Contents

Preface

This is a textbook on Galois theory. Galois theory has a well-deserved reputation as one of the most beautiful subjects in mathematics. I was seduced by its beauty into writing this book. I hope you will be seduced by its beauty in reading it.

This book begins at the beginning. Indeed (and perhaps a little unusually for a mathematics text), it begins with an informal introductory chapter, Chapter 1. In this chapter we give a number of examples in Galois theory, even before our terms have been properly defined. (Needless to say, even though we proceed informally here, everything we say is absolutely correct.) These examples are sort of an airport beacon, shining a clear light at our destination as we navigate a course through the mathematical skies to get there.

Then we start with our proper development of the subject, in Chapter 2. We assume no prior knowledge of field theory on the part of the reader. We develop field theory, with our goal being the Fundamental Theorem of Galois Theory (the *FTGT*). On the way, we consider extension fields, and deal with the notions of normal, separable, and Galois extensions. Then, in the penultimate section of this chapter, we reach our main goal, the *FTGT*.

Roughly speaking, the content of the *FTGT* is as follows: To every Galois extension $\mathbf{E}$ of a field $\mathbf{F}$ we can associate its Galois group $G = \mathrm{Gal}(\mathbf{E}/\mathbf{F})$. By definition, G is the group of automorphisms of $\mathbf{E}$ that are the identity on $\mathbf{F}$. Then the *FTGT* establishes a one-to-one correspondence between fields $\mathbf{B}$ that are intermediate between $\mathbf{E}$ and $\mathbf{F}$, i.e., between fields $\mathbf{B}$ with $\mathbf{F} \subseteq \mathbf{B} \subseteq \mathbf{E}$, and subgroups of G. This connection allows us to use the techniques of group theory to answer questions about fields that would otherwise be intractable. (Indeed, historically Galois theory has been used to solve questions about fields that were outstanding for centuries, and even for millenia. We will treat some of these questions in this book.) In the final section of this chapter, we return to the informal examples with which we started the book, as well as treat-

ing more intricate and advanced ones that we can handle with our new-found knowledge.

In Chapter 3 we further develop and apply Galois theory. In this chapter we deal with a variety of different topics, some of which we mention here. In the first section we use Galois theory to investigate the field of symmetric functions and the ring of symmetric polynomials. Galois theory allows us to completely determine the structure of finite fields, and we do this in the third section. Two important properties of fields are the existence of primitive elements and normal bases, and we prove these in Sections 3.5 and 3.6. We can also say quite a bit about abelian extensions (i.e., extensions with abelian Galois groups), and we treat these in Section 3.7.

We develop Galois theory in complete generality, with careful consideration to the situation in positive characteristic as well as in characteristic 0. But we are especially interested in algebraic number fields, i.e., finite extensions of the field of rational numbers $\mathbf{Q}$. We devote Chapter 4 to considering extensions of $\mathbf{Q}$. Again we deal with a variety of different topics. We consider cyclotomic polynomials. We consider the question as to when equations are solvable by radicals (and prove Abel's theorem that the general equation of degree at least 5 is not). We show that the three classical geometric problems of Greek antiquity: trisecting the angle, duplicating the cube, and squaring the circle, are unsolvable with straightedge and compass. We deal with quadratic fields and their relation to cyclotomic fields, and we deal with radical polynomials, i.e., polynomials of the form $X^n - a$, which have a particular theory.

In Chapter 5 we consider more advanced topics in Galois theory. In particular, we prove that every field has an algebraic closure, and that the field of complex numbers $\mathbf{C}$ is algebraically closed, in Section 5.3, and we develop Galois theory for infinite algebraic extensions in Section 5.4.

Note that in Chapters 1 through 4, we assume that all field extensions are finite, except where explicitly stated otherwise. In Chapter 5 we allow extensions to be infinite.

There are three appendices. In the first we develop some necessary group theory. (We have put this in the appendix for logical reasons. The main text deals with field theory, and to develop the necessary group theory would lead to digressions in the main line of argument. Thus we collect these facts in an appendix in order to have a clear line of argument.) The second appendix revisits some material in the text from a more advanced point of view, which we do not want to presuppose of the reader, while the third appendix presents an elementary but tricky argument that enables us to avoid relying on Dirichlet's theorem about primes in an elementary progression at one point.

Our approach has been heavily influenced by Artin's classic 1944 text *Galois Theory*. Artin's approach emphasized linear algebra, and our approach

has the same (and perhaps greater) emphasis. We have tried to have minimal prerequisites for this book, but, given this emphasis, the reader should have a sound knowledge of linear algebra. Beyond that the reader should know the basic facts about groups and rings, and especially about polynomial rings. As a source for this background material we naturally recommend our previous book, *Algebra: An Approach via Module Theory*, by William A. Adkins and Steven H. Weintraub, Springer-Verlag Graduate Texts in Mathematics No. 136. We refer to this text as [AW] when we have occasion to cite it. Also, the reader should be familiar with elementary number theory (the material contained in any standard undergraduate course in the subject will more than suffice). Finally, the Krull topology is the key to understanding infinite Galois extensions, so in the final section of this book (Section 5.4), and in this section alone, the reader must have a good knowledge of point-set topology.

There is, roughly speaking, enough material in this book for a year-long course in Galois theory. A one-semester course could consist of Chapters 1 and 2 (both of which can be easily covered in a semester) plus additional material from Chapters 3 and 4 as interest dictates and time permits.

We would like to mention that our previous book, [AW], treated groups, rings, modules, and linear algebra. This book treats field theory, so together these two books cover the topics of a standard one-year graduate algebra course. Also, given our particular attention to Galois theory over $\mathbf{Q}$, we feel this book would be especially well-suited to students with an interest in algebraic number theory.

Our numbering system in this book is fairly standard. Theorem a.b.c refers to Theorem b.c in section b of Chapter a (or Appendix a). We denote the end of proofs by $\square$, as usual. In case a result is immediate, we simply append this symbol to its statement. Theorems, etc., are in italics, so are naturally set off from the remaining text. Definitions, etc., are in roman, and so are not. To delimit them, we end them with the symbol $\diamond$. Our notation is also fairly standard, but we call the reader's attention to the following conventions: We use $A \subseteq B$ to mean that A is a subset of B, while $A \subset B$ means that A is a proper subset of B. We denote fields by boldface letters and the integers by $\mathbb{Z}$. We will often be considering the situation where the field $\mathbf{E}$ is an extension of the field $\mathbf{F}$, and in this situation we will use greek letters ($\alpha, \beta, \gamma, \ldots$) to denote elements of $\mathbf{E}$ and roman letters ($a, b, c, \ldots$) to denote elements of $\mathbf{F}$. The greek letter ω will denote the primitive complex cube root of unity $\omega = (-1 + i\sqrt{3})/2$. The letter p will always denote a prime. Finally, id will denote the identity automorphism of whatever object is under consideration.

June 2005 *Steven H. Weintraub*