

Abstract Algebra with Applications

Abstract Algebra with Applications provides a friendly and concise introduction to algebra, with an emphasis on its uses in the modern world. The first part of this book covers groups, after some preliminaries on sets, functions, relations, and induction, and features applications such as public-key cryptography, Sudoku, the finite Fourier transform, and symmetry in chemistry and physics. The second part of this book covers rings and fields, and features applications such as random number generators, error-correcting codes, the Google page rank algorithm, communication networks, and elliptic curve cryptography.

The book's masterful use of colorful figures and images helps illustrate the applications and concepts in the text. Real-world examples and exercises will help students contextualize the information. Meant for a year-long undergraduate course in algebra for math, engineering, and computer science majors, the only prerequisites are calculus and a bit of courage when asked to do a short proof.

CAMBRIDGE MATHEMATICAL TEXTBOOKS

Cambridge Mathematical Textbooks is a program of undergraduate and beginning graduate-level textbooks for core courses, new courses, and interdisciplinary courses in pure and applied mathematics. These texts provide motivation with plenty of exercises of varying difficulty, interesting examples, modern applications, and unique approaches to the material.

ADVISORY BOARD

John B. Conway, *George Washington University*

Gregory F. Lawler, *University of Chicago*

John M. Lee, *University of Washington*

John Meier, *Lafayette College*

Lawrence C. Washington, *University of Maryland, College Park*

A complete list of books in the series can be found at

www.cambridge.org/mathematics

Recent titles include the following:

Chance, Strategy, and Choice: An Introduction to the Mathematics of Games and Elections, S. B. Smith

Set Theory: A First Course, D. W. Cunningham

Chaotic Dynamics: Fractals, Tilings, and Substitutions, G. R. Goodson

A Second Course in Linear Algebra, S. R. Garcia & R. A. Horn

Introduction to Experimental Mathematics, S. Eilers & R. Johansen

Exploring Mathematics: An Engaging Introduction to Proof, J. Meier & D. Smith

A First Course in Analysis, J. B. Conway

Introduction to Probability, D. F. Anderson, T. Seppäläinen & B. Valkó

Linear Algebra, E. S. Meckes & M. W. Meckes

A Short Course in Differential Topology, B. I. Dundas

Abstract Algebra with Applications

AUDREY TERRAS

University of California, San Diego, CA, USA



CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

79 Anson Road, #06–04/06, Singapore 079906

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/9781107164079

© Audrey Terras 2019

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 2019

Printed and bound in Great Britain by Clays Ltd, Elcograf S.p.A.

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

ISBN 978-1-107-16407-9 Hardback

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.

To the bears and koalas

Contents

<i>List of Figures</i>	ix
<i>Preface</i>	xiii

PART I GROUPS

1 Preliminaries	3
1.1 Introduction	3
1.2 Sets	6
1.3 The Integers	9
1.4 Mathematical Induction	14
1.5 Divisibility, Greatest Common Divisor, Primes, and Unique Factorization	19
1.6 Modular Arithmetic, Congruences	26
1.7 Relations	30
1.8 Functions, the Pigeonhole Principle, and Binary Operations	34
2 Groups: A Beginning	43
2.1 What is a Group?	43
2.2 Visualizing Groups	52
2.3 More Examples of Groups and Some Basic Facts	56
2.4 Subgroups	64
2.5 Cyclic Groups are Our Friends	72
3 Groups: There's More	81
3.1 Groups of Permutations	81
3.2 Isomorphisms and Cayley's Theorem	89
3.3 Cosets, Lagrange's Theorem, and Normal Subgroups	93
3.4 Building New Groups from Old, I: Quotient or Factor Groups G/H	98
3.5 Group Homomorphism	102
3.6 Building New Groups from Old, II: Direct Product of Groups	108
3.7 Group Actions	114
4 Applications and More Examples of Groups	124
4.1 Public-Key Cryptography	124
4.2 Chemistry and the Finite Fourier Transform	129
4.3 Groups and Conservation Laws in Physics	135
4.4 Puzzles	142
4.5 Small Groups	146

PART II RINGS

5	Rings: A Beginning	157
5.1	Introduction	157
5.2	What is a Ring?	158
5.3	Integral Domains and Fields are Nicer Rings	166
5.4	Building New Rings from Old: Quotients and Direct Sums of Rings	173
5.5	Polynomial Rings	180
5.6	Quotients of Polynomial Rings	185
6	Rings: There's More	189
6.1	Ring Homomorphisms	189
6.2	The Chinese Remainder Theorem	193
6.3	More Stories about $F[x]$ Including Comparisons with \mathbb{Z}	198
6.4	Field of Fractions or Quotients	202
7	Vector Spaces and Finite Fields	206
7.1	Matrices and Vector Spaces over Arbitrary Fields and Rings like \mathbb{Z}	206
7.2	Linear Functions or Mappings	218
7.3	Determinants	224
7.4	Extension Fields: Algebraic versus Transcendental	229
7.5	Subfields and Field Extensions of Finite Fields	233
7.6	Galois Theory for Finite Fields	239
8	Applications of Rings	244
8.1	Random Number Generators	244
8.2	Error-Correcting Codes	256
8.3	Finite Upper Half Planes and Ramanujan Graphs	265
8.4	Eigenvalues, Random Walks on Graphs, and Google	272
8.5	Elliptic Curve Cryptography	282
	<i>References</i>	299
	<i>Index</i>	305

Figures

0.1	Benzene C_6H_6	xiv
0.2	Photoshopped flower	xiv
0.3	Hibiscus in Kauai	xiv
0.4	Picture with symmetry coming from the action of 2×2 matrices with nonzero determinant and elements in a finite field with 11 elements	xv
1.1	Intersection and union of square A and heart B	7
1.2	Cartesian product $[0, 1] \times \{2\}$	8
1.3	$[0, 1]^3$	8
1.4	Graph representing the hypercube $[0, 1]^4$	9
1.5	Integers on the line – only even ones are labelled	13
1.6	The first principle of mathematical induction. A penguin surveys an infinite line of equally spaced dominos. If the n th domino is close enough to knock over the $(n + 1)$ th domino, then once the penguin knocks over the first domino, they should all fall over	14
1.7	Here is an attempt to picture the second mathematical induction principle in which we arrange dominos so that various numbers of dominos are needed to knock over the dominos to their left. In this picture step 1 would be for the penguin to knock over d_1 and d_2	17
1.8	A color is placed at the (m, n) entry of a 101×101 matrix according to the value of $\gcd(m, n)$. This is an ArrayPlot in Mathematica	25
1.9	Rolling up the integers modulo 3	27
1.10	Mathematica picture of the $x < y$ relation for the integers between 1 and 50	31
1.11	Mathematica picture of the $y x$ relation for the integers between 1 and 50	31
1.12	Mathematica picture of the $x \equiv y \pmod{5}$ relation for the integers between 1 and 50	32
1.13	Poset diagram of the positive divisors of 24	34
1.14	The pigeonhole principle	39
2.1	The symmetries of a regular triangle are pictured	44
2.2	Part of a design with translational symmetry which should be imagined to stretch out to ∞ and $-\infty$	47
2.3	A figure with C_8 symmetry – not D_8 symmetry	48
2.4	Art from the Raja Ampat islands in the Indonesian part of New Guinea	48
2.5	Wallpaper from a Fourier series in two variables	50
2.6	Spherical wallpaper from spherical harmonics	51
2.7	Hyperbolic wallpaper from a modular form known as Δ on the upper half plane – a function with an invariance property under fractional linear transformation $(az + b)/(cz + d)$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$	51

2.8	Group Explorer version of the multiplication table for C_6 , a cyclic group of order 6	52
2.9	Group Explorer version of the multiplication table for D_3 (alias S_3) with our upper case R and F replaced by lower case letters	52
2.10	Cayley graph of cyclic group $G = \langle a \rangle$ of order 6 with generating set $S = \{a\}$	53
2.11	Cayley graph of D_3 with generating set $\{R, F\}$. Our upper case letters are replaced by lower case in the diagram. If there are arrows in both directions on an edge, we omit the arrows	53
2.12	Undirected version of Cayley graph for $C_6 = \langle a \rangle$, generating set $S = \{a, a^{-1}\}$	53
2.13	Cayley graph of $C_6 = \langle a \rangle$, generating set $S = \{a, a^3, a^5\}$	53
2.14	Group Explorer version of the multiplication table for the Klein 4-group	54
2.15	Symmetrical designs	54
2.16	The Platonic solids	57
2.17	Poset diagram for subgroups of D_3 as defined in (2.8)	68
2.18	The Group Explorer version of the multiplication table for a cyclic group of order 10	73
2.19	Cayley graph $X(\langle a \rangle, \{a, a^{-1}\})$ for a cyclic group $\langle a \rangle$ of order 10	76
2.20	A less boring picture of a 10-cycle	76
2.21	Poset diagram of the subgroups of \mathbb{Z}_{24} under addition	78
2.22	Cycle diagram in the multiplicative group \mathbb{Z}_{15}^*	80
3.1	Tetrahedron	87
3.2	On the left is the Cayley graph for the Klein 4-group $K_4 = \{e, h, v, hv\}$, with generating set $S = \{h, v\}$ using the notation of Figure 2.14. On the right is the Schreier graph for K_4/H , where $H = \{e, h\}$, with the same set $S = \{h, v\}$	97
3.3	Roll up \mathbb{Z} to get $\mathbb{Z}/n\mathbb{Z}$	105
3.4	Roll up the real line to get a circle $\mathbb{T} \cong \mathbb{R}/\mathbb{Z}$	106
3.5	Cayley graph for $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ with the generating set $\{(1, 0), (0, 1)\}$ and bears at the vertices	109
3.6	Cayley graph for $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ with the generating set $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ and koalas at the vertices	109
3.7	Cayley graph for $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ with the generating set $\{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\}$	110
3.8	A finite torus, which is the Cayley graph $X(\mathbb{Z}_{10} \oplus \mathbb{Z}_5, \{(\pm 1, 0), (0, \pm 1)\})$	111
3.9	The continuous torus (obtained from the plane modulo its integer points; i.e., $\mathbb{R} \oplus \mathbb{R}$ modulo $\mathbb{Z} \oplus \mathbb{Z}$)	111
3.10	Cayley graph for the quaternion group with generating set $\{\pm i, \pm j\}$	113
3.11	The 13 necklaces with six beads of two colors	121
3.12	The dodecahedron graph drawn by Mathematica	122
3.13	The cuboctahedron drawn by Mathematica	123
4.1	Vibrating system of two masses	142
4.2	Group Explorer's multiplication table for the semi-direct product $C_3 \rtimes C_4$	149
4.3	Group Explorer draws the Cayley graph $X(C_3 \rtimes C_4, \{a, b\})$	149
4.4	The Cayley graph $X(\text{Aff}(5), S_{1,2})$, with generating set defined by equation (4.16), has edges given by solid green lines while the dashed magenta lines are the edges of a dodecahedron	150

List of Figures

xi

4.5	Butterfly from Cayley graph of $\text{Heis}(\mathbb{Z}/169\mathbb{Z})$	151
4.6	A spanning tree for the tetrahedron graph is indicated in solid fuchsia lines. Since the three dashed purple edges are left out, the fundamental group of the tetrahedron graph is the free group on three generators. The arrows show a closed path on the tetrahedron graph	153
4.7	The bouquet of three loops obtained by collapsing the tree in the tetrahedron graph of Figure 4.6 to point a	153
4.8	A passion flower	154
5.1	The color at point $(x, y) \in \mathbb{Z}_{163}^2$ indicates the value of $x^2 + y^2 \pmod{163}$	157
5.2	Points (x, y) , for $x, y \in \mathbb{Z}_{11^2}, y \neq 0$, have the same color if $z = x + y\sqrt{\delta}$ are equivalent under the action of non-singular 2×2 matrices $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries in \mathbb{Z}_{11} . The action of g on z is by fractional linear transformation $z \rightarrow (az + b)/(cz + d) = gz$. Here δ is a fixed non-square in the field \mathbb{F}_{121} with 121 elements	158
5.3	Poset diagram of the ideals in \mathbb{Z}_{12}	178
5.4	A feedback shift register diagram corresponding to the finite field $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ and the multiplication table given in the text	186
6.1	The Cayley graph $X(\mathbb{Z}_{15}, \{\pm 1 \pmod{15}\})$	196
6.2	The Cayley graph $X(\mathbb{Z}_{15}, \{5, 6, 9, 10 \pmod{15}\})$	196
7.1	The poset of subfields of $\mathbb{F}_{2^{24}}$	234
8.1	The Cayley graph $X(\mathbb{Z}_{17}^*, \{3 \pmod{17}\})$	245
8.2	The same graph as in Figure 8.1 except that now the vertices are given the usual ordering $1, 2, 3, 4, \dots, 16$	245
8.3	Plot of points $P_j = (j, v_j)$ whose second component is the real number $\frac{1}{499}$ times $7^j \pmod{499}$, identifying $7^j \pmod{499}$ as an integer between 1 and 498	248
8.4	Plot of points $P_j = (v_j, v_{j+1})$ whose first component is the real number $\frac{1}{499}$ times $7^j \pmod{499}$, identifying $7^j \pmod{499}$ as an integer between 1 and 498	248
8.5	Plot of points $P_j = (v_j, v_{j+1}, v_{j+2})$ whose first component is the real number $\frac{1}{499}$ times $7^j \pmod{499}$, identifying $7^j \pmod{499}$ as an integer between 1 and 498	249
8.6	Plot of points $P_j = (v_j, w_j)$ whose first component is the real number $\frac{1}{499}$ times $7^j \pmod{499}$, identifying $7^j \pmod{499}$ as an integer between 1 and 498 and whose second component is the analog with 499 replaced with 503	249
8.7	Points (v_i, w_i, z_i) from three vectors v, w, z formed from powers of generators of \mathbb{F}_p^* for $p = 499, 503$, and 521 , respectively	250
8.8	Feedback shift register corresponding to example 2	252
8.9	Sending a message of 0s and 1s to Professor Bolukxy on the planet Xotl	257
8.10	The matrix H_{32} where the 1s and -1 s have become red and purple	263
8.11	Color at point $z = x + y\sqrt{\delta}$ in H_{163} is found by computing the Poincaré distance $d(z, \sqrt{\delta})$	268
8.12	The graph on the left is $X_3(-1, 1)$, an octahedron, and that on the right is $X_5(2, 1)$ with the edges in green. The pink dashed lines on the right are the dodecahedron	269
8.13	Another version of Figure 5.2	270

8.14	A random walk on a pentagon. At time $t=0$, the big penguin is at vertex 1. At time $t=1$ the penguin has probability $\frac{1}{2}$ of being at vertex 2 and probability $\frac{1}{2}$ of being at vertex 5. So the penguins at these vertices are half size	275
8.15	Surfing a very small web	277
8.16	Real points (x, y) on the elliptic curve $y^2 = x^3 + x^2$	282
8.17	Real points (x, y) on the elliptic curve $y^2 = x^3 - x + 1$	283
8.18	Real points (x, y) on the elliptic curve $y^2 = x^3 - x$	283
8.19	Addition $A + B = C$ on the elliptic curve $y^2 = x^3 - x$ over \mathbb{R}	286
8.20	The rational points on the curve $y^2 + y = x^3 - x^2$ are a, b, c, d and the point at ∞	287
8.21	The pink squares indicate the points (x, y) on the elliptic curve $y^2 = x^3 - x + 1 \pmod{59}$. Points marked are: $A = (15, 36), B = (22, 40), C = (32, 46)$, with $A + B = -C = (32, 13)$	289
8.22	Level “curves” of $y^2 - x^3 - x + 1 \pmod{29}$	296
8.23	Smoothed level “curves” of $y^2 - x^3 - x + 1 \pmod{29}$	297
8.24	A photoshopped version of the level curves of $(y + 2x)^4 + (x - 2y)^4 \pmod{101}$	297