Graduate Texts in Mathematics 167

Springer
New York
Berlin
Heidelberg
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Santa Clara
Singapore
Tokyo

Graduate Texts in Mathematics

continued after index

Patrick Morandi

Field and Galois Theory

With 18 Illustrations

Springer

Patrick Morandi
Department of Mathematical Sciences
New Mexico State University
Las Cruces, NM 88003
USA

Mathematics Subject Classifications (1991): 12-01, 12F10, 12F20

Library of Congress Cataloging-in-Publication Data
Morandi, Patrick.
Field and Galois theory/Patrick Morandi.
p. cm. – (Graduate texts in mathematics ; 167)
Includes bibliographical references and index.
ISBN-13: 978-1-4612-8475-8 e-ISBN-13: 978-1-4612-4040-2
DOI: 10.1007/978-1-4612-4040-2
1. Algebraic fields. 2. Galois theory. I. Title. II. Series.
QA247.M67 1996
512'.3–dc20 96-13581

Printed on acid-free paper.

Softcover reprint of the hardcover 1st edition 1996

Production managed by Hal Henglein; manufacturing supervised by Joe Quatela.
Camera-ready copy prepared from the author's LaTeX files.

9 8 7 6 5 4 3 2 1

Preface

In the fall of 1990, I taught Math 581 at New Mexico State University for the first time. This course on field theory is the first semester of the year-long graduate algebra course here at NMSU. In the back of my mind, I thought it would be nice someday to write a book on field theory, one of my favorite mathematical subjects, and I wrote a crude form of lecture notes that semester. Those notes sat undisturbed for three years until late in 1993 when I finally made the decision to turn the notes into a book. The notes were greatly expanded and rewritten, and they were in a form sufficient to be used as the text for Math 581 when I taught it again in the fall of 1994.

Part of my desire to write a textbook was due to the nonstandard format of our graduate algebra sequence. The first semester of our sequence is field theory. Our graduate students generally pick up group and ring theory in a senior-level course prior to taking field theory. Since we start with field theory, we would have to jump into the middle of most graduate algebra textbooks. This can make reading the text difficult by not knowing what the author did before the field theory chapters. Therefore, a book devoted to field theory is desirable for us as a text. While there are a number of field theory books around, most of these were less complete than I wanted. For example, Artin's wonderful book [1] barely addresses separability and does not deal with infinite extensions. I wanted to have a book containing most everything I learned and enjoyed about field theory.

This leads to another reason why I wanted to write this book. There are a number of topics I wanted to have in a single reference source. For instance, most books do not go into the interesting details about discriminants and how to calculate them. There are many versions of discriminants in different fields of algebra. I wanted to address a number of notions of discriminant and give relations between them. For another example, I wanted to discuss both the calculation of the Galois group of a polynomial of degree 3 or 4, which is usually done in Galois theory books, and discuss in detail the calculation of the roots of the polynomial, which is usually not done. I feel it is instructive to exhibit the splitting field of a quartic as the top of a tower of simple radical extensions to stress the connection with solvability of the Galois group. Finally, I wanted a book that does not stop at Galois theory but discusses non-algebraic extensions, especially the extensions that arise in algebraic geometry. The theory of finitely generated extensions makes use of Galois theory and at the same time leads to connections between algebra, analysis, and topology. Such connections are becoming increasingly important in mathematical research, so students should see them early.

The approach I take to Galois theory is roughly that of Artin. This approach is how I first learned the subject, and so it is natural that I feel it is the best way to teach Galois theory. While I agree that the fundamental theorem is the highlight of Galois theory, I feel strongly that the concepts of normality and separability are vital in their own right and not just technical details needed to prove the fundamental theorem. It is due to this feeling that I have followed Artin in discussing normality and separability before the fundamental theorem, and why the sections on these topics are quite long. To help justify this, I point out that results in these sections are cited in subsequent chapters more than is the fundamental theorem.

This book is divided into five chapters, along with five appendices for background material. The first chapter develops the machinery of Galois theory, ending with the fundamental theorem and some of its most immediate consequences. One of these consequences, a proof of the fundamental theorem of algebra, is a beautiful application of Galois theory and the Sylow theorems of group theory. This proof made a big impression on me when I first saw it, and it helped me appreciate the Sylow theorems.

Chapter II applies Galois theory to the study of certain field extensions, including those Galois extensions with a cyclic or Abelian Galois group. This chapter takes a diversion in Section 10. The classical proof of the Hilbert theorem 90 leads naturally into group cohomology. While I believe in giving students glimpses into more advanced topics, perhaps this section appears in this book more because of my appreciation for cohomology. As someone who does research in division algebras, I have seen cohomology used to prove many important theorems, so I felt it was a topic worth having in this book.

In Chapter III, some of the most famous mathematical problems of antiquity are presented and answered by using Galois theory. The main questions of ruler and compass constructions left unanswered by the ancient Greeks, such as whether an arbitrary angle can be trisected, are resolved. We combine analytic and algebraic arguments to prove the transcendence of π and

e. Formulas for the roots of cubic and quartic polynomials, discovered in the sixteenth century, are given, and we prove that no algebraic formula exists for the roots of an arbitrary polynomial of degree 5 or larger. The question of solvability of polynomials led Galois to develop what we now call Galois theory and in so doing also developed group theory. This work of Galois can be thought of as the birth of abstract algebra and opened the door to many beautiful theories.

The theory of algebraic extensions does not end with finite extensions. Chapter IV discusses infinite Galois extensions and presents some important examples. In order to prove an analog of the fundamental theorem for infinite extensions, we need to put a topology on the Galois group. It is through this topology that we can determine which subgroups show up in the correspondence between subextensions of a Galois extension and subgroups of the Galois group. This marks just one of the many places in algebra where use of topology leads to new insights.

The final chapter of this book discusses nonalgebraic extensions. The first two sections develop the main tools for working with transcendental extensions: the notion of a transcendence basis and the concept of linear disjointness. The latter topic, among other things, allows us to extend to arbitrary extensions the idea of separability. The remaining sections of this chapter introduce some of the most basic ideas of algebraic geometry and show the connections between algebraic geometry and field theory, notably the theory of finitely generated nonalgebraic extensions. It is the aim of these sections to show how field theory can be used to give geometric information, and vice versa. In particular, we show how the dimension of an algebraic variety can be calculated from knowledge of the field of rational functions on the variety.

The five appendices give what I hope is the necessary background in set theory, group theory, ring theory, vector space theory, and topology that readers of this book need but in which they may be partially deficient. These appendices are occasionally sketchy in details. Some results are proven and others are quoted as references. Their purpose is not to serve as a text for these topics but rather to help students fill holes in their background. Exercises are given to help to deepen the understanding of these ideas.

Two things I wanted this book to have were lots of examples and lots of exercises. I hope I have succeeded in both. One complaint I have with some field theory books is a dearth of examples. Galois theory is not an easy subject to learn. I have found that students often finish a course in Galois theory without having a good feel for what a Galois extension is. They need to see many examples in order to really understand the theory. Some of the examples in this book are quite simple, while others are fairly complicated. I see no use in giving only trivial examples when some of the interesting mathematics can only be gleaned from looking at more intricate examples. For this reason, I put into this book a few fairly complicated and nonstandard examples. The time involved in understanding these examples will be time well spent. The same can be said about working the exercises. It is impossible to learn any mathematical subject merely by reading text. Field theory is no exception. The exercises vary in difficulty from quite simple to very difficult. I have not given any indication of which are the hardest problems since people can disagree on whether a problem is difficult or not. Nor have I ordered the problems in any way, other than trying to place a problem in a section whose ideas are needed to work the problem. Occasionally, I have given a series of problems on a certain theme, and these naturally are in order. I have tried not to place crucial theorems as exercises, although there are a number of times that a step in a proof is given as an exercise. I hope this does not decrease the clarity of the exposition but instead improves it by eliminating some simple but tedious steps.

Thanks to many people need to be given. Certainly, authors of previously written field theory books need to be thanked; my exposition has been influenced by reading these books. Adrian Wadsworth taught me field theory, and his teaching influenced both the style and content of this book. I hope this book is worthy of that teaching. I would also like to thank the colleagues with whom I have discussed matters concerning this book. Al Sethuraman read preliminary versions of this book and put up with my asking too many questions, Irena Swanson taught Math 581 in fall 1995 using it, and David Leep gave me some good suggestions. I must also thank the students of NMSU who put up with mistake-riddled early versions of this book while trying to learn field theory. Finally, I would like to thank the employees at TCI Software, the creators of Scientific Workplace. They gave me help on various aspects of the preparation of this book, which was typed in LaTeX using Scientific Workplace.

April 1996 Pat Morandi
Las Cruces, New Mexico

Notes to the Reader

The prerequisites for this book are a working knowledge of ring theory, including polynomial rings, unique factorization domains, and maximal ideals; some group theory, especially finite group theory; vector space theory over an arbitrary field, primarily existence of bases for finite dimensional vector spaces, and dimension. Some point set topology is used in Sections 17 and 21. However, these sections can be read without worrying about the topological notions. Profinite groups arise in Section 18 and tensor products arise in Section 20. If the reader is unfamiliar with any of these topics, as mentioned in the Preface there are five appendices at the end of the book that cover these concepts to the depth that is needed. Especially important is Appendix A. Facts about polynomial rings are assumed right away in Section 1, so the reader should peruse Appendix A to see if the material is familiar.

The numbering scheme in this book is relatively simple. Sections are numbered independently of the chapters. A theorem number of 3.5 means that the theorem appears in Section 3. Propositions, definitions, etc., are numbered similarly and in sequence with each other. Equation numbering follows the same scheme. A problem referred to in the section that it appears will be labeled such as Problem 4. A problem from another section will be numbered as are theorems; Problem 13.3 is Problem 3 of Section 13. This numbering scheme starts over in each appendix. For instance, Theorem 2.3 in Appendix A is the third numbered item in the second section of Appendix A.

Definitions in this book are given in two ways. Many definitions, including all of the most important ones, are spelled out formally and assigned a number. Other definitions and some terminology are given in the body of the text and are emphasized by italic text. If this makes it hard for a reader to find a definition, the index at the end of the book will solve this problem.

There are a number of references at the end of the book, and these are cited occasionally throughout the book. These other works are given mainly to allow the reader the opportunity to see another approach to parts of field theory or a more in-depth exposition of a topic. In an attempt to make this book mostly self-contained, substantial results are not left to be found in another source. Some of the theorems are attributed to a person or persons, although most are not. Apologies are made to anyone, living or dead, whose contribution to field theory has not been acknowledged.

Notation in this book is mostly standard. For example, the subset relation is denoted by $\subseteq$ and proper subset by $\subset$. If B is a subset of A, then the set difference $\{x : x \in A, x \notin B\}$ is denoted by $A - B$. If I is an ideal in a ring R, the coset $r + I$ is often denoted by $\overline{r}$. Most of the notation used is given in the List of Symbols section. In that section, each symbol is given a page reference where the symbol can be found, often with definition.

Contents

List of Symbols

Listed here are most of the symbols used in the text, along with the meaning and a page reference for each symbol.

Symbol	**Meaning**	**Page**
$\subseteq$	subset	1
K/F	field extension $F \subseteq K$	1
$[K : F]$	degree of field extension	2
$\mathbb{N}$	natural numbers	2
$\mathbb{Z}$	integers	2
$\mathbb{Q}$	rational numbers	2
$\mathbb{R}$	real numbers	2
$\mathbb{C}$	complex numbers	2
$\mathbb{F}_p$	integers mod p	2
$\{a : \mathcal{P}(a)\}$	set builder notation	3
ev_a	evaluation homomorphism	5
$F[\alpha], F(\alpha)$	ring and field generated by F and α	5
$F[\alpha_1, \dots, \alpha_n]$	ring generated by F and $\alpha_1, \dots \alpha_n$	5
$F(\alpha_1, \dots, \alpha_n)$	field generated by F and $\alpha_1, \dots, \alpha_n$	5
$F(X)$	field generated by F and X	5
$\min(F, \alpha)$	minimal polynomial of α over F	6
$\ker(\varphi)$	kernel of φ	7
$\deg(f(x))$	degree of $f(x)$	8
$\gcd(f(x), g(x))$	greatest common divisor	8

Symbol	Meaning	Page
L_1L_2	composite of L_1 and L_2	12
$\mathrm{Aut}(K)$	group of field automorphisms of K	15
$\mathrm{Gal}(K/F)$	Galois group of K/F	16
id	identity function	15
$f\|_S$	restriction of f to S	15
$\mathcal{F}(S)$	fixed field of S	18
F^*	multiplicative group of F	19
$\mathrm{char}(F)$	characteristic of F	22
$F(\sqrt{a})$	field generated by F and $\sqrt{a}$	23
$PGL_n(F)$	projective general linear group	26
$\mathbb{A}$	algebraic numbers	31
$A \times B$	Cartesian product	31
$\|S\|$	cardinality of S	32
$A - B$	set difference	35
$\cong$	isomorphic	39
F^p	set of p-powers in F	40
$f'(x)$	formal derivative of $f(x)$	40
$[K:F]_s$	separable degree of K/F	48
$[K:F]_i$	purely inseparable degree of K/F	48
$\subset$	proper subset	50
$\langle\sigma\rangle$	cyclic group generated by σ	52
$A \times B, A \bigoplus B$	direct sum	53
S_n	symmetric group	59
$N(H)$	normalizer	60
Q_8	quaternion group	61
$\exp(G)$	exponent of G	65
R^*	group of units of R	72
$\phi(n)$	Euler phi function	72
$\Psi_n(x)$	nth cyclotomic polynomial	73
$\mathbb{Q}_n$	nth cyclotomic field	75
$\mathrm{End}_F(V)$	space of endomorphisms	78
$M_n(F)$	ring of $n \times n$ matrices	78
$\det(A), \|A\|$	determinant of A	79
$\mathrm{Tr}(A)$	trace of A	79
L_a	left multiplication by a	79
$N_{K/F}$	norm of K/F	79
$T_{K/F}$	trace of K/F	79
$i \bmod n$	least nonnegative integer congruent to i modulo n	89
$\wp$	p-function	90
D_n	dihedral group	92
$\mathbb{Z}[G]$	integral group ring	95