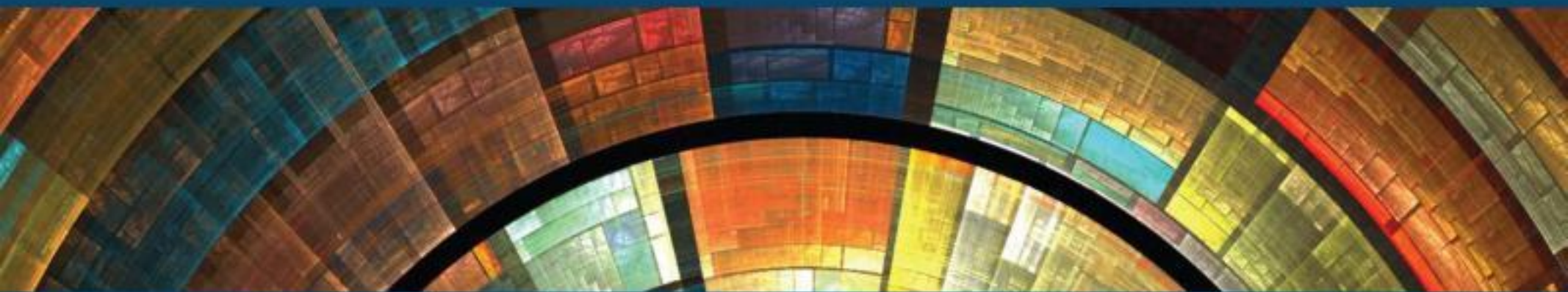


Paul B. Garrett



ABSTRACT ALGEBRA



Chapman & Hall/CRC
Taylor & Francis Group

Chapman & Hall/CRC
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2008 by Taylor & Francis Group, LLC
Chapman & Hall/CRC is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-58488-689-1 (Hardcover)

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

No part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC) 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Garrett, Paul B.
Abstract algebra / Paul B. Garrett.
p. cm.
Includes index.
ISBN 978-1-58488-689-1 (hardback : alk. paper)
1. Algebra, Abstract--Textbooks. I. Title.

QA162.G375 2007
512'.02--dc22

2007028460

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

Preface

Introduction

1	The integers	1
1.1	Unique factorization	1
1.2	Irrationalities	6
1.3	$\mathbb{Z}/m$, the integers mod m	7
1.4	Fermat's little theorem	9
1.5	Sun-Ze's theorem	12
1.6	Worked examples	13
	Exercises	16
2	Groups I	19
2.1	Groups	19
2.2	Subgroups, Lagrange's theorem	21
2.3	Homomorphisms, kernels, normal subgroups	25
2.4	Cyclic groups	27
2.5	Quotient groups	29
2.6	Groups acting on sets	32
2.7	The Sylow theorem	34
2.8	Trying to classify finite groups, part I	37
2.9	Worked examples	47
	Exercises	49
3	The players: rings, fields, etc.	51
3.1	Rings, fields	51
3.2	Ring homomorphisms	54
3.3	Vector spaces, modules, algebras	56
3.4	Polynomial rings I	59
	Exercises	63
4	Commutative rings I	65
4.1	Divisibility and ideals	65
4.2	Polynomials in one variable over a field	67
4.3	Ideals	70
4.4	Ideals and quotient rings	73
4.5	Maximal ideals and fields	74
4.6	Prime ideals and integral domains	75
4.7	Fermat-Euler on sums of two squares	76
4.8	Worked examples	79
	Exercises	83
5	Linear algebra I: dimension	85
5.1	Some simple results	85
5.2	Bases and dimension	86
5.3	Homomorphisms and dimension	88
	Exercises	90

6	Fields I	91
6.1	Adjoining things	91
6.2	Fields of fractions, fields of rational functions	95
6.3	Characteristics, finite fields	97
6.4	Algebraic field extensions	99
6.5	Algebraic closures	103
	Exercises	105
7	Some irreducible polynomials	107
7.1	Irreducibles over a finite field	107
7.2	Worked examples	110
	Exercises	112
8	Cyclotomic polynomials	115
8.1	Multiple factors in polynomials	115
8.2	Cyclotomic polynomials	117
8.3	Examples	121
8.4	Finite subgroups of fields	123
8.5	Infinitude of primes $p \equiv 1 \pmod n$	124
8.6	Worked examples	125
	Exercises	128
9	Finite fields	131
9.1	Uniqueness	131
9.2	Frobenius automorphisms	133
9.3	Counting irreducibles	136
	Exercises	137
10	Modules over PIDs	139
10.1	The structure theorem	139
10.2	Variations	140
10.3	Finitely-generated abelian groups	142
10.4	Jordan canonical form	144
10.5	Conjugacy versus $k[x]$ -module isomorphism	149
10.6	Worked examples	157
	Exercises	165
11	Finitely-generated modules	167
11.1	Free modules	167
11.2	Finitely-generated modules over a domain	171
11.3	PIDs are UFDs	174
11.4	Structure theorem, again	176
11.5	Recovering the earlier structure theorem	178
11.6	Submodules of free modules	179
	Exercises	180
12	Polynomials over UFDs	181
12.1	Gauss' lemma	181
12.2	Fields of fractions	183
12.3	Worked examples	186
	Exercises	190

13 Symmetric groups	191
13.1 Cycles, disjoint cycle decompositions	191
13.2 Transpositions	192
13.3 Worked examples	193
Exercises	197
14 Naive set theory	199
14.1 Sets	199
14.2 Posets, ordinals	202
14.3 Transfinite induction	206
14.4 Finiteness, infiniteness	207
14.5 Comparison of infinities	207
14.6 Example: transfinite Lagrange replacement	209
14.7 Equivalents of the Axiom of Choice	210
Exercises	212
15 Symmetric polynomials	213
15.1 The theorem	213
15.2 First examples	215
15.3 A variant: discriminants	217
Exercises	218
16 Eisenstein's criterion	219
16.1 Eisenstein's irreducibility criterion	219
16.2 Examples	220
Exercises	221
17 Vandermonde determinants	223
17.1 Vandermonde determinants	223
17.2 Worked examples	227
Exercises	230
18 Cyclotomic polynomials II	233
18.1 Cyclotomic polynomials over $\mathbb{Z}$	233
18.2 Worked examples	235
Exercises	240
19 Roots of unity	243
19.1 Another proof of cyclicity	243
19.2 Roots of unity	244
19.3 $\mathbb{Q}$ with roots of unity adjoined	245
19.4 Solution in radicals, Lagrange resolvents	251
19.5 Quadratic fields, quadratic reciprocity	256
19.6 Worked examples	260
Exercises	268
20 Cyclotomic III	269
20.1 Prime-power cyclotomic polynomials over $\mathbb{Q}$	269
20.2 Irreducibility of cyclotomic polynomials over $\mathbb{Q}$	271
20.3 Factoring $\Phi_n(x)$ in $\mathbb{F}_p[x]$ with $p n$	272
20.4 Worked examples	273
Exercises	289

21	Primes in arithmetic progressions	291
21.1	Euler's theorem and the zeta function	291
21.2	Dirichlet's theorem	293
21.3	Dual groups of abelian groups	296
21.4	Non-vanishing on $\operatorname{Re}(s) = 1$	298
21.5	Analytic continuations	300
21.6	Dirichlet series with positive coefficients	301
22	Galois theory	303
22.1	Field extensions, imbeddings, automorphisms	304
22.2	Separable field extensions	305
22.3	Primitive elements	308
22.4	Normal field extensions	309
22.5	The main theorem	311
22.6	Conjugates, trace, norm	313
22.7	Basic examples	314
22.8	Worked examples	315
	Exercises	325
23	Solving equations by radicals	327
23.1	Galois' criterion	327
23.2	Composition series, Jordan-Hölder theorem	329
23.3	Solving cubics by radicals	329
23.4	Worked examples	332
	Exercises	336
24	Eigenvectors, spectral theorems	337
24.1	Eigenvectors, eigenvalues	337
24.2	Diagonalizability, semi-simplicity	340
24.3	Commuting endomorphisms $ST = TS$	343
24.4	Inner product spaces	344
24.5	Projections without coordinates	349
24.6	Unitary operators	350
24.7	Spectral theorems	351
24.8	Corollaries of the spectral theorem	352
24.9	Worked examples	354
	Exercises	360
25	Duals, naturality, bilinear forms	361
25.1	Dual vector spaces	361
25.2	First example of naturality	365
25.3	Bilinear forms	367
25.4	Worked examples	370
	Exercises	376
26	Determinants I	379
26.1	Prehistory	379
26.2	Definitions	382
26.3	Uniqueness and other properties	382
26.4	Existence	387
	Exercises	387

27	Tensor products	389
27.1	Desiderata	389
27.2	Definitions, uniqueness, existence	391
27.3	First examples	395
27.4	Tensor products $f \otimes g$ of maps	398
27.5	Extension of scalars, functoriality, naturality	399
27.6	Worked examples	402
	Exercises	413
28	Exterior powers	415
28.1	Desiderata	415
28.2	Definitions, uniqueness, existence	416
28.3	Some elementary facts	419
28.4	Exterior powers $\bigwedge^n f$ of maps	421
28.5	Exterior powers of free modules	422
28.6	Determinants revisited	425
28.7	Minors of matrices	426
28.8	Uniqueness in the structure theorem	427
28.9	Cartan's lemma	428
28.10	Cayley-Hamilton theorem	430
28.11	Worked examples	432
	Exercises	443
	Index	445