Algebra

From *rings* to *modules* to *groups* to *fields*, this undergraduate introduction to abstract algebra follows an unconventional path. The text emphasizes a modern perspective on the subject, with gentle mentions of the unifying categorical principles underlying the various constructions and the role of universal properties. A key feature is the treatment of *modules*, including a proof of the classification theorem for finitely generated modules over Euclidean domains. Noetherian modules and some of the language of exact complexes are introduced. In addition, standard topics—such as the Chinese Remainder Theorem, the Gauss Lemma, the Sylow Theorems, simplicity of alternating groups, standard results on field extensions, and the Fundamental Theorem of Galois Theory—are all treated in detail. Students will appreciate the text's conversational style, 400+ exercises, appendix with complete solutions to around 150 of the main text problems, and appendix with general background on basic logic and naïve set theory.

Paolo Aluffi is Professor of Mathematics at Florida State University. Aluffi earned a Ph.D. from Brown University with a dissertation on the enumerative geometry of plane cubic curves, under the supervision of William Fulton. His research interests are in algebraic geometry, particularly intersection theory and its application to the theory of singularities and connections with theoretical physics. He has authored about 70 research publications and given lectures on his work in 15 countries. Beside *Notes from the Underground*, he has published a graduate-level textbook in algebra (*Algebra: Chapter 0*, AMS) and a mathematics book for the general public, in Italian (*Fare matematica*, Aracne Editrice).

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, A. Terras

Algebra

PAOLO ALUFFI
Florida State University

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/9781108958233
DOI: 10.1017/9781108955911

First published 2021

Printed in the United Kingdom by TJ Books Limited, Padstow Cornwall

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

ISBN 978-1-108-95823-3 Paperback

Contents

Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Frontmatter
More Information

Cambridge University Press
978-1-108-95823-3 — Algebra
Paolo Aluffi
Frontmatter
More Information

Introduction

This is an introductory textbook on abstract algebra. A glance at the table of contents will immediately reveal its basic organization and salient features: it belongs to the 'rings-first' camp, and places an unusual emphasis on *modules,* which (to my puzzlement) are often essentially omitted in textbooks at this level. A few section titles will also reveal passing nods to the notion of category, which is not developed or used in the main body of the text, but is also not intentionally hidden from sight.

Why 'rings first'? Why not 'groups'? This textbook is meant as a first approach to the subject of algebra, for an audience whose background does not include previous exposure to the subject, or even very extensive exposure to abstract mathematics. It is my belief that such an audience will find *rings* an easier concept to absorb than *groups.* The main reason is that rings are defined by a rich pool of axioms with which readers are already essentially familiar from elementary algebra; the axioms defining a group are fewer, and they require a higher level of abstraction to be appreciated. While $\mathbb{Z}$ is a fine example of a group, in order to view it as a group rather than as a ring, the reader needs to forget the existence of one operation. This is in itself an exercise in abstraction, and it seems best to *not* subject a naïve audience to it. I believe that the natural port of entry into algebra is the reader's familiarity with $\mathbb{Z}$, and this familiarity leads naturally to the notion of *ring.* Natural examples leading to group theory could be the symmetric or the dihedral groups; but these are not nearly as familiar (if at all) to a naïve audience, so again it seems best to wait until the audience has bought into the whole concept of 'abstract mathematics' before presenting them.

Thus, my choice to wait until later chapters before introducing groups is essentially dictated by the wish to provide a *gentle* introduction to the subject, where the transition to the needed level of abstraction can happen gradually. The treatment in the first several sections of this book is intentionally very elementary, with detailed explanations of comparatively simple material. A reader with no previous exposure to this material should be able to read the first two chapters without excessive difficulty, and in the process acquire the familiarity needed to approach later chapters. (Rings are introduced in Chapter 3.) The writing becomes more demanding as the material is developed, as is necessary—after all, the intended readership is expected to reach, by the end of the book, a good comfort level with rather sophisticated material, such as the basics of Galois theory. It is my hope that the reader will emerge from the book well equipped to approach graduate-level algebra. In fact, this is what many students in my undergraduate algebra courses have done.

The book could be used for a group-first approach, provided that the audience is 'mature' enough to cope right away with the higher level of abstraction of groups, and that the instructor is willing to occasionally interpolate references to previous chapters. In fact, the reliance of the chapters on groups in Part III on material developed in previous chapters is minimal, and mostly contextual (with the exception of a treatment of cyclic groups, which is carried out in Part II). However, the writing in Part III is naturally terser and puts more demands on the reader; so, again, this is not recommended for a naïve audience. Part IV deals with fields, and here the audience is certainly expected to be comfortable handling abstract concepts, perhaps at the level of a Master's student. I would definitely not recommend a 'fields-first' approach in an introduction to algebra.

More than 50 years ago, Atiyah and Macdonald wrote in their *Introduction to Commutative Algebra*: "...following the modern trend, we put more emphasis on modules and localization." Apparently, what was the 'modern trend' in 1970 has not really percolated yet to the standard teaching of an introductory course in algebra in 2020, since it seems that most standard textbooks at this level omit the subject of modules altogether. In this book, *modules* are presented as equal partners with other standard topics—groups, rings, fields. After all, most readers will have had some exposure to linear algebra, and therefore will be familiar to some extent with vector spaces; and they will emerge from studying rings with a good understanding of ideals and quotient rings. These are all good examples of modules, and the opportunity to make the reader familiar with this more encompassing notion should not be missed.

The opportunity to emphasize modules was in itself sufficient motivation to write this book. I believe that readers will be more likely to encounter modules, complexes, exact sequences, introduced here in §9.2, in their future studies than many other seemingly more standard traditional topics covered in introductory algebra books (and also covered in this text, of course).

Having made this choice, it is natural to view abelian groups as particular cases of modules, and the classification theorem for finitely generated abelian groups is given as a particular case of the analogous results for finitely generated modules over Euclidean domains (proved in full). Groups are presented as generalizations of abelian groups; this goes counter to the prevailing habit of presenting abelian groups as particular cases of groups. After treating groups, the text covers the standard basic material on field extensions, including a proof of the Fundamental Theorem of Galois Theory.

On the whole, the progression rings–modules–abelian groups–groups–fields simply seems to me the most natural in a first approach to algebra directed at an audience without previous exposure to the subject. While it is possible to follow a different progression (e.g., start with groups and/or avoid modules) I would have to demand more of my audience in order to carry that out successfully.

I could defend the same conclusion concerning categories. My graduate(-leaning) algebra textbook[1] has somehow acquired the reputation of 'using categories'. It would be more accurate to state that I did not go out of my way to *avoid* using the basic language

[1] *Algebra: Chapter 0.* Graduate Studies in Mathematics, No. 104. American Mathematical Society, Providence, RI.

of categories in that textbook. For this textbook, aimed at a more naïve audience, I have resolved to steer away from direct use of the language. I have even refrained from giving the definition of a category! On the other hand, the material itself practically demands a few mentions of the concept—again, if one does not go out of one's way to avoid such mentions. It is possible, but *harder,* to do without them. It seemed particularly inevitable to point out that many of the constructions examined in the book satisfy universal properties, and in the exercises the reader is encouraged to flesh out this observation for some standard examples, such as kernels or (co)products. My hope is that the reader will emerge from reading these notes with a natural predisposition for absorbing the more sophisticated language of categories whenever the opportunity arises.

The main prerequisite for this text is a general level of familiarity with the basic language of naive set theory. For the convenience of the reader, a quick summary of the relevant concepts and notions is included in the Appendix A, with the emphasis on equivalence relations and partitions. I describe in some detail a decomposition of set-functions that provides a template for the various 'isomorphism theorems' encountered in the book. However, this appendix is absolutely not required in order to read the book; it is only provided for the convenience of the reader who may be somewhat rusty on standard set-theoretic operations and logic, and who may benefit from being reminded of the various typical 'methods of proof'. There are no references to the appendix from the main body of the text, other than a suggestion to review (if necessary) the all-important notions of equivalence relations and partitions. As stressed above, the text begins very gently, and I believe that the motivated reader with a minimum of background can understand it without difficulty.

It is also advisable that readers have been exposed to a little linear algebra, particularly to benefit the most from examples involving, e.g., matrices. This is not strictly necessary; linear algebra is not used in any substantial way in the development of the material. The linear algebra needed in Part II is developed from scratch. In fact, one subproduct of covering modules in some detail in this text should be that readers will be better equipped to understand linear algebra more thoroughly in their future encounters with that subject.

Appendix B includes extensive solutions to about one-third of the exercises listed at the end of each chapter; these solved problems are marked with the symbol ▹. These are all (and only) the problems quoted directly from the text. In the text, the reader may be asked to provide details for parts of a proof, or construct an example, or verify a claim made in a remark, and so on. Readers should take the time to perform these activities on their own, and the appendix will give an opportunity to compare their work with my own 'solution'. I believe this can be very useful, particularly to readers who may not have easy access to an alternative source to discuss the material developed in this book. In any case, the appendix provides a sizeable amount of material that complements the main text, and which instructors may choose to cover or not cover, or assign as extra reading (*after* students have attempted to work it out on their own, of course!).

How to use this book? I cover the material in this book in the order it is written, in a two-semester sequence in abstract algebra at the undergraduate level at Florida State University. Instructors who, like me, have the luxury of being able to spend two semesters on this material are advised to do the same. One semester will suffice for the first part, on rings; and some time will be left to begin discussing modules. The second semester will complete modules and cover groups and fields.

Of course, other ways to navigate the content of this book are possible. By design, the material on groups has no hard references back to Chapter 6, 7, or 9. Therefore, if only one semester is available, one could plan on covering the core material on rings (Chapters 1–5), modules (Chapter 8), and groups (Chapter 11). It will be necessary to also borrow some material from Chapter 10, such as the definition and basic features of cyclic groups, as these are referenced within Chapter 11. This roadmap should leave enough time to cover parts of Chapter 12 (more advanced material on groups) or Chapter 13 (basic material on field extensions), at the discretion of the instructor.

The pedagogical advantages of the rings-first approach have been championed in Hungerford's excellent undergraduate-level algebra text, which I have successfully used several times for my courses. Readers who are familiar with Hungerford's book will detect an imprint of it in this book, particularly in the first several sections and in the choice of many exercises.

Thanks are due to the students taking my courses, for feedback as I was finding this particular way of telling this particular story. I also thank Ettore Aldrovandi for spotting a number of large and small errors in an earlier version of these notes, and several anonymous reviewers for very constructive comments. I thank Sarah Lewis for the excellent copyediting work, and Kaitlin Leach and Amy Mower at Cambridge University Press for expertly guiding the book from acquisition through production. Lastly, thanks are due to the University of Toronto and to Caltech, whose hospitality was instrumental in bringing this text into the present form.

Before we Begin

Dear reader: This book introduces you to the subject of *abstract algebra,* and specifically the study of certain structures—rings, modules, groups, and fields—which are the basic pillars of abstract algebra. While learning this material, you are not the end-user of a set of tools (as a calculus student may be); rather, you are taking a guided tour through the factory that produces those tools, and you are expected to learn how the tools themselves are put together. Your attention should be directed towards the deep reasons that make things work the way they do. These reasons are encapsulated in the various statements we will encounter, and these statements will deal with the precise definitions we will introduce. Your focus will be on *understanding* these definitions, these statements, and why the statements are true.

Unavoidably, in the main text I must assume that you have reached a certain level of 'mathematical maturity' and can read and write proofs, follow and construct logical arguments, and are familiar with the basic language of naive set theory. If you do not have this background, or if it dates too far back, you will want to spend some time perusing Appendix A, which attempts to cover these preliminary notions in a concise fashion. In any case, I have written the first several sections of the main text with particular abundance of details and explanations; a minimum level of familiarity with the way the notation is used should suffice in order to understand the material in these early sections, and the practice acquired in the process should be helpful in reading the later chapters, where the writing is necessarily more terse and your task is altogether more demanding.

The book includes a large number of exercises. They were also chosen so as to be more straightforward in earlier sections and gradually increase in complexity as the text progresses. Many exercises (marked with the symbol ▹ in the lists given at the end of each chapter) are quoted from within the text: these may ask you to complete a proof, or to fill in the details of an example, or to verify a claim made in a remark, and so on. While reading a mathematical text, it is very common to have to stop and carry out such verifications; indeed, this is an integral part of the process of understanding mathematics. My hope is that these exercises will help you gain this healthy habit. Appendix B includes the solutions to *all* these exercises. Comparing your work to my solution will hopefully provide you with useful feedback. Of course you shouldn't look up the solution to an exercise until you have given it your best shot; and you are warmly encouraged to try and solve *every* exercise in the book, whether a solution is provided or not.

Three indices are provided: the first two list definitions and theorems, and the third one is a standard subject index. The *definitions* are probably the most important component in a subject like algebra: they trace the path along which the material is developed, and most of the theorems one proves at this level have the purpose of expressing the precise way in which these definitions are related to one another. You should expect to look up the exact meaning of specific terms introduced in this book very often. The corresponding index will help you do this quickly when the need arises.

'Algebra' as we understand it currently, and as I will attempt to present it in these notes, was developed over the course of many decades if not centuries, and reached a very mature form long ago. It deals with certain types of objects (rings, groups, ...), that are introduced by choosing suitable collections of axioms to describe their general features precisely. These axioms are often chosen to model features of 'concrete' examples, such as the conventional algebra of integers; and indeed, this text begins with a discussion of the algebra of ordinary integers from a viewpoint which naturally leads to the definition of the notion of *ring.* The other algebraic structures treated in this text arise just as naturally. These structures have been extremely successful in the development of higher-level concepts and important branches of modern mathematics. Indeed, algebra is the language in which entire modern fields of mathematics are 'spoken': for example, algebraic geometry and algebraic number theory; but also seemingly distant fields like particle physics rely on sophisticated algebraic notions. Making any sense of such fields will require the background you are beginning to acquire by reading this book.

The book consists of four 'parts': on *rings,* on *modules,* on *groups,* and on *fields.* These are listed roughly in order of increasing abstraction. By the end of the text, we will gain an appreciation of *Galois theory,* which will answer very sophisticated questions about polynomials with integer coefficients. Such questions could be posed (and indeed were posed) before any of the more abstract scaffolding was put into place; but answering such questions really only becomes possible by using the abstract tools we will develop.

Before beginning in earnest, I will mention a concept that is even more basic and abstract than the main structures we are going to study. In fact, this concept gives a unifying view of such structures, and you have likely (and unwittingly) gathered an intuitive feeling for it in earlier studies. At some level, you are familiar with *sets:* they are a formalization of the notion of 'collections' of arbitrary things (called 'elements'); and we use *functions* to transfer information from a set to another set. (If you are not familiar with these notions, spend some time with Appendix A in this book!) You are also (likely) familiar with *vector spaces:* vector spaces are certain objects you study in linear algebra, and in that case also there is a way to 'transfer information' from one object to another object. Specifically, *linear maps* act between vector spaces, and you can describe them efficiently by means of matrices. Depending on your mathematical history to date, you may have run across the same template elsewhere. For example, if you have seen a little topology, then you have encountered *topological spaces,* and ways to go from one topological space to another one, that is, *continuous functions.*

After running into several such examples, you get used to the idea that studying a specific subject amounts to understanding the *objects* you are dealing with (for example, sets, vector spaces, topological spaces, and so on), and the type of functions that may be used to move from one object to another object of the same kind. In general, these 'functions' are called *morphisms.* (For example, morphisms are ordinary functions for sets, linear maps for vector spaces, continuous functions for topological spaces, and so on.) A 'category' is an abstract entity that captures this general template: categories consist of *objects,* and of *morphisms* between objects. There are a few axioms spelling out general requirements on objects and morphisms, which we do not need to list now but which would look familiar based on our experience with sets and functions, and with the other examples mentioned above. (For example, every object is required to have an 'identity morphism', just as every set has an 'identity function' and every vector space has an 'identity linear map', corresponding to the identity matrix.)

Large areas of mathematics can be understood, at least as a first approximation, as the study of certain categories. This unifying principle underlies *everything we will cover in these notes.* There is a category of *rings,* a category of *groups,* and several other categories of interest in the field of algebra. These categories have several common features. For example, we will be able to define 'quotients' of rings and 'quotients' of groups. These constructions all have a common thread, and this will become evident when we go through them. The reason is that they are all instances of general constructions that could be defined simultaneously for certain types of categories.

Studying algebra at this introductory level means to a large extent understanding how these constructions are performed in several key instances. We will not really use the language of categories in these notes, but it will secretly underlie most of what we will do. Some latent awareness of this fact may be beneficial to you, as it is to me. In any case, you will learn much more about this point of view when you move on to texts covering this material at a more advanced level.

Exercises

0.1 Read (or at least skim through) the Wikipedia page on 'category theory'.