability of the algebraic structures they have studied.

The aim of this book is to convey to senior undergraduate students, graduate students, and lecturers/instructors the fact that concepts of abstract algebra encountered previously in a first algebra course can be used in many areas of applications. Of course, in order to apply algebra, we first need some theory which then can be applied. Hence we tried to blend the theory and its applications so that the reader can experience both parts.

This book assumes knowledge of the material covered in a course on linear algebra and, preferably, a first course in (abstract) algebra covering the basics of groups, rings, and fields, although this book will provide the necessary definitions and brief summaries of the main results that will be required from such a course in algebra.

This second edition includes major changes to the first edition, published in 1984: it contains corrections and, as we believe, substantial improvements to the first four chapters of the first edition. It includes a largely new chapter on Cryptology (Chapter 5) and an enlarged chapter on Applications of Groups (Chapter 6). An extensive Chapter 7 has been added to survey other (mostly quite recent) applications, many of which

were not included in the first edition. An interdependence chart of the material in the sections is presented below.

For a one-semester course (2–3 hours per week) on Applied Algebra or Discrete Mathematics, we recommend the following path: §§1, 2, 3, 4, 6–17, 21, 22, 23, and selected topics in Chapter 7 chosen by the instructor.

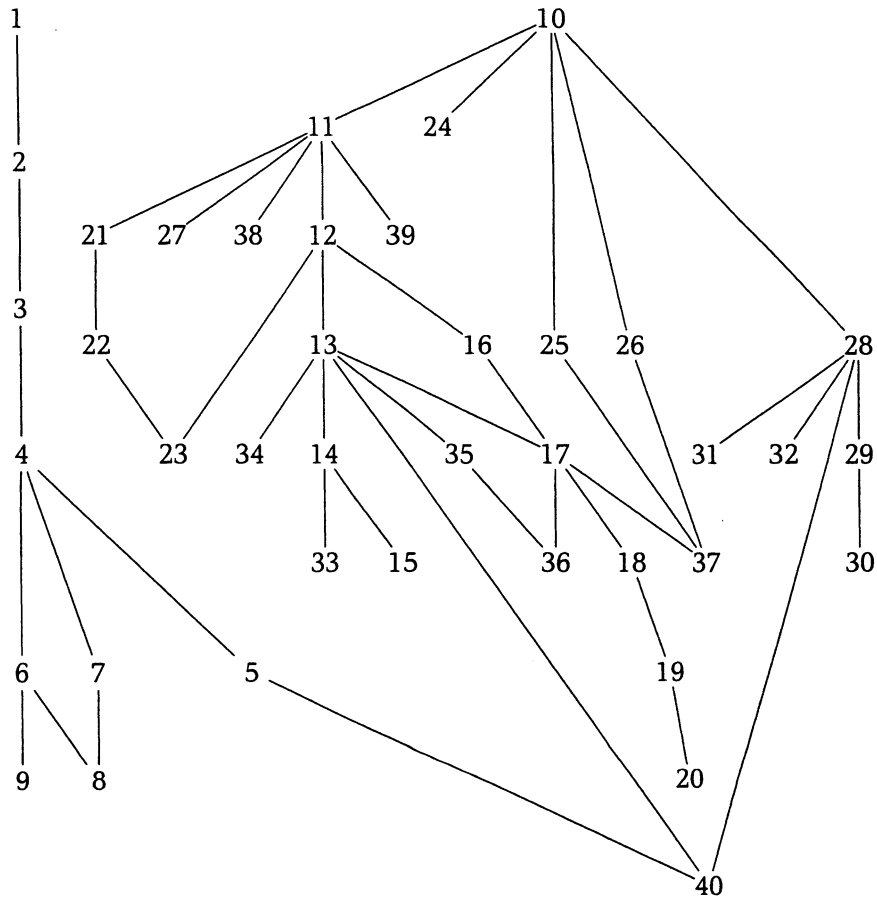
As in the first edition, we again emphasize the inclusion of worked-out examples and computational aspects in presenting the material. More than 500 exercises accompany the 40 sections. A separate solution manual for all these exercises is available from the publisher. The book also includes some historical notes and extensive references for further reading.

The text should be useful to mature mathematics students, to students in computer or information science with an interest and background knowledge in algebra, and to physical science or engineering students with a good knowledge in linear and some abstract algebra. Many of the topics covered are relevant to and have connections with computer science, computer algebra, physical sciences, and technology.

It is a great pleasure to acknowledge the assistance of colleagues and friends at various stages of preparing this second edition. Most of all, we would like to express our sincere appreciation to Franz Binder, who prepared many drafts and the final version of the entire book with LaTeX. Through his expertise in algebra, he was able to suggest many improvements and provided valuable information on many topics. Many useful suggestions and comments were provided by: E. Aichinger (Linz, Austria), G. Birkenmeier (Lafayette, Louisiana), J. Ecker (Linz, Austria), H. E. Heatherly (Lafayette, Louisiana), H. Kautschitsch (Klagenfurt, Austria), C. J. Maxson (College Station, Texas), W. B. Müller (Klagenfurt, Austria), G. L. Mullen (University Park, Pennsylvania), C. Nöbauer, P. Paule (Linz, Austria), A. P. J. Van der Walt (Stellenbosch, South Africa), and F. Winkler (Linz, Austria). Special thanks are due to L. Shevrin and I. O. Koryakov (Ekaterinenburg, Russia) for preparing a Russian translation of the first edition of our text. Their comments improved the text substantially. We also wish to thank Springer-Verlag, especially Mr. Thomas von Foerster, Mr. Steven Pisano, and Mr. Brian Howe, for their kind and patient cooperation.

October 1997 R.L. and G.P.

Interdependence Chart



Among the numerous general texts on algebra, we mention Birkhoff & MacLane (1977), Childs (1995), Herstein (1975), Jacobson (1985), and Lang (1984). Application-oriented books include Biggs (1985), Birkhoff & Bartee (1970), Bobrow & Arbib (1974), Cohen, Giusti & Mora (1996), Dorninger & Müller (1984), Fisher (1977), Gilbert (1976), Prather (1976), Preparata & Yeh (1973), Spindler (1994), and Stone (1973). A survey of the present "state of the art" in algebra is Hazewinkel (1996) (with several more volumes to follow). Historic notes on algebra can be found in Birkhoff (1976). Applications of linear algebra (which are not covered in this book) can be found in Goult (1978), Noble & Daniel (1977), Rorres & Anton (1984), and Usmani (1987). Lipschutz (1976) contains a large collection of Exercises. Good books on computational aspects ("Computer Algebra") include Geddes, Czapor & Labahn (1993), Knuth (1981), Lipson (1981), Sims (1984), Sims (1994), and Winkler (1996).

Contents

List of Symbols