

Algebra

A Graduate Course

I. Martin Isaacs

**Graduate Studies
in Mathematics**

Volume 100



American Mathematical Society

Algebra

A Graduate Course

I. Martin Isaacs

Graduate Studies
in Mathematics

Volume 100



American Mathematical Society
Providence, Rhode Island

EDITORIAL COMMITTEE

David Cox (Chair)
Steven G. Krantz
Rafe Mazzeo
Martin Scharlemann

2000 *Mathematics Subject Classification*. Primary 00A05;
Secondary 12–01, 13–01, 16–01, 20–01.

For additional information and updates on this book, visit
www.ams.org/bookpages/gsm-100

Library of Congress Cataloging-in-Publication Data

Isaacs, I. Martin, 1940–

Algebra : a graduate course / I. Martin Isaacs.

p. cm. — (Graduate studies in mathematics ; v. 100)

Originally published: Pacific Grove, Calif. : Brooks/Cole, c1994.

Includes bibliographical references and index.

ISBN 978-0-8218-4799-2 (alk. paper)

1. Algebra—Textbooks. I. Title.

QA154.2.I83 2009
512—dc22

2008047416

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

© 1994 held by the American Mathematical Society, All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.

Printed in the United States of America.

⊗ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 14 13 12 11 10 09

To Deborah

Preface

When I started graduate school at Harvard in 1960, I knew essentially no abstract algebra. I had seen the definition of a group when I was an undergraduate, but I doubt that I had ever seen a factor group, and I am sure that I had never even heard of modules. Despite my ignorance of algebra (or perhaps because of it), I decided to register for the first half of the graduate algebra sequence, which was being taught that year by Professor Lynn Loomis. I found the course exciting and beautiful, and by the end of the semester I had decided that I wanted to be an algebraist. This decision was reinforced by an equally spectacular second semester.

I have now been teaching mathematics for more than a quarter-century, and I have taught the two-semester first-year graduate algebra course many times. (This has been mostly at the University of Wisconsin, Madison, but I also taught parts of the corresponding courses at Chicago and at Berkeley.) I have never forgotten Professor Loomis's course at Harvard, and in many ways, I try to imitate it. Loomis, for example, used the first semester mostly for noncommutative algebra, and he discussed commutative algebra in the second half of the course. I too divide the year this way, which is reflected in the organization of this book: Part 1 covers group theory and noncommutative rings, and Part 2 deals with field theory and commutative rings.

The course that I took at Harvard "sold" me on algebra, and when I teach it, I likewise try to "sell" the subject. This affects my choice of topics, since I seldom teach a definition, for example, unless it leads to some exciting (or at least interesting) theorem. This philosophy carries over from my teaching into this book, in which I have tried to capture as well as I can the "feel" of my lectures. I would like to make my students and my readers as excited about algebra as I became during my first year of graduate school.

Students in my class are expected to have had an undergraduate algebra course in which they have seen the most basic ideas of group theory, ring theory, and field

theory, and they are also assumed to know elementary linear algebra and matrix theory. Most important, they should be comfortable with mathematical proofs; they should know how to read them, invent them, and write them. I do not require, however, that my students actually remember the theorems or even the definitions from their undergraduate algebra courses. Given my own lack of preparation as a first-year graduate student, I am well aware that a few in my audience may be completely innocent of algebra, and I want to conduct the course so that a student such as I was can enjoy it. But this is a graduate course, and it would not be fair to the majority to go on endlessly with “review” material. I resolve this contradiction by making my presentation complete: giving all definitions and basic results, but I do this quickly, and I intersperse the review material with ideas that very few of my audience have seen before. I have attempted to do the same in this book.

By the end of a year-long graduate algebra course, a good student is ready to go more deeply into one or more of the many branches of algebra. She or he might enroll in a course in finite groups, algebraic number theory, ring theory, algebraic geometry, or any of a number of other specialized topics. While I do not pretend that this book would be suitable as a text for any of these second-year courses, I have attempted to include some of the important material from many of them. I hope that this provides a convenient way for interested readers to sample a number of these topics without having to cope with the somewhat inconsistent notations and different assumptions about readers’ backgrounds that are found in the various specialized books. No attempt has been made, however, to designate in the text which chapters and sections are first-year material and which are second; this is simply not well defined. Lecturers who teach from this book undoubtedly do not agree on what, precisely, should be the content of a first-year course. In addition to providing opportunities for students to sample advanced topics, the additional material here should provide some flexibility for instructors to construct a course compatible with their own tastes. Also, those with very well-prepared and capable students might elect to leave out much of the “easy stuff” and build a course consisting largely of what I think of as “second-year” topics.

Since it is impossible, in my opinion, to cover all of the material in this book in a two-semester course, some topics must be skipped, and others might be assigned to the students for independent reading. Perhaps it would be useful for me to describe the content of the course as I teach it at Madison.

I cover just about all of the first four chapters on basic group theory, and I do most of Chapter 5 on the Sylow theorems and p -groups, although I omit Theorem 5.27 and Section 5D on Brodkey’s theorem. I do Chapter 6 on symmetric and alternating groups except for Section 6D. In Chapter 7, I cover direct products, but I omit Theorem 7.16 and Section 7C on semidirect products. In Chapter 8 on solvable and nilpotent groups, I omit most of Sections 8C and 8D and all of 8F. I do present the Frattini argument (8.10) and the most basic definitions and facts about nilpotent groups. Chapter 9 on transfer theory I skip entirely.

Chapters 10 and 11 on operator groups are a transition between group theory and module theory. I cover Sections 10A and 10B on the Jordan-Hölder theorem for operator groups, but I omit Section 10C on the Krull-Schmidt theorem. I cover

Sections 11A and 11B on chain conditions, but I touch 11C only lightly. I discuss Zorn's lemma (11.17), but I do not present a proof.

Chapter 12 begins the discussion of ring theory, and some readers may feel that there is a downward "jump discontinuity" in the level of sophistication at this point. As in Chapters 1 and 2, where the definitions and most basic properties of groups are presented (reviewed), it seems that here too it is important to give clear definitions and discussions of elementary properties for the sake of those few readers who may not be comfortable with this material. Section 12A could be assigned as independent reading, but I usually go over it quickly in class. I cover all of Chapter 12 in my course. I do Sections 13A and 13B on the Jacobson radical completely, but sometimes I skip Section 13C on the Jacobson density theorem. (I often find that I am running short of time when I get here.) I do Sections 13D and 14A and as much of 14B on the Wedderburn-Artin theorems as I have time for, and I omit the rest of Chapter 14 and all of Chapter 15.

In the second semester, I start with Chapter 16, and I cover almost all of that, except that I go lightly over Section 16D. I construct fraction fields for domains, but I do not discuss localization more generally. Chapters 17 and 18 discuss basic field extension theory and Galois theory; I cover them in their entirety. I discuss Section 19A on separability, but usually I do only a small amount of 19B on purely inseparable extensions, and I skip 19C. I cover Sections 20A and 20B on cyclotomic extensions, but I skip 20C and go very quickly over 20D on compass and straightedge constructions. In Chapter 21 on finite fields, I cover only Sections 21A and 21D: the basic material and the Wedderburn theorem on finite division rings. In Chapter 22, I omit Sections 22C and 22E, but, of course, I cover 22A and 22B on the solvability of polynomials thoroughly, and I present the fundamental theorem of algebra in 22D. In Chapter 23, I do only Sections 23A, 23B, and 23C, discussing norms and traces, Hilbert's Theorem 90, and a very rudimentary introduction to cohomology. I generally skip Chapter 24 on transcendental extensions completely, and I almost completely skip Chapter 25. (I may mention the Artin-Schreier theorem, but I never discuss formally real fields.)

Chapter 26 begins the discussion of the ideal theory of commutative rings. I cover the first two sections, but I skip Section 26C on localization. In Chapter 27 on noetherian rings, I usually cover only the first two sections and seldom get as far as 27C on the uniqueness of primes in the Lasker-Noether theorem. (I wish that I could discuss Krull's results on the heights of prime ideals in Section 27E, but it seems impossible to find the time to do that.) In Chapter 28 on integrality, I cover only the first three sections. I try to cover at least Section 29A, giving the basic properties of Dedekind domains, but often I find that I must skip Chapter 29 entirely because of time pressure. I always leave enough time, however, to prove Hilbert's Nullstellensatz in Section 30A, and that completes the course.

The user of this book will choose what to read (or teach) and what to skip, but I, as the author, was forced to make other choices. For most of these, there were arguments in both directions, and I am certain that very few will agree with all of my decisions, and perhaps I cannot even hope for a majority agreement on each of them separately. I elected not to include tensor products, for example, because

there just didn't seem to be much interesting that one could say about them without going deeply either into the theory of simple algebras or into homological algebra. Somewhat similarly, I decided not to discuss injective modules. It would have taken considerable effort just to prove that they exist in most cases, and there did not seem much that one could do with them without going into areas of ring theory beyond what I wished to discuss. Also, I did not discuss fully the characterization of finitely generated modules over PIDs, but I did include what seem to be the two most important special cases: the fundamental theorem for finite abelian groups and the fact that torsion-free, finitely generated modules over PIDs are free.

Some of my inclusions (for example, the Berlekamp factorization algorithm and character theory) may seem too specialized for a book of this sort. I discussed the factorization algorithm for polynomials over finite fields, for instance, mostly because I think it is a really slick idea, but also because computer algebra software has become widely available recently, and it seemed that students of "theoretical" algebra ought to receive at least a glimpse of the sort of algorithms that underlie these programs. I included some character theory (Chapter 15 and part of Chapter 28) partly because it provides nice applications of some of the theory, but also, I must admit, because that is my own primary research interest.

I also had to make decisions about notation. I suspect that the most controversial are those concerning functions and function composition. To me (and I think to most group theorists) it seems more natural to write " fg " rather than " gf " to denote the result of doing first function f and then function g . It did not seem wise to use left-to-right composition in the group theory chapters and then to switch and use right-to-left notation in the rest of the book, and so I decided to make consistency a high priority. Since I am a group theorist (and group theory is the first topic in the book), I elected to use left-to-right composition everywhere.

Customarily, when functions are composed left-to-right, the name of the function is written to the right of the argument. A critic of my left-to-right composition challenged my claim to consistency by betting that I did not write $(x)\sin$ and $(y)(d/dx)$ to denote the sine of x or the derivative of y with respect to x . He was right, of course. Like most mathematicians, I write most functions on the left. Nevertheless, I always (in this book at least) compose left-to-right. By my notational scheme, therefore, the following silly looking equation is technically correct: $f(g(x)) = (gf)(x)$. In order to avoid such strange looking formulas, I take the view that the function name may be written on *either* side of its argument, whichever is most convenient at the moment. In contexts where function composition is important, I nearly always choose to put the function name on the right, but I am perfectly comfortable in writing $\sin(x)$, since we are not generally interested in compositions of trigonometric functions. No information is lost by allowing the same function to appear sometimes on the left and sometimes on the right because the composition rule is always left-to-right and is independent of how the function is written.

Another of my decisions that will not meet with universal approval is that by my definition, rings have unity elements. There are a few places where this is not a good idea: one cannot conveniently state the theorem, for example, that a right artinian "ring" with no nonzero nilpotent ideals must have a unity. Most of the time,

however, assuming the existence of a unity is a convenience, and so we have built it into the definition. We have also required in the definition of a module that the unity of the ring act as an identity on the module.

Whatever notational scheme one adopts, it is important that students learn of the existence of common alternatives; how else could they read the literature or attend courses from other lecturers? For this reason, I have attempted to mention competing notations and definitions whenever appropriate in the text.

At the end of each chapter, there is a fairly extensive list of problems. Few of these are routine exercises, and some of them I consider to be quite difficult. The purpose of these problems is not just to give practice with the definitions and with understanding the theorems. My hope is that by working these problems, students will get a feeling of what it is actually like to *do* algebra, and not just to learn it. (I should mention that when I teach my algebra course, I assign five problems per week.)

This is not a “scholarly” book; I have not attempted to trace back to their sources the various definitions, lemmas, theorems, and ideas presented here. I have credited items to individuals in cases such as the “Sylow theorems,” the “Jacobson radical,” and the “Hilbert basis theorem” where such attribution is standard and well known and in other situations where it seemed appropriate. Even in these cases, however, I have not given bibliographic references to the original sources.

I am grateful to the following reviewers for their helpful comments: Michael Aschbacher, California Institute of Technology; Carl Widland, Indiana University; Edward Green, Virginia Polytechnic Institute and State University; Seth Warner, Duke University; E. Graham Evans, Jr., University of Illinois, Urbana-Champaign; Robert L. Griess, Jr., University of Michigan, Ann Arbor; Ancel Mewborn, University of North Carolina at Chapel Hill; Peter Norman, University of Massachusetts, Amherst; and Gerald Janusz, University of Illinois, Urbana-Champaign.

Let me close this preface by expressing my hope that this book will engender, in some readers at least, the same excitement and love for algebra that I received from Professor Loomis in my first year of graduate school.

I. Martin Isaacs
Madison, WI
1992

Contents

PART ONE
Noncommutative Algebra 1

CHAPTER 1
Definitions and Examples of Groups 3

CHAPTER 2
Subgroups and Cosets 14

CHAPTER 3
Homomorphisms 30

CHAPTER 4
Group Actions 42

CHAPTER 5
The Sylow Theorems and p -groups 55

CHAPTER 6
Permutation Groups 70

CHAPTER 7	
<i>New Groups from Old</i>	83
CHAPTER 8	
<i>Solvable and Nilpotent Groups</i>	99
CHAPTER 9	
<i>Transfer</i>	115
CHAPTER 10	
<i>Operator Groups and Unique Decompositions</i>	129
CHAPTER 11	
<i>Module Theory without Rings</i>	142
CHAPTER 12	
<i>Rings, Ideals, and Modules</i>	159
CHAPTER 13	
<i>Simple Modules and Primitive Rings</i>	177
CHAPTER 14	
<i>Artinian Rings and Projective Modules</i>	194
CHAPTER 15	
<i>An Introduction to Character Theory</i>	213

PART TWO
Commutative Algebra 231

CHAPTER 16
Polynomial Rings, PIDs, and UFDs 233

CHAPTER 17
Field Extensions 254

CHAPTER 18
Galois Theory 274

CHAPTER 19
Separability and Inseparability 293

CHAPTER 20
Cyclotomy and Geometric Constructions 307

CHAPTER 21
Finite Fields 326

CHAPTER 22
Roots, Radicals, and Real Numbers 342

CHAPTER 23
Norms, Traces, and Discriminants 359

CHAPTER 24
Transcendental Extensions 379

CHAPTER 25	
<i>The Artin-Schreier Theorem</i>	401
CHAPTER 26	
<i>Ideal Theory</i>	418
CHAPTER 27	
<i>Noetherian Rings</i>	433
CHAPTER 28	
<i>Integrality</i>	453
CHAPTER 29	
<i>Dedekind Domains</i>	474
CHAPTER 30	
<i>Algebraic Sets and the Nullstellensatz</i>	493
<i>Index</i>	507

This page intentionally left blank

Index

- Abel, N. 274
abelian group 11, 19, 37, 90–93, 139, 314
 characters of 229
abelian X -group 142–153, 156, 157, 167
ACC (ascending chain condition) 143–145, 433
action
 of group 42–43
 on cosets 44, 45, 115
 via automorphisms 95, 112, 114
adjectives 163
adjoint matrix 439, 456
affine group of line 8, 29
afforded character 216
algebra (over a field) 166, 171, 172, 173, 213, 295
algebraic closure 267–268, 271
 of finite degree 401–407, 415
algebraic element 254–259, 386, 398
algebraic field extension, definition of 256
algebraic geometry 493
algebraic integer 454, 463, 469, 471–472
algebraic number 256
algebraic number field 256
algebraic numbers, field of 256, 259, 268, 410
algebraic point 494
algebraic set 493–505
algebraically closed field 267–269, 303, 355
algebraically independent elements 379–380, 383, 398
alternating group 75
 simplicity of 77
annihilator (*see also* prime annihilator) 163, 176, 177, 210–211, 440, 442
antichain 157
archimedean ordered field 412–413
Artin, E. 145–146
Artin-Rees theorem 461
Artin-Schreier theorem 401
Artin's theorem 260, 262, 389
artinian module 170, 444
artinian ring (*see* right artinian ring *or* left artinian ring)
artinian commutative ring 252, 428
artinian X -group 145–146, 148–149, 150, 157
ascending central series (*see* upper central series)
ascending chain condition (*see* ACC)
associated factors 338
associated prime ideal 440–442, 450
associative property 9
augmentation ideal 173
augmentation map 173
automorphism
 of group 19–22
 of symmetric group 79–80
automorphism group
 of algebraically closed field 405
 of group 20, 28, 41, 310
axiom of choice 5, 144–145, 153, 269
basis for free module 202, 434
Berkamp algorithm 333–339, 464
bijection 4
binary operation 9

- binomial coefficient 55
- block diagonal representation 216, 219
- bracket operation 305
- Brodkey's theorem 66
- Burnside, W. 51, 115
- Burnside's fusion lemma 121
- Burnside's theorem on normal p -complements 122
- Burnside's two-prime theorem 66, 115, 213, 467–471

- cancellation in direct products 85, 139–140
- canonical homomorphism 30, 32
- cardinal number 269–270
- casus irreducibilis 351
- Cauchy-Frobenius theorem 50–51
- Cauchy's theorem 54, 57
- Cayley, A. 9
- Cayley's theorem 12, 161
- center
 - of character 225, 229, 230
 - of dihedral group 19
 - of group 19, 39, 229
 - of p -group 63
 - of ring 174
- center with finite index 119–120, 128
- central chief factor 141
- central extension 118
- central product 97
- central series 105–107
- centralizer 18–19
 - in homomorphic image 53
 - in ring 174
- centralizer ring of module 184
- chain 143
- character 213–230, 468–471, 473
 - definition of 216
- character induction and restriction 225–226
- character table 218
- characteristic
 - of field 214, 271, 281, 296–299, 308, 326, 401, 404
 - of ring 173
- characteristic polynomial 359–362
- characteristic subgroup 19, 21
- chief factor 102, 141
- chief series 102, 131
- Chinese remainder theorem 334, 341, 431, 480
- Classification theorem for simple groups 38, 99
- choice function 145

- class (*see* conjugacy class)
- class equation 49
- class function 217, 221, 226, 227
- class number 480
- classical adjoint 439, 456
- Clifford's theorem 158
- closed elements in Galois connection 276
- closure operator 276
- closure of coset product 24–25
- closure property 6, 9, 14
- coboundary 368
- cochain 368
- cocycle 368
- coefficient
 - of cyclotomic polynomial 309–310, 323
 - of polynomial 233, 272, 457
 - sequence 234
- cohomology group 367–368, 369
- colored cubes 53
- colored squares 52–53
- comaximal ideals 341, 431
- commutative diagram 32
- commutative ring 160
- commutator
 - of elements 27, 37, 106, 110
 - of subgroups 27, 37, 105–106, 110, 114
- commutator subgroup (*see* derived subgroup)
- compass 315–316
- complement in X -group 149
- complement to normal subgroup 94, 377
- completely reducible module 170, 197–198
- completely reducible X -group 149–153, 158
- complex conjugate 223
- complex number field 264, 355, 316, 383
- composition factor 38, 101, 102, 132
 - having specified type 140
 - of module 212
- composition length 134, 146, 150–151, 188
- composition of mappings 4, 6, 7, 12, 159
- composition series 38, 101, 102, 131 (*see also* X -composition series)
- compositum of fields 289, 312–313
- conjugacy class 47, 48, 120, 217, 468, 470
 - in symmetric group 73, 81
- conjugacy of point stabilizers 77
- conjugate elements 20, 120
- conjugate permutations 72–73
- conjugate subgroups 20, 57, 77
- conjugation action 43, 49
- constant polynomial 235
- constituent of representation 216, 219
- constructible number 316–320, 325
- construction of abelian groups 91

- continuous functions, ring of 252, 429–430
 contraction 426–427
 coprime elements of UFD 241
 coproduct 86
 core
 of subgroup 45, 113
 of Sylow subgroup 66
 Correspondence theorem 35, 36
 for rings 164
 for X -groups 130
 coset 22–24
 cosets, action on 44, 45, 115
 counting colored cubes 53
 counting colored squares 52–53
 counting conjugates 48–49
 counting orbits 50
 counting Sylow subgroups 58–59
 crossed homomorphism 366–368, 370
 cycle 70, 81
 cycle structure 72, 76, 465
 cyclic group 16–18, 21, 28, 91–92, 98, 260, 310
 automorphisms of 28, 310, 312
 isomorphism of 18, 32
 cyclic Sylow subgroup 82, 118, 122, 127
 cyclotomic field 310–313, 315, 323–324
 cyclotomic polynomial 246, 308–311, 314–315, 323–324, 340
 cyclotomy 307

 DCC (descending chain condition) 143–145
 on prime ideals 421, 443
 Dedekind, R. 474
 Dedekind domain 436, 464, 474–492
 Dedekind's lemma 27, 40
 on independence of field automorphisms 346, 366
 degree
 of character 216, 219, 468, 473
 of field extension 255–256, 259, 289, 299, 301, 302, 311, 316, 351, 354
 of polynomial 236, 252, 261, 328, 351
 of representation 215
 dense subring 185, 187
 derivation 293–295, 304–305
 derivative 293–294, 296 (*see also* formal derivative)
 derived length 101, 112
 derived series 100
 derived subgroup 37, 41, 100, 115, 133
 descending central series (*see* lower central series)

 descending chain condition (*see* DCC)
 determinant 30, 165, 359–361, 373
 development of Sylow subgroups 57
 diagonal matrix 223
 diagonal subgroup 96, 97
 diamond 34, 40
 Diamond theorem 33, 36
 dihedral group 7, 12, 19, 21, 47, 229
 direct product 83–89, 107, 108, 134–135, 137, 141
 of cyclic groups 90–93, 98, 251
 of simple groups 96, 97
 direct sum (*see* direct product)
 of ideals (*see* direct sum of rings)
 of rings 160, 199–200, 211, 212, 334, 431, 480
 of X -simple X -groups 151–152
 Dirichlet's theorem 314
 discriminant
 of field extension 370–371, 374, 463
 of polynomial 371–376, 378, 398
 disjoint cycle decomposition (*see* cycle structure)
 disjoint permutations 70
 distinct roots 279, 295–296
 divisible group 98
 Division algorithm 236
 division ring 165, 167, 168, 172, 184–185, 201, 339
 matrix ring over 169, 188–189, 191–192, 200
 vector space over 187–188, 192
 divisor in ring 238
 domain 172, 233, 237, 304, 437, 448, 450, 484, 486, 490, 491 (*see also* Dedekind domain)
 of mapping 4
 of specialization 396
 Double centralizer theorem 187
 double coset 53
 doubly transitive action 53
 dual group 93–94
 duplicating a cube 315–317

 Eisenstein criterion 245, 264
 elementary abelian group 13, 102
 elementary symmetric function 292, 361, 472
 embedded prime ideal 442, 450, 452
 endomorphism 129, 135
 endomorphism ring 159, 160, 161, 167, 184–191, 192
 Euclidean algorithm 333
 Euclidean construction 316

- Euler's function 17, 28, 308, 312–313, 356
- evaluation map 235–236
- even permutation 74–76, 372
- expansion 426
- extension by root of unity 311
- extension of groups 94, 118, 369, 378
- extension field (*see* field extension)
- external direct product or sum 83–87

- F*-automorphism 275
- F*-isomorphism 263–264, 267, 271, 273, 305
- factor group 25, 30
 - subgroup of 36
- factor module 170
- factor ring 164
- Factor-replacement theorem 137
- factor set 368
- factorization polynomial 335
- factorization row 336
- faithful action 43
- faithful module 187, 190
- FCP (*see* fundamental counting principle)
- Fermat prime 321–322
- Fermat's last theorem 474
- field 165, 168
- field extension 254–273
- field of fractions 243–245, 248, 251, 253, 304, 454, 457, 475
- finite algebraic set 500–502
- Finite approximation theorem 480
- finite degree field extension 256, 260, 279
- finite index subgroup 45
- finite field 326–341, 504
- finite generation 131–147, 150, 157, 386, 433–434, 451, 462, 477, 496
- finite ring 172
- finitely generated module 172, 183, 439, 442–443, 455, 475, 487
- finiteness condition 131, 143, 150, 152
- Fischer-Greiss group 38
- Fitting subgroup 109, 110, 113, 157
- Fitting's theorem 135
- fixed field 275–277, 285, 286
- focal subgroup 120
- Focal subgroup theorem 120
- foo ring 187
- formal derivative 295
- formal differentiation (*see* formal derivative)
- formally real field 405–406, 409–411, 414–417 (*see also* realclosed field)
- fraction field (*see* field of fractions)
- fractional ideal(s) 475–477, 484
 - group of 476, 479
- Frobenius argument 103
- Frobenius complement 128, 227
- Frobenius, G. 68, 123, 213
- Frobenius reciprocity theorem 226
- Frobenius's theorem
 - on groups with a Frobenius complement 128, 213, 228–229
 - on normal p -complements 124
- function composition 4, 6, 7, 12, 159, 346
- fundamental counting principle 47–50
- Fundamental theorem
 - of abelian groups 90, 139, 250–251
 - of algebra 264, 355, 383
 - of character theory 217
 - of Galois theory 284, 286
- fusion 120–121, 124, 128

- Galois connection 275, 495
- Galois, E. 99, 274
- Galois extension of fields 277–278, 282–285, 290–291, 399, 461
- Galois field 327 (*see also* finite field)
- Galois group 99, 274–277, 364
 - cyclic 329, 347, 358, 365
 - determination of 375–376, 464–467
 - order of 284–286
 - prescribed 314, 323, 345, 358, 394–396, 400
 - specific computation of 287–288, 291, 311–312, 329, 345, 358, 376
 - subgroups of 286, 290
- Galois theory 261, 264, 274–292, 301
- Galois's theorem on polynomial solvability 100, 274, 342–344
- Gauss sum 324
- Gaussian elimination 337
- Gauss's lemma 244, 465
- Gauss's theorem
 - on constructible polygons 321–322
 - on cyclotomic polynomials 311
- gcd (*see* greatest common divisor)
- GD (*see* Going down theorem)
- general linear group 8, 12, 30, 215
- generating set for group 15, 27
- generator for field extension 255
- generators for symmetric group 77, 81, 82
- generic point 505
- geometric construction 315–322
- Going down theorem 461
- Going up theorem 460
- greatest common divisor 17
 - for polynomials 333
- Greiss, R. 38

- ground field 254
 group action 42–43
 group algebra 173, 174, 175, 192, 214–215
 complex numbers 215, 219–222, 470
 group
 definition of 9, 10
 of symmetries 7, 8, 47
 of transformations 3
 of units 165
 with operators 129 (*see also* X -group)
 with given order 60–63, 65, 67, 68, 72, 76,
 78, 81, 122
 Grün's theorems 127
 GU (*see* Going up theorem)
- Hall, P. 104
 Hall subgroup 39, 67, 103, 120
 Hall's commutator identity 27, 110–111
 Hall's theorem 103
 Hamilton 166, 167
 height of prime ideal 444, 446–448, 503
 Heine-Borel theorem 429
 Hilbert basis theorem 434, 495
 Hilbert Nullstellensatz (*see* Nullstellensatz)
 Hilbert's irreducibility theorem 394, 396
 Hilbert's Theorem 90 365
 additive form 377
 homomorphism 30–33, 35, 39, 43, 53
 construction of 115
 of rings 161, 163, 179
 homomorphism theorems 36
 for rings 164
 Hopkins's theorem 198
- ideal, definition of 163
 ideal number 474
 idempotent 174, 181, 190, 191, 192, 196–
 197, 199, 207, 211, 429
 in group algebra 222, 224
 identity element 10
 identity element of ring (*see* unity element)
 identity map 4
 image of mapping 4
 imaginary number with rational power 324
 INC (*see* Incomparability theorem)
 Inclusion-exclusion principle 331
 Incomparability theorem 460
 indecomposable group 134, 136, 139
 indecomposable module 206
 indeterminate 233
 index of subgroup 23, 28, 44
 induced character 226
 induced class function 226
- infinite element 412
 infinitesimal element 412
 initial segment 154, 157
 injective homomorphism 32
 injective mapping 4
 inner automorphism 20–22, 39
 inner derivation 293, 305
 inner product 217, 224
 inseparable extension of fields 301–302, 369,
 482 (*see also* purely inseparable
 extension)
 inseparable polynomial 281, 297
 integer 454
 integers in field extension 457–458, 461–464,
 471, 482, 492
 integral basis 371, 463
 integral domain (*see* domain)
 integral element of overring 453–458
 integral extension of rings 458–462, 471–472
 integrally closed domain 454, 457, 473 (*see*
 also standard hypotheses)
 integrally closed subring 454–455
 intermediate field 260–261, 284, 286,
 290, 329
 internal direct product or sum 84–86
 intersection
 of algebraic sets 494
 of primary ideals 436, 440
 of maximal ideals 500
 of maximal right ideals 180
 of subgroups 15
 of Sylow subgroups 59, 66, 125
 inverse element 10
 inverse map 5
 invertible element of ring (*see* unit)
 invertible ideal 476–477, 484
 invertible fractional ideal 476–477
 involution 8
 irreducible algebraic set 499
 irreducible character 216–222, 224, 227, 229
 irreducible element of domain 237–242
 irreducible polynomial 245, 252, 260, 271,
 272
 set of roots 277
 over finite field 330–332
 isolated prime ideal 421–423, 430, 435, 440–
 441, 449
 isomorphism 11, 18, 30, 161 (*see also*
 X -isomorphism)
 of direct products 87
 of field extensions 262–263, 267 (*see also*
 F -isomorphism)
 of finite fields 327
 Isomorphism theorem 31, 36
 isotypic component 152–153

- Jacobi identity 305
 Jacobson density theorem 185
 Jacobson radical 179–184, 191, 192, 193,
 194–195, 198, 207, 211, 504
 Jordan, C. 81
 Jordan-Hölder theorem 38, 130, 132
- Kantor, W. 99
 Kaplansky's theorem 490
 kernel
 of action 43, 45
 of character 225
 of homomorphism 31, 35, 38, 162–164
 Klein group 78
 Krull dimension 448–449
 Krull intersection theorem 437
 Krull-Schmidt theorem 92, 135, 139–140
 Krull's theorem on heights of primes 444
 Kummer's theorem 347–348
 prime characteristic analog of 404
- Lagrange's theorem 23, 45
 converse of 55
 Landau's theorem 48
 Lasker-Noether decomposition 440
 Lasker-Noether theorem 436, 439
 lattice diagram 34, 40
 lcm (*see* least common multiple)
 leading coefficient 236
 least common multiple 312
 left artinian ring 171, 175
 left coset 22
 left ideal 163
 left inverse 5, 165
 left module 170
 left noetherian ring 171, 175
 length (*see* composition length)
 Levitsky's theorem 210
 Lie ring 294, 305
 Lindemann's theorem 316
 linear character 216–217
 number of 229
 linear independence of field automorphisms
 346
 linearly disjoint fields 387–388, 399
 linearly ordered set 143, 154
 LO (*see* Lying over theorem)
 local ring 173, 252, 427
 local subgroup 124
 localization 243, 246–249, 252–253, 426–
 428, 430, 445, 473, 491
 long division 236, 333
 lower central series 105–107, 111, 124
- Lüroth's theorem 262, 389, 391
 Lying over theorem 458–459
- Maschke's theorem 214
 Mathieu, E. 38
 matrix ring 160, 165, 169, 175, 188–189, 191,
 196, 200
 matrix unit 169
 maximal condition 144, 433
 on radical ideals 423
 maximal ideal 168, 191, 240, 419, 425–427,
 430, 444, 500–501
 maximal right ideal 180, 182
 maximal subgroup 27, 64, 97, 102, 107, 113,
 127
 maximally disjoint ideal 419
 metabelian group 41
 Migotti's theorem 310, 323
 minimal algebraic set 500
 minimal condition 144
 minimal normal subgroup 88, 97, 102, 113,
 114
 minimal polynomial 259, 298, 311, 362, 457
 minimal prime over an ideal (*see* isolated prime
 ideal)
 minimal right ideal 190, 196
 minimally potent right ideal 206–208, 212
 Möbius function 330
 module
 definition of 169
 over Dedekind domain 484–490
 over PID 250
 monic polynomial 236
 multiplication table 11
 multiplicative group 165, 260
 multiplicative system in ring 246–249, 419,
 430
- N/C theorem 41
 $n!$ theorem 44
 Nakayama's lemma 183
 Natural irrationalities theorem 288–289, 313,
 348, 353
 natural F -representation 359
 nil ideal 194–195, 209–210, 504
 nilpotence class 107, 112, 123, 127
 nilpotent element 173, 180, 181, 201, 341,
 420
 nilpotent endomorphism 135–136
 nilpotent finite group 89
 nilpotent group 105–110, 112, 113, 114
 nilpotent ideal 194–195, 209–210
 nilpotent matrix 214, 502
 nilradical 179, 420

- Noether, E. 145
 Noether's equations 366
 additive form 370
 noetherian commutative ring 238, 421, 428, 433–452
 noetherian module 170
 noetherian ring (*see* right noetherian ring, left noetherian ring, *or* noetherian commutative ring)
 noetherian X -group 145–149, 150, 157
 nonconstructible number 317
 nongenerator 27
 nonsimplicity criterion 44, 65, 75, 115, 120–124, 127 (*see also* group with given order)
 nonsolvable polynomial 345
 norm map for fields 360, 362–365, 376–377, 398
 normal closure 290
 normal complement 94
 normal endomorphism 135–136
 normal extension of fields 278–279, 282, 290, 301, 305
 normal p -complement 121–122, 123–124
 normal subgroup 20–21, 24, 28, 31, 37–38, 44–45, 79, 96
 normalizer 26, 28, 29, 46, 49, 58–59, 113
 normalizer growth 64, 107
 Nullstellensatz 495–496, 498, 500
- odd permutation 74–75, 372
 one-to-one 4
 onto 4
 operations of group 3
 operator set 129
 opposite ring 171, 182, 188–191
 orbit 46–48, 50
 order
 of group 7
 of element 8, 16–17, 24, 46
 of permutation 72
 ordered field 410–413
 orthogonal idempotents 211
 orthogonality of characters 217, 224
- p -group 57, 63–64, 68, 105, 107, 114
 p -local subgroup 124
 p -normal group 127
 p -regular element 124
 p -solvable group 141
 partially ordered set (*see* poset)
 Peirce decomposition 197
 Pell's equation 364–365
 perfect field 271, 297–299
 perfect group 113
 permutation 6, 70–75
 permutation character 50–51, 53
 permutation group 6, 14, 42
 physical motion 6, 7
 PID 233, 237, 240–241, 252, 474, 488, 490, 491
 module over 250
 PIR 163, 233, 238, 433, 481
 plane rotation 7
 point stabilizer 46, 77
 pointwise stabilizer 46
 Pólya, G. 51
 polynomial 233–235
 polynomial factorization (*see* Berlekamp algorithm)
 polynomial ring 234, 434, 444
 in several indeterminates 244–245, 253, 434, 449, 456, 500
 over field 237, 252
 over UFD 241–242
 polynomial with real roots 351
 poset 143–144, 154, 156, 157
 potent right ideal 206–208, 212
 power-sum polynomial 371
 primary ideal 425–428, 430–431, 436, 440, 491
 primary submodule 450
 prime annihilator 440, 442
 prime element of domain 239–243, 245
 prime ideal
 and localization 252, 427–428, 430
 associated 440–442, 450
 definition of 195, 239
 embedded 442, 450, 452
 height of 444, 446–448
 in Dedekind domain 475–477, 480
 in general commutative ring 418–432, 451, 483, 491
 in integral extension 458–461
 in noetherian commutative ring 438, 440, 446, 448, 476, 491
 isolated 421–423, 430, 435, 440–441, 449
 union of 424, 447
 prime ring 195
 prime spectrum (*see* spectrum)
 prime subfield 326
 primitive element in field extension 260, 272
 Primitive element theorem 284
 primitive ideal 179, 187, 191
 primitive idempotent 211
 primitive permutation group 81
 primitive polynomial 241–243
 primitive ring 187, 189, 191, 192
 primitive root of unity 307–308, 323
 principal character 216

- principal crossed homomorphism 367–368, 370
 principal fractional ideal 475
 principal ideal 163, 233, 423–424, 440, 450, 480
 principal ideal ring (*see* PIR)
 principal ideal domain (*see* PID)
 Principal ideal theorem 444
 probability 53, 332, 367
 product of subgroups 22, 25–26, 50, 108, 113
 projective indecomposable module 206, 208
 projective general linear group 400
 projective module 204–206, 208, 484–485, 488
 pure subgroup 98
 purely inseparable extension 298–302, 306, 377
 purely transcendental extension 380–382, 388–389
- quotient field (*see* field of fractions)
 quotient group (*see* factor group)
 quasiregular element 180
 quaternion group 13, 28, 39
 quaternion division ring 166, 167, 176
- radical 342–343
 radical extension of fields 342–343, 347, 358
 radical ideal 421, 423, 430, 435, 452, 498–499
 radical of ideal 420–422, 429–431, 437, 440, 494
 radical of ring 179 (*see also* Jacobson radical)
 range of mapping 4
 rank
 of free module 175
 of torsion-free module 486–487
 rational function field 254, 380
 rational integer 454
 Rational root theorem 455
 real radical extension 324, 351–354
 realclosed field 405–410, 415–416
 regular action 43
 regular character 216, 222
 regular extension of fields 398
 regular module 170, 188, 202, 206
 regular polygon 315, 321
 regular permutation group 12
 regular representation 216
 relatively prime polynomials 389–390, 399
 repeated radical extension 343–344, 351
 repeated square-root extension 357
 representation 114, 128, 186, 213, 215–216, 219, 223
 diagonal matrix in 223
 of field 359
 representative set of modules 199, 219–221
 residually finite group 291
 restricted direct product 86
 restriction of character 225–226, 230
 right artinian ring 171–172, 175, 194–196, 198, 201, 206–209, 211–212 (*see also* Wedderburn ring)
 right artinian simple ring 187, 189, 191
 right coset 22
 right cosets, action on 43, 45
 right ideal 163
 right inverse 5, 165
 right module (*see* module)
 right noetherian ring 171–172, 175, 176, 198, 210
 right quasiregular element 180–181
 ring, definition of 159
 ring with unit 160
 root of polynomial 254, 261, 265, 272, 342 (*see also* distinct roots)
 existence in extension field 265
 root of unity 307, 311, 347–348, 471 (*see also* primitive root of unity)
 rotation 6, 7, 48
 rotation group 7, 8, 11
 of cube 8, 11–12
 Rubik cube puzzle 8, 9
- Schafarevitch's theorem 314
 Schreier generators of subgroup 128
 Schur, I. 118
 Schur multiplier 118
 Schur-Zassenhaus theorem 103
 Schur's lemma 167, 174
 Schur's theorem on center with finite index 119–120, 128
 semidirect product 95
 semisimple 149, 199
 semifoo ring 187
 semiprime ring 195, 210–211
 semiprimitive ring 187, 214–215
 separable element 281
 separable elements, set of 300
 separable extension of fields 278, 281–282, 284, 290, 298, 369, 461–462
 separable part of degree 302–303, 305
 separable polynomial 280–282, 298
 setwise stabilizer 46
 shoes 145
 similar matrices 359
 similar representations 216
 simple field extension 260

- simple group 37–38, 44, 68, 77, 95, 99, 126, 127, 140, 468
- simple module 170, 178–179, 184–187, 190, 199, 209, 212
 - representative set for 199, 219–221
- simple ring 169, 187, 189
- socks 145
- socle 96
- solvable by radicals 344 (*see also* solvable polynomial)
- solvable group 99–103, 113, 140, 156, 157–158
 - chief factor of 102
 - maximal subgroup of 102, 113
- solvable polynomial 99–100, 274, 342–343, 350
- special linear group 31
- specialization 396
- spectrum 420, 424, 429, 443, 459
- split extension 94, 97
- split polynomial 264–266, 272
- splitting field 266–267, 277–279, 282, 290, 327, 351
 - degree of 273
- sporadic simple group 38
- square roots of primes 291
- square-root extension 357
- squaring a circle 315–317
- squaring a geometric figure 316, 325
- stabilizer 46, 47
- standard hypotheses 461–462
- standard primary decomposition 440
- straightedge 315–316
- subfield of finite field 328–329
- subgroup
 - definition of 14
 - of abelian group 41
 - of cyclic group 17
 - of factor group 36
- subgroup generation 15
- submodule 170
- subring 161
- sum of squares 405–406, 415
- summand multiplicity function 130
- supersolvable group 102, 113, 133
- surjective homomorphism 32, 35, 40, 53, 67, 100
- surjective mapping 4
- Sylow C-theorem 57
- Sylow counting theorem 59
- Sylow D-theorem 57
- Sylow E-theorem 56
- Sylow subgroup 56–59, 89, 107, 108, 121
 - abelian 118, 122–123
 - cyclic 82, 118, 122, 127
 - intersection of 59, 66, 125
 - fusion in 121, 124, 125
 - normalizer of 58, 59, 67, 113, 122–123, 127
- Sylow theorem analog 104
- Sylow theorems 44, 55–57, 59
- symbolic power 428, 430
- symmetric group 6, 11, 14, 43, 70–77, 79
 - as Galois group 292, 345, 358, 396
 - automorphism of 79–80
 - normal subgroup of 79
- symmetric group element, order of 72
- symmetric polynomial 371–372, 395–396 (*see also* elementary symmetric function)
- symmetry group 7, 8, 47
- target of mapping 4
- Three subgroups lemma 111–112
- Thompson, J. 126, 128
- Thompson subgroup 126
- topological space 429, 494, 504
- torsion-free module 250, 484, 486–487
- torsion submodule 491
- totally ordered set (*see* linearly ordered set)
- totally transcendental extension 258, 272, 380–381, 389
- totient function (*see* Euler's function)
- trace of matrix 214, 359–361
- trace map for fields 360, 362–364, 369, 370, 376–377, 398
- transcendence basis 382–385, 399
- transcendence degree 385, 391, 504–505
- transcendental element 254–255, 258, 379–380, 390
 - over rational numbers 270, 316
- transcendental extension 379–400 (*see also* totally transcendental extension *and* purely transcendental extension)
- transfer 115–120
- Transfer evaluation lemma 118–119
- transformation group 3
- transitive action 46
 - of Galois group 277
- transitive group 12
- transposition 74
- transversal 27, 115–116
- trisecting an angle 315, 317
- trivial action 42, 367
- two-generator ideal 475, 482
- UFD 239–245, 251, 252, 454, 490
- union
 - of algebraic sets 494, 499
 - of subgroups 26, 27, 49, 147
 - of prime ideals 424, 447
- unique factorization domain (*see* UFD)

- uniqueness of factorization 238, 474
- unit 165, 168, 173, 211, 238–239, 241
- unity element 160
- unitary overring 235, 453, 472
- unitary subring 160, 176
- unrestricted direct product 86
- upper bound 154
- upper central series 105–107

- Vandermonde matrix 373
- variety 499
- von Neumann regular ring 191, 430–431

- weak generating set 486
- Wedderburn, M. 169, 176
- Wedderburn ring 196–199, 205
- Wedderburn-Artin theorems 196
- Wedderburn-Artin structure theorem 199, 220
- Wedderburn-Artin classification theorem 200
- Wedderburn's theorem on finite division rings 339
- Wielandt, H. 56

- weakly closed subgroup 127
- well-ordered set 154
- wreath product 123

- X -composition series 131–132
- X -endomorphism 135, 161
- X -group 129–141
- X -homomorphism 130, 167
- X -isomorphism 130
- X -series 131
- X -simple X -groups 131, 149, 151–153, 167
- X -subgroup 130

- Yoshida, T. 123

- Zariski topology 494, 504
- Zariski's theorem 496
- zero divisor 452
- zero-set of polynomials 493
- Zorn's lemma 150, 153–156, 269, 382, 399, 415, 421–422

This book, based on a first-year graduate course the author taught at the University of Wisconsin, contains more than enough material for a two-semester graduate-level abstract algebra course, including groups, rings and modules, fields and Galois theory, an introduction to algebraic number theory, and the rudiments of algebraic geometry. In addition, there are some more specialized topics not usually covered in such a course. These include transfer and character theory of finite groups, modules over artinian rings, modules over Dedekind domains, and transcendental field extensions.

This book could be used for self study as well as for a course text, and so full details of almost all proofs are included, with nothing being relegated to the chapter-end problems. There are, however, hundreds of problems, many being far from trivial. The book attempts to capture some of the informality of the classroom, as well as the excitement the author felt when taking the corresponding course as a student.

ISBN 978-0-8218-4799-2



9 780821 847992

GSM/100



For additional information
and updates on this book, visit

www.ams.org/bookpages/gsm-100

AMS *on the Web*
www.ams.org