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.

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

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

To the bears and koalas

Contents

PART II RINGS

Figures

Preface

My goal for this book is to provide a friendly concise introduction to algebra with emphasis on its uses in the modern world – including a little history, concrete examples, and visualization. Beyond explaining the basics of the theory of groups, rings, and fields, I aim to give many answers to the question: What is it good for?" The standard undergraduate mathematics course in the 1960s (when I was an undergraduate) proceeded from Definition 1.1.1 to Corollary 14.5.59 with little room for motivation, examples, history, and applications. I plan to stay as far as possible from that old format, modeling my discussion on G. Strang's book [115], where the preface begins: "I believe that the teaching of linear algebra has become too abstract." My feeling is that the teaching of modern algebra (the non-linear part) has become even more abstract. I will attempt to follow Strang's lead and treat modern algebra in a way that will make sense to a large variety of students. On the other hand, the goal is to deal with some abstractions – groups, rings, and such things. Yes, it is abstraction and generalization that underlies the power of mathematics. Thus there will be some conflict between the applied and pure aspects of our subject.

The book is intended for a year-long undergraduate course in algebra. The intended audience is the less theoretically inclined undergraduates majoring in mathematics, the physical and social sciences, or engineering – including those in applied mathematics or those intending to get a teaching credential.

The prerequisites are minimal: comfort with the real numbers, the complex numbers, matrices, vector spaces at the level of calculus courses – and a bit of courage when asked to do a short proof.

In this age of computers, algebra may have replaced calculus (analysis) as the most important part of mathematics. For example:

1. Error-correcting codes are built into the DVD player and the computer. Who do you call to correct errors? The algebraist, that's who!
2. Digital signal processing (such as that involved in medical scanners, weather prediction, the search for oil) is dominated by the fast Fourier transform or FFT. What is this? The FFT is a finite sum whose computation has been sped up considerably by an algebra trick which goes back to Gauss in 1805. Once more algebra, not analysis, rules.
3. In chemistry and physics, one studies structures with symmetry such as the benzene molecule (C_6H_6) depicted in Figure 0.1. What does the 6-fold symmetry have to do with the properties of benzene? Group theory is the tool one needs for this.
4. The search for secret codes – cryptography. Much of the modern world – particularly that which lives on the internet – depends on these codes being secure. But are they? We will consider public-key codes. And who do you call to figure out these codes? An algebraist!

5. The quest for beauty in art and nature. I would argue that symmetry groups are necessary tools for this quest. See Figures 0.2–0.4.

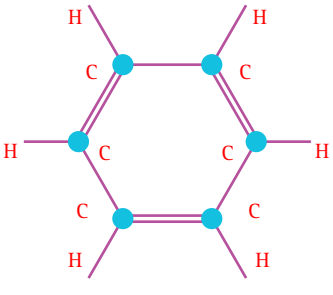

Figure 0.1 Benzene C_6H_6

Figure 0.2 Photoshopped flower

Figure 0.3 Hibiscus in Kauai

Our goal here is to figure out enough group and ring theory to understand many of these applications. And we should note that both algebra and analysis are necessary for the applications. In fact, we shall see some limits, derivatives, and integrals before the last pages of this book. You can skip all the applications if you just want to learn the basics

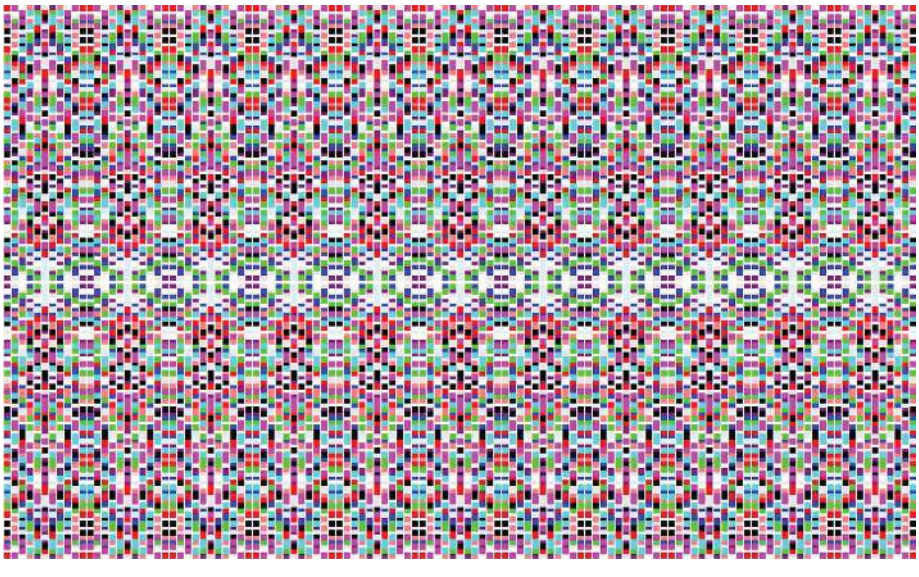

Figure 0.4 Picture with symmetry coming from the action of 2×2 matrices with nonzero determinant and elements in a finite field with 11 elements

of modern algebra. The non-applied sections are all independent of those on applications. However, you would be missing one of the big reasons that the subject is taught. And feel free to skip any applied sections you want to skip – or to add any missing application that you want to understand.

The first part of this book covers groups, after some preliminaries on sets, functions, relations, the integers, and mathematical induction. Of course every calculus student is familiar with the group of real numbers under addition and similarly with the group of nonzero real numbers under multiplication. We will consider many more examples – favorites being finite groups such as the group of symmetries of an equilateral triangle.

Much of our subject began with those favorite questions from high school algebra such as finding solutions to polynomial equations. It took methods of group theory to know when the solutions could not be found in terms only of nth roots. Galois, who died at age 21 in a duel in 1832, laid the foundations to answer such questions by looking at groups of permutations of the roots of a polynomial. These are now called Galois groups. See Edna E. Kramer [59, Chapter 16] or Ian Stewart [114] for some of the story of Galois and the history of algebra. Another reference for stories about Galois and the many people involved in the creation of this subject is *Men of Mathematics* by Eric Temple Bell [8]. This book is often criticized for lack of accuracy, but it is more exciting than most. I found it inspirational as an undergraduate – despite the title.

Another area that leads to our subject is number theory: the study of the ring of integers

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}.$$

The origins of this subject go back farther than Euclid's *Elements*. Euclid lived in Alexandria around 300 BC and his book covers more than the plane geometry we learned in high school. Much of the basic theory of the integers which we cover in Chapter 1 is to be found in Euclid's *Elements*. Why is it that the non-plane geometry part of Euclid's *Elements* does not seem to be taught in high school?

Polynomial equations with integer coefficients are often called Diophantine equations in honor of Diophantus who also lived in Alexandria, but much later (around AD 200). Yes, algebra is an old subject and one studied in many different countries. For example, the name "algebra" comes the word *al-jabr*, one of the two operations used to solve quadratic equations by the Persian mathematician and astronomer Mohamed ibn Musa al-Khwārizmī, who lived around AD 800.

A large part of this subject was created during many attempts to prove Fermat's last theorem. This was a conjecture of Pierre de Fermat in 1637 stating that the equation $x^n + y^n = z^n$ can have no integer solutions x, y, z with $xyz \neq 0$ and $n > 2$. Fermat claimed to have a proof that did not fit in the margin of the book in which he wrote this conjecture. People attempted to prove this theorem without success until A. Wiles with the help of R. Taylor in 1995. People still seek an "elementary" proof.

Groups are sets with one operation satisfying the axioms to be listed in Section 2.1. After the basic definitions, we consider examples of small groups. We will visualize groups using Cayley graphs and various other diagrams such as Hasse or poset diagrams as well as cycle diagrams. Other topics of study include subgroups, cyclic groups, permutation groups, functions between groups preserving the group operations (homomorphisms), cosets of subgroups, building new groups whose elements are cosets of normal subgroups, direct products of groups, actions of groups on sets. We will consider such applications as public-key cryptography, the finite Fourier transform, and the chemistry of benzene. Favorite examples of groups include cyclic groups, permutation groups, symmetry groups of the regular polygons, matrix groups such as the Heisenberg group of 3×3 upper triangular matrices with real entries and 1 on the diagonal, the group operation being matrix multiplication.

The second part of this book covers rings and fields. Rings have two operations satisfying the axioms listed in Section 5.2. We denote the two operations as addition $+$ and multiplication $*$ or $\cdot$. The identity for addition is denoted 0. It is NOT assumed that multiplication is commutative: that is, it is not assumed that $ab = ba$. If multiplication is commutative, then the ring is called commutative. A field F is a commutative ring with an identity for multiplication (called $1 \neq 0$) such that the nonzero elements of F form a multiplicative group. Most of the rings considered here will be commutative. We will be particularly interested in finite fields like the field of integers modulo p, $\mathbb{Z}/p\mathbb{Z}$ where p is prime. You must already be friends with the field $\mathbb{Q}$ of rational numbers – fractions with integer numerator and nonzero integer denominator. And you know the field $\mathbb{R}$ of real numbers from calculus: that is, limits of Cauchy sequences of rationals. We are not supposed to say the word "limit" as this is algebra. So we will not talk about constructing the field of real numbers $\mathbb{R}$. Ring theory topics include: definitions and basic properties of rings, fields, ideals, and functions between rings which preserve the ring operations (ring homomorphisms). We will also build new rings (quotient rings) whose elements are cosets $x + I$ of an ideal I in ring R, for x in ring R. Note that here R is an arbitrary ring, not necessarily the field of real numbers. We will look at rings of polynomials and their similarity to the ring of integers. We can do linear algebra for finite-dimensional vector spaces over arbitrary fields in a similar way to the linear algebra that is included in calculus sequences. Our favorite rings are the ring $\mathbb{Z}$ of integers and the quotient ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n, in which x, is identified with all integers of the form $x + nk$, for integer k. Another favorite is the ring of Hamilton quaternions which is isomorphic to four-dimensional space over the real numbers with basis $1, i, j, k$ and with multiplication defined by $ij = k = -ji$, $i^2 = j^2 = k^2 = -1$.

Historically, much of our subject came out of number theory and the desire to prove Fermat's last theorem by knowing about factorization into irreducibles in rings like $\mathbb{Z}\left[\sqrt{m}\right] = \left\{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\right\}$, where m is a non-square integer. For example, it turns out that, when $m = -5$, we have two different factorizations:

$$2 \cdot 3 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right).$$

So the fundamental theorem of arithmetic – true for $\mathbb{Z}$ as is shown in Section 1.5 – is false for $\mathbb{Z}\left[\sqrt{-5}\right]$.

Assuming that such factorizations were unique, Lamé thought that he had proved Fermat's last theorem in 1847. Dedekind fixed up arithmetic in such rings by developing the arithmetic of ideals, which are certain sets of elements of the ring to be considered in Section 5.4. One then had (at least in rings of integers in algebraic number fields) unique factorization of ideals as products of prime ideals, up to order. Of course, Lamé's proof of Fermat's last theorem was still invalid (lame – sorry for that).

The favorite field of the average human mathematics student is the field of real numbers $\mathbb{R}$. A favorite finite field for a computer is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where $p =$ prime. Of course you can define $\mathbb{Z}/n\mathbb{Z}$, for any positive integer n, but you only get a ring and not a field if n is not a prime. We consider $\mathbb{Z}/n\mathbb{Z}$ as a group under addition in Section 1.6. In Chapter 5 we view it as a ring with two operations, addition and multiplication.

Finite rings and fields were really invented by Gauss (1801) and earlier Euler (1750). Galois and Abel worked on field theory to figure out whether nth degree polynomial equations are solvable with equations involving only radicals $\sqrt[m]{a}$. In fact, finite fields are often called "Galois fields."

The terminology of algebra was standardized by mathematicians such as Richard Dedekind and David Hilbert in the late 1800s. Much of abstract ring theory was developed in the 1920s by Emmy Noether. Discrimination against both women and Jews made it hard for her to publish. The work became well known thanks to B. L. Van der Waerden's two volumes [124] on modern algebra. Van der Waerden wrote these books after studying with Emmy Noether in 1924 in Göttingen. He had also heard lectures of Emil Artin in Hamburg earlier. See Edna E. Kramer [59] for more information on Noether and the other mathematicians who developed the view of algebra we are aiming to present.

The abstract theory of algebras (which are special sorts of rings) was applied to group representations by Emmy Noether in 1929. This has had a big impact on the way people do harmonic analysis, number theory, and physics. In particular, certain adelic group representations are central to the Wiles proof of Fermat's last theorem.

It would perhaps shock many pure mathematics students to learn how much algebra is part of the modern world of applied mathematics – both for good and ill. Google's motto: "Don't be evil," has not always been the motto of those using algebra. Of course, the Google search engine itself is a triumph of modern linear algebra, as we shall see.

We will consider many applications of rings in Chapter 8. Section 8.1 concerns random number generators from finite rings and fields. These are used in simulations of natural phenomena. In prehistoric times like the 1950s sequences of random numbers came from tables like that published by the Rand corporation. Random numbers are intrinsic to Monte Carlo methods. These methods were named for a casino in Monaco by J. von Neumann and S. Ulam in the 1940s while working on the atomic bomb. Monte Carlo methods are useful in computational physics and chemistry (e.g., modeling the behavior of galaxies, weather on earth), engineering (e.g., simulating the impact of pollution), biology (simulating

the behavior of biological systems such as a cancer), statistics (hypothesis testing), game design, finance (e.g., to value options, analyze derivatives – the very thing that led to the horrible recession/depression of 2008), numerical mathematics (e.g., numerical integration, stochastic optimization), and the gerrymandering of voting districts.

In Section 8.2 we will show how the finite field with two elements and vector spaces over this field lead to error-correcting codes. These codes are used in DVDs and in the transmission of information between a Mars spacecraft and NASA on the earth. Section 8.3 concerns (among other things) the construction of Ramanujan graphs which can provide efficient communication networks.

Section 8.4 gives applications of the eigenvalues of matrices to Googling. Section 8.5 gives applications of elliptic curves over finite fields to cryptography.

The rush to abstraction of twentieth-century mathematics has had some odd consequences. One of the results of the abstract ring theory approach was to create such an abstract version of Fourier analysis that few can figure out what is going on. A similar thing has happened in number theory. On the other hand, modern algebra has often made it easier to see the forest for the trees by simplifying computations, removing subsubscripts, doing calculations once in the general case rather than many times, once for each example.

The height of abstraction was achieved in the algebra books of Nicolas Bourbaki (really a group of French mathematicians). I am using the Bourbaki notation for the fields of real numbers, complex numbers, rational numbers, and the ring of integers. But Bourbaki seems to have disliked pictures as well as applications. I do not remember seeing enough examples or history when I attempted to read Bourbaki's *Algebra* as an undergrad. In an interview, one of the members of Bourbaki, Pierre Cartier (see Marjorie Senechal [102]) said: "The Bourbaki were Puritans, and Puritans are strongly opposed to pictorial representations of truths of their faith." More information on Bourbaki as well as other fashions in mathematics can be found in Edna E. Kramer's history book [59]. She also includes a brief history of women in mathematics as well as the artificial separation between pure and applied mathematics.

As I said in my statement of goals, I will attempt to be as non-abstract as possible in this book and will seek to draw pictures in a subject where few pictures ever appear. I promise to give examples of every concept, but hope not to bury the reader in examples either, since I do aim for brevity. As I am a number theorist interested in matrix groups, there will be lots of numbers and matrices. Each chapter will have many exercises. It is important to do them – or as many of them as you can. Some exercises will be needed later in the book. The answers (mostly sketchy outlines) to odd-numbered exercises will be online hopefully. See my website. There may also be hints on others. No proof is intended to be very long. The computational problems might be slightly longer and sometimes impossible without the help of a computer. I will be using Mathematica, Scientific Workplace, and Group Explorer to help with computations.

Suggestions for Further Reading

A short list of possible references is: Garrett Birkhoff and Saunders Maclane [9], Larry L. Dornhoff and Franz E. Hohn [25], David S. Dummit and Richard M. Foote [28], Gertrude Ehrlich [29], John B. Fraleigh [32], Joseph A. Gallian [33], William J. Gilbert and W. Keith Nicholson [35], Israel N. Herstein [42], Audrey Terras [116]. There is also a free program: Group Explorer, which you can download and use to explore small groups. Another free but harder to use program is SAGE. I will be using Mathematica and Scientific Workplace. The Raspberry Pi computer ($35) comes with Mathematica (and not much else). There are many

books on line as well. One example is Judson [50]. It includes computer exercises using SAGE. An on line group theory book making use of the Group Explorer program is that of Carter [12]. Wikipedia is often very useful – or just asking Google to answer a question. It is easier to be a student now than it was in my time – thanks to the multitude of resources to answer questions. On the other hand, it was nice just to have the one small book – in my case, Birkhoff and Maclane [9] – to deal with. And – perhaps needless to say – online sources can lie. Even the computer can lie – witness the arithmetic error in the Pentium chip that was revealed by number theorists' computations in the 1990s. But I have found that Wikipedia is usually very useful in its discussions of undergraduate mathematics, as is the mathematical software I have used.

It is often enlightening to look at more than one reference. Where something is mumbled about in one place, that same thing may be extremely clearly explained in another. Also feel free to read a book in a non-linear manner. If you are interested in a particular result or application, start there.

Acknowledgments

I should thank the Mathematical Sciences Research Institute, Berkeley, for support during the writing of some of this book, as well as the students in my applied algebra courses at the University of California, San Diego.