P.M. Cohn

Basic Algebra

Groups, Rings and Fields

Springer

P.M. Cohn, MA, PhD, FRS
Department of Mathematics, University College London,
Gower Street, London WC1E 6BT, UK

British Library Cataloguing in Publication Data
Cohn, P. M. (Paul Moritz)
Basic algebra: groups, rings and fields
I. Algebra 2. Rings (Algebra) 3. Algebraic fields
I. Title
512
ISBN 978-1-4471-1060-6

Library of Congress Cataloging-in-Publication Data
Cohn, P.M. (Paul Moritz)
Basic algebra: groups, rings, and fields/P.M. Cohn.
p. cm.
Includes bibliographical references and indexes.
ISBN 978-1-4471-1060-6 ISBN 978-0-85729-428-9 (eBook)
DOI 10.1007/978-0-85729-428-9
1. Algebra. I. Title.

QA154.3.C64 2002
512–dc21 2002070686

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

springeronline.com

© Professor P.M. Cohn 2003
Originally published by Springer-Verlag London Berlin Heidelberg in 2003
Softcover reprint of the hardcover 1st edition 2003

2nd printing 2005

The use of registered names, trademarks etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Typesetting by BC Typesetting, Bristol BS31 1NZ
12/3830-54321 Printed on acid-free paper SPIN 11329916

Contents

Preface ix
Conventions on Terminology xi

1. Sets
   - 1.1 Finite, Countable and Uncountable Sets 1
   - 1.2 Zorn's Lemma and Well-ordered Sets 8
   - 1.3 Graphs 15

2. Groups
   - 2.1 Definition and Basic Properties 25
   - 2.2 Permutation Groups 32
   - 2.3 The Isomorphism Theorems 34
   - 2.4 Soluble and Nilpotent Groups 37
   - 2.5 Commutators 42
   - 2.6 The Frattini Subgroup and the Fitting Subgroup 46

3. Lattices and Categories
   - 3.1 Definitions; Modular and Distributive Lattices 51
   - 3.2 Chain Conditions 60
   - 3.3 Categories 65
   - 3.4 Boolean Algebras 70

4. Rings and Modules
   - 4.1 The Definitions Recalled 79
   - 4.2 The Category of Modules over a Ring 84
   - 4.3 Semisimple Modules 91
   - 4.4 Matrix Rings 96
   - 4.5 Direct Products of Rings 101
   - 4.6 Free Modules 105
   - 4.7 Projective and Injective Modules 110
   - 4.8 The Tensor Product of Modules 117
   - 4.9 Duality of Finite Abelian Groups 125

5. Algebras
5.1 Algebras; Definition and Examples 131
5.2 The Wedderburn Structure Theorems 137
5.3 The Radical 141
5.4 The Tensor Product of Algebras 146
5.5 The Regular Representation; Norm and Trace 153
5.6 Möbius Functions 157

6. Multilinear Algebra
6.1 Graded Algebras 165
6.2 Free Algebras and Tensor Algebras 168
6.3 The Hilbert Series of a Graded Ring or Module 173
6.4 The Exterior Algebra on a Module 179

7. Field Theory
7.1 Fields and their Extensions 189
7.2 Splitting Fields 195
7.3 The Algebraic Closure of a Field 200
7.4 Separability 203
7.5 Automorphisms of Field Extensions 206
7.6 The Fundamental Theorem of Galois Theory 211
7.7 Roots of Unity 217
7.8 Finite Fields 223
7.9 Primitive Elements; Norm and Trace 227
7.10 Galois Theory of Equations 232
7.11 The Solution of Equations by Radicals 238

8. Quadratic Forms and Ordered Fields
8.1 Inner Product Spaces 249
8.2 Orthogonal Sums and Diagonalization 252
8.3 The Orthogonal Group of a Space 256
8.4 The Clifford Algebra and the Spinor Norm 259
8.5 Witt's Cancellation Theorem and the Witt Group of a Field 268
8.6 Ordered Fields 272
8.7 The Field of Real Numbers 275
8.8 Formally Real Fields 279
8.9 The Witt Ring of a Field 291
8.10 The Symplectic Group 298
8.11 Quadratic Forms in Characteristic Two 301

9. Valuation Theory
9.1 Divisibility and Valuations 307
9.2 Absolute Values 312
9.3 The p-adic Numbers 322
9.4 Integral Elements 331
9.5 Extension of Valuations 336

10. Commutative Rings
10.1 Operations on Ideals 347
10.2 Prime Ideals and Factorization 349
10.3 Localization 354
10.4 Noetherian Rings 361
10.5 Dedekind Domains 362
10.6 Modules over Dedekind Domains 371
10.7 Algebraic Equations 376
10.8 The Primary Decomposition 380
10.9 Dimension 386
10.10 The Hilbert Nullstellensatz 391

11. Infinite Field Extensions
11.1 Abstract Dependence Relations 397
11.2 Algebraic Dependence 402
11.3 Simple Transcendental Extensions 405
11.4 Separable and p-radical Extensions 409
11.5 Derivations 414
11.6 Linearly Disjoint Extensions 418
11.7 Composites of Fields 427
11.8 Infinite Algebraic Extensions 431
11.9 Galois Descent 437
11.10 Kummer Extensions 441

Bibliography 449
List of Notations 453
Author Index 457
Subject Index 459