Springer Undergraduate Mathematics Series

Advisory Board
M.A.J. Chaplain, *University of St. Andrews*
A. MacIntyre, *Queen Mary University of London*
S. Scott, *King's College London*
N. Snashall, *University of Leicester*
E. Süli, *University of Oxford*
M.R. Tehranchi, *University of Cambridge*
J.F. Toland, *University of Bath*

More information about this series at http://www.springer.com/series/3423

Gregory T. Lee

Abstract Algebra

An Introductory Course

Springer

Gregory T. Lee
Department of Mathematical Sciences
Lakehead University
Thunder Bay, ON
Canada

ISSN 1615-2085 ISSN 2197-4144 (electronic)
Springer Undergraduate Mathematics Series
ISBN 978-3-319-77648-4 ISBN 978-3-319-77649-1 (eBook)
https://doi.org/10.1007/978-3-319-77649-1

Library of Congress Control Number: 2018935845

Mathematics Subject Classification (2010): 20-01, 16-01, 12-01

© Springer International Publishing AG, part of Springer Nature 2018
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

In memory of my father

Preface

This book is intended for students encountering the beautiful subject of abstract algebra for the first time. My goal here is to provide a text that is suitable for you, whether you plan to take only a single course in abstract algebra, or to carry on to more advanced courses at the senior undergraduate and graduate levels. Naturally, I wish to encourage you to study the subject further and to ensure that you are prepared if you do so.

At many universities, including my own, abstract algebra is the first serious proof-based course taken by mathematics majors. While it is quite possible to get through, let us say, a course in calculus simply by memorizing a list of rules and applying them correctly, without really understanding why anything works, such an approach would be disastrous here. To be sure, you must carefully learn the definitions and the statements of theorems, but that is nowhere near sufficient. In order to master the material, you need to understand the proofs and then be able to prove things yourself. This book contains hundreds of problems, and I cannot stress strongly enough the need to solve as many of them as you can. Do not be discouraged if you cannot get all of them! Some are very difficult. But try to figure out as many as you can. You will only learn by getting your hands dirty.

As different universities have different sequences of courses, I am not assuming any prerequisites beyond the high school level. Most of the material in Part I would be covered in a typical course on discrete mathematics. Even if you have had such a course, I urge you to read through it. In particular, you absolutely must understand equivalence relations and equivalence classes thoroughly. (In my experience, many students have trouble with these concepts.) From time to time, throughout Parts II and III, some examples involving matrices or complex numbers appear. These can be bypassed if you have not studied linear algebra or complex numbers, but in any case, the material you need to know is not difficult and is discussed in the appendices. In Part IV, it is necessary to know some linear algebra, but all of the theorems used are proved in the text.

The fundamental results about groups are covered in Chaps. 3 and 4, those about rings are in Chaps. 8 and 9, and the introductory theorems concerning fields and polynomials are found in Chap. 11. I think that these chapters are essential in any course. Beyond that, there is a fair amount of flexibility in the choice of topics.

I confess my first encounter with abstract algebra was a joyous experience. I found (and still find!) the subject fascinating, and I will consider the time I put into this book well spent if you emerge with an appreciation for the field.

I would like to thank Lynn Brandon and Anne-Kathrin Birchley-Brun at Springer for their help in making this book a reality. Also, thanks to the reviewers for their many useful suggestions. I thank my wife and family for their ongoing support. Finally, thanks to my teacher, Prof. Sudarshan Sehgal, both for his advice concerning this book and for all of his help over the years.

Thunder Bay, ON, Canada Gregory T. Lee

Contents

Part I Preliminaries

1 Relations and Functions 3
1.1 Sets and Set Operations 3
1.2 Relations 5
1.3 Equivalence Relations 6
1.4 Functions 10

2 The Integers and Modular Arithmetic 15
2.1 Induction and Well Ordering 15
2.2 Divisibility 19
2.3 Prime Factorization 24
2.4 Properties of the Integers 26
2.5 Modular Arithmetic 27

Part II Groups

3 Introduction to Groups 35
3.1 An Important Example 35
3.2 Groups 38
3.3 A Few Basic Properties 42
3.4 Powers and Orders 44
3.5 Subgroups 48
3.6 Cyclic Groups 54
3.7 Cosets and Lagrange's Theorem 57

4 Factor Groups and Homomorphisms 61
4.1 Normal Subgroups 61
4.2 Factor Groups 65
4.3 Homomorphisms 69
4.4 Isomorphisms 72

4.5 The Isomorphism Theorems for Groups 78
4.6 Automorphisms 81

5 Direct Products and the Classification of Finite Abelian Groups 85
5.1 Direct Products 85
5.2 The Fundamental Theorem of Finite Abelian Groups 88
5.3 Elementary Divisors and Invariant Factors 93
5.4 A Word About Infinite Abelian Groups 97

6 Symmetric and Alternating Groups 101
6.1 The Symmetric Group and Cycle Notation 101
6.2 Transpositions and the Alternating Group 105
6.3 The Simplicity of the Alternating Group 108

7 The Sylow Theorems 115
7.1 Normalizers and Centralizers 115
7.2 Conjugacy and the Class Equation 119
7.3 The Three Sylow Theorems 122
7.4 Applying the Sylow Theorems 125
7.5 Classification of the Groups of Small Order 128

Part III Rings

8 Introduction to Rings 135
8.1 Rings 135
8.2 Basic Properties of Rings 138
8.3 Subrings 140
8.4 Integral Domains and Fields 142
8.5 The Characteristic of a Ring 146

9 Ideals, Factor Rings and Homomorphisms 149
9.1 Ideals 149
9.2 Factor Rings 152
9.3 Ring Homomorphisms 155
9.4 Isomorphisms and Automorphisms 159
9.5 Isomorphism Theorems for Rings 165
9.6 Prime and Maximal Ideals 167

10 Special Types of Domains 171
10.1 Polynomial Rings 171
10.2 Euclidean Domains 176
10.3 Principal Ideal Domains 182
10.4 Unique Factorization Domains 185
Reference 188

Part IV Fields and Polynomials

11 Irreducible Polynomials 191
11.1 Irreducibility and Roots 191
11.2 Irreducibility over the Rationals 195
11.3 Irreducibility over the Real and Complex Numbers 200
11.4 Irreducibility over Finite Fields 202
Reference 205

12 Vector Spaces and Field Extensions 207
12.1 Vector Spaces 207
12.2 Basis and Dimension 210
12.3 Field Extensions 215
12.4 Splitting Fields 221
12.5 Applications to Finite Fields 225
Reference 229

Part V Applications

13 Public Key Cryptography 233
13.1 Private Key Cryptography 233
13.2 The RSA Scheme 236

14 Straightedge and Compass Constructions 241
14.1 Three Ancient Problems 241
14.2 The Connection to Field Extensions 244
14.3 Proof of the Impossibility of the Problems 250

Appendix A: The Complex Numbers 253

Appendix B: Matrix Algebra 257

Solutions 263

Index 297