Preface

This book is a textbook for a semester-long or a year-long introductory course in abstract algebra.

There is a lot of information in that sentence, so let us unpack it. First of all, this is a book, not an encyclopedia. What is the difference? An encyclopedia is a massive collection of information, while a book has a theme. Our book certainly does, and that theme is number theory. To be clear, this is not a text book on number theory, but we have decided on which topics to cover with an eye towards number theory, and we have included several sections that show applications of general algebraic ideas to topics in number theory. At the same time, a theme has variations, so we have not strictly restricted ourselves but have covered other topics as well.

This is an introduction, which means that we have presupposed no prior knowledge of abstract algebra. We do, however, assume that you (the student) have had a good course in linear algebra. By a good course we mean one that treats vector spaces and linear transformations in general, not one that is restricted to matrix manipulations (but of course does include that). And naturally, at this point in your mathematical development, you should be comfortable with doing rigorous mathematics, and this is certainly a rigorous book. We prove just about everything we claim or use, except that on occasion we mention a result that goes beyond the bounds of this book for the further edification of the reader.

There is enough material here for a year-long course, but we realize that you (the instructor) may not have the luxury of spending a year on it, so we have tried to write this book in a modular way, so that you may choose which topics to go into, and go into them as far as you like, before moving on to next one, covering what you wish in the course of a semester. Of course, some topics are required for others, so your choice will not be completely free. And for you (the student), if you are in a one-semester course, this book offers you the opportunity to read further in whatever particularly interests you.

Naturally, having written this book, we think highly of it, and think that it would provide an excellent basis for further study in abstract algebra in general. But, given our emphasis, we think that it would provide an ideal basis for further study in algebraic number theory.

The devil is in the details, as the saying goes, so here they are.

We begin, in Chapter 1, with set theory. This is often skipped, or presupposed, but we have decided to begin with it for several reasons. First, you may not be familiar with this material. Second, we treat quotients in many places in the book, so we wanted to present a particularly careful discussion of equivalence relations. And third, we wanted to take the opportunity to present the Schröder–Bernstein theorem (with proof, of course), which you may not be likely to see elsewhere.

In Chapter 2, we turn our attention to group theory. We concentrate on finite groups, but begin by treating groups in general, with examples such as matrix groups, so you can see the widespread appearance of groups throughout mathematics. (Too often, in our opinion, groups are treated purely for their own sake, which is of course appropriate in a specialized text, but is an approach that leads the reader to think of them in isolation rather than being of general interest.) We treat the standard, and essential, topics: homomorphisms, subgroups, quotient groups, etc. We also prove the fundamental structure theorem for finite abelian groups, and for finitely generated abelian groups, something that is not always done in texts at this level. We then have a section on applications to number theory, where we prove Fermat's little theorem and the basic facts on quadratic residues, all from a group-theoretic point of view. We study the actions of groups on sets, in preparation for proving Cauchy's theorem, results on the structure of p-groups, and the Sylow theorems. We briefly treat solvable groups, as we will be studying the solvability of equations by radicals in our chapter on field theory. We conclude this chapter by studying permutations and the symmetric groups.

Chapter 3 deals with ring theory. We begin in complete generality, considering both commutative and noncommutative rings, and rings with and without 1, and we study ideals, both one-sided and two-sided, ring homomorphisms, and quotients. But, in line with our emphasis, we fairly quickly turn our attention to commutative rings with 1, and further to integral domains. We study polynomial rings and prove the Hilbert basis theorem. We concentrate on the issues of divisibility and unique factorization in integral domains, proving the standard results that all Euclidean domains are principal ideal domains and that all principal ideal domains are unique factorization domains, developing Euclid's algorithm in the process. Our approach highlights the role played by the greatest common divisor (GCD), and on our way to our main results we define GCD domains (integral domains in which any set of elements, not all zero, has a gcd) and study their properties. We again have a section on applications to number theory, which has two main results. First, we use the fact that the Gaussian integers are a Euclidean domain (which we have earlier proved) to give Dedekind's proof of Fermat's theorem that every prime congruent to 1 modulo 4 is a sum of two squares in an essentially unique way. Second, we give Zolotarev's proof of Gauss's lemma and the Law of Quadratic Reciprocity by considering signs of permutations. We give, and prove, examples of unique and non-unique factorization, including, in particular, a variety of examples of rings of algebraic integers in quadratic fields. We consider quotient fields and localization, and study polynomial rings in detail. We conclude by studying prime and maximal ideals, proving the standard result that maximal ideals are prime, though not in general conversely, and also the less standard result that an integral domain in which all nonzero prime ideals are maximal is a principal ideal domain if and only if it is a unique factorization domain.

Chapter 4 deals with field theory in general and Galois theory in particular. We feel that our treatment here is quite distinctive.

We begin in a very concrete way, first showing how to make computations in field extensions. We then "front-load" our treatment of Galois theory by giving many examples of field extensions and Galois groups, even before arriving at the fundamental theorem of Galois theory (FTGT). Then we turn to proving the FTGT. As a first step, we show that an extension is Galois if and only if it is normal and separable. We then prove the FTGT *per se*. While our proof follows the spirit of Artin's approach, it is different in detail, and we do not need to use Dedekind's theory of group characters, as Artin does. (We think that our proof is thus more direct and conceptually a bit simple.) Having provide the FTGT, we go on to study further examples of field extensions. We prove the theorem of the primitive element and give a quite extensive study, far more than is usually done, of primitive elements in field extensions. We determine the structure of finite fields, and of cyclotomic fields. We conclude by deriving important consequences of field and Galois theory. We prove Abel's theorem that the general polynomial of degree five is not solvable by radicals. Indeed, we prove this for any degree $d \geq 5$, the proof of this more general result being identical to the proof for $d = 5$. For any prime $p \geq 5$ we give an explicit construction of a polynomial of degree p over the rationals for which this is the case. (Of course, this can be done for any degree at least five, but in light of this being an introductory text, we do not introduce the complications necessary to do so for the general case.) We show that the classical problems of antiquity — trisecting the angle, doubling the cube, and squaring the circle — are impossible to solve by straightedge and compass constructions. (Here we completely prove the first two of these but content ourselves with quoting Lindemann's theorem that π is transcendental in proving the third.) Finally, we give a proof of the fundamental theorem of algebra. Despite its name, this theorem cannot have a purely algebraic proof, as the real and complex numbers cannot be constructed purely algebraically, but we give a proof that uses the irreducible minimum of analytic results — only the theorem that a polynomial of odd degree with real coefficients must have a real roots – but otherwise is entirely algebraic, using Galois theory and group theory. Throughout this chapter we heavily use the viewpoint that an extension $\mathbb{E}$ of a field $\mathbb{F}$ is an $\mathbb{F}$-vector space, and so, as we have said, we are presupposing familiarity with vector spaces in general.

We conclude in Chapter 5 by studying Dedekind rings. Logically speaking, this could be part of Chapter 3, but pedagogically speaking, we feel it would be a mistake to put it there, as at that point we would have no examples to work with. But, having developed field theory in Chapter 4, we have rings of integers in algebraic number fields as examples, and we first prove that these are always Dedekind rings. Then we prove the main result about Dedekind rings, that nonzero ideals have unique factorization as a product of prime ideals, and then we give concrete examples chosen from rings of algebraic integers.

There are two appendices. To get started in Chapter 2 with group theory, we need to know basic properties of the integers (e.g., primes and unique factorization). But these results are part of ring theory, which we do not treat until Chapter 3. So in Appendix A we simply state these results, in order to have them available at the start when we need them. Of course, we do prove them in Chapter 3, and indeed in a more general context. Our proof of the theorem of the primitive element in Chapter 4 uses a result from linear algebra that, although standard, is not always presented, so in Appendix B we provide the statement and a proof of this result in order to have it available as well.

Each chapter concludes with a variety of exercises ranging from the straight-forward to the challenging. Some of these are particular examples that illustrate the theory while others are general results that develop the theory further.

Finally, some remarks on numbering and notation: We use three-level numbering, so that, for example, Theorem 4.10.3 is the third numbered item in Chapter 4, Section 10. We denote the end of proofs by □, as usual. Theorems, etc., are set in italics, so are demarcated by their typeface. Definitions, etc., are not, so we mark their end by $\Diamond$. Our mathematical notation is standard, though we want to point out that if A and B are sets, $A \subseteq B$ means that A is a subset of B and $A \subset B$ means that A is a proper subset of B.

We have enjoyed writing this book and we trust that you will enjoy reading it, and thinking deeply about the matter within it, as well.

Steven H. Weintraub
Bethlehem, PA, USA
May 2021

Contents