

Basic Algebra II

NATHAN JACOBSON

Basic Algebra II

NATHAN JACOBSON

YALE UNIVERSITY



W. H. FREEMAN AND COMPANY
San Francisco

Sponsoring Editor: Peter Renz
Project Editor: Patricia Brewer
Copyeditor: Tate Snyder
Production Coordinator: William Murdock
Compositor: Typesetting Services Limited
Printer and Binder: The Maple-Vail Book
Manufacturing Group

Library of Congress Cataloging in Publication Data

Jacobson, Nathan, 1910-
Basic algebra.

Includes bibliographical references.

1. Algebra. I. Title.
QA154.2.J32 512.9 73-22316
ISBN 0-7167-1079-X (v. 2)

Copyright © 1980 by W. H. Freeman and Company

No part of this book may be reproduced
by any mechanical, photographic, or electronic process,
or in the form of a phonographic recording,
nor may it be stored in a retrieval system, transmitted,
or otherwise copied for public or private use,
without written permission from the publisher.

Printed in the United States of America

Preface

This volume is a text for a second course in algebra that presupposes an introductory course covering the type of material contained in the Introduction and the first three or four chapters of *Basic Algebra I*. These chapters dealt with the rudiments of set theory, group theory, rings, modules, especially modules over a principal ideal domain, and Galois theory focused on the classical problems of solvability of equations by radicals and constructions with straight-edge and compass.

Basic Algebra II contains a good deal more material than can be covered in a year's course. Selection of chapters as well as setting limits within chapters will be essential in designing a realistic program for a year. We briefly indicate several alternatives for such a program: Chapter 1 with the addition of section 2.9 as a supplement to section 1.5, Chapters 3 and 4, Chapter 6 to section 6.11, Chapter 7 to section 7.13, sections 8.1–8.3, 8.6, 8.12, Chapter 9 to section 9.13. A slight modification of this program would be to trade off sections 4.6–4.8 for sections 5.1–5.5 and 5.9. For students who have had no Galois theory it will be desirable to supplement section 8.3 with some of the material of Chapter 4 of *Basic Algebra I*. If an important objective of a course in algebra is an understanding of the foundations of algebraic structures and the

relation between algebra and mathematical logic, then all of Chapter 2 should be included in the course. This, of course, will necessitate thinning down other parts, e.g., homological algebra. There are many other possibilities for a one-year course based on this text.

The material in each chapter is treated to a depth that permits the use of the text also for specialized courses. For example, Chapters 3, 4, and 5 could constitute a one-semester course on representation theory of finite groups, and Chapter 7 and parts of Chapters 8, 9, and 10 could be used for a one-semester course in commutative algebras. Chapters 1, 3, and 6 could be used for an introductory course in homological algebra.

Chapter 11 on real fields is somewhat isolated from the remainder of the book. However, it constitutes a direct extension of Chapter 5 of *Basic Algebra I* and includes a solution of Hilbert's problem on positive semi-definite rational functions, based on a theorem of Tarski's that was proved in Chapter 5 of the first volume. Chapter 11 also includes Pfister's beautiful theory of quadratic forms that gives an answer to the question of the minimum number of squares required to express a sum of squares of rational functions of n real variables (see section 11.5).

Aside from its use as a text for a course, the book is designed for independent reading by students possessing the background indicated. A great deal of material is included. However, we believe that nearly all of this is of interest to mathematicians of diverse orientations and not just to specialists in algebra. We have kept in mind a general audience also in seeking to reduce to a minimum the technical terminology and in avoiding the creation of an overly elaborate machinery before presenting the interesting results. Occasionally we have had to pay a price for this in proofs that may appear a bit heavy to the specialist.

Many exercises have been included in the text. Some of these state interesting additional results, accompanied with sketches of proofs. Relegation of these to the exercises was motivated simply by the desire to reduce the size of the text somewhat. The reader would be well advised to work a substantial number of the exercises.

An extensive bibliography seemed inappropriate in a text of this type. In its place we have listed at the end of each chapter one or two specialized texts in which the reader can find extensive bibliographies on the subject of the chapter. Occasionally, we have included in our short list of references one or two papers of historical importance. None of this has been done in a systematic or comprehensive manner.

Again it is a pleasure for me to acknowledge the assistance of many friends in suggesting improvements of earlier versions of this text. I should mention first the students whose perceptions detected flaws in the exposition and sometimes suggested better proofs that they had seen elsewhere. Some of the students

who have contributed in this way are Monica Barattieri, Ying Cheng, Daniel Corro, William Ellis, Craig Huneke, and Kenneth McKenna. Valuable suggestions have been communicated to me by Professors Kevin McCrimmon, James D. Reid, Robert L. Wilson, and Daniel Zelinsky. I have received such suggestions also from my colleagues Professors Walter Feit, George Seligman, and Tsuneo Tamagawa. The arduous task of proofreading was largely taken over by Ying Cheng, Professor Florence Jacobson, and James Reid. Florence Jacobson assisted in compiling the index. Finally we should mention the fine job of typing that was done by Joyce Harry and Donna Belli. I am greatly indebted to all of these individuals, and I take this opportunity to offer them my sincere thanks.

January 1980

Nathan Jacobson

Contents

Contents of *Basic Algebra I* xiii

Preface xvii

INTRODUCTION 1

- 0.1 Zorn's lemma 2
- 0.2 Arithmetic of cardinal numbers 3
- 0.3 Ordinal and cardinal numbers 4
- 0.4 Sets and classes 6

1 CATEGORIES 8

- 1.1 Definition and examples of categories 9
- 1.2 Some basic categorical concepts 15
- 1.3 Functors and natural transformations 18
- 1.4 Equivalence of categories 26
- 1.5 Products and coproducts 32
- 1.6 The hom functors. Representable functors 37
- 1.7 Universals 41
- 1.8 Adjoints 46

2 UNIVERSAL ALGEBRA 52

- 2.1 Ω -algebras 53
- 2.2 Subalgebras and products 58
- 2.3 Homomorphisms and congruences 60
- 2.4 The lattice of congruences Subdirect products 66
- 2.5 Direct and inverse limits 70
- 2.6 Ultraproducts 75
- 2.7 Free Ω -algebras 78

- 2.8 Varieties 81
- 2.9 Free products of groups 87
- 2.10 Internal characterization of varieties 91

3 MODULES 94

- 3.1 The categories $R\text{-mod}$ and $\text{mod-}R$ 95
- 3.2 Artinian and Noetherian modules 100
- 3.3 Schreier refinement theorem. Jordan-Hölder theorem 104
- 3.4 The Krull-Schmidt theorem 110
- 3.5 Completely reducible modules 117
- 3.6 Abstract dependence relations. Invariance of dimensionality 122
- 3.7 Tensor products of modules 125
- 3.8 Bimodules 133
- 3.9 Algebras and coalgebras 137
- 3.10 Projective modules 148
- 3.11 Injective modules. Injective hull 156
- 3.12 Morita contexts 164
- 3.13 The Wedderburn-Artin theorem for simple rings 171
- 3.14 Generators and progenerators 173
- 3.15 Equivalence of categories of modules 177

4 BASIC STRUCTURE THEORY OF RINGS 184

- 4.1 Primitivity and semi-primitivity 185
- 4.2 The radical of a ring 192
- 4.3 Density theorems 197
- 4.4 Artinian rings 202
- 4.5 Structure theory of algebras 210
- 4.6 Finite dimensional central simple algebras 215
- 4.7 The Brauer group 226
- 4.8 Clifford algebras 228

5 CLASSICAL REPRESENTATION THEORY OF FINITE GROUPS 246

- 5.1 Representations and matrix representation of groups 247
- 5.2 Complete reducibility 251
- 5.3 Application of the representation theory of algebras 257
- 5.4 Irreducible representations of S_n 265
- 5.5 Characters. Orthogonality relations 269
- 5.6 Direct products of groups. Characters of abelian groups 279
- 5.7 Some arithmetical considerations 282
- 5.8 Burnside's $p^a q^b$ theorem 284
- 5.9 Induced modules 286

- 5.10 Properties of induction. Frobenius reciprocity theorem 292
- 5.11 Further results on induced modules 299
- 5.12 Brauer's theorem on induced characters 305
- 5.13 Brauer's theorem on splitting fields 313
- 5.14 The Schur index 314
- 5.15 Frobenius groups 317

6 ELEMENTS OF HOMOLOGICAL ALGEBRA WITH APPLICATIONS 326

- 6.1 Additive and abelian categories 327
- 6.2 Complexes and homology 331
- 6.3 Long exact homology sequence 334
- 6.4 Homotopy 337
- 6.5 Resolutions 339
- 6.6 Derived functors 342
- 6.7 Ext 346
- 6.8 Tor 353
- 6.9 Cohomology of groups 355
- 6.10 Extensions of groups 363
- 6.11 Cohomology of algebras 370
- 6.12 Homological dimension 375
- 6.13 Koszul's complex and Hilbert's syzygy theorem 378

7 COMMUTATIVE IDEAL THEORY: GENERAL THEORY AND NOETHERIAN RINGS 388

- 7.1 Prime ideals. Nil radical 389
- 7.2 Localization of rings 393
- 7.3 Localization of modules 397
- 7.4 Localization at the complement of a prime ideal.
Local-global relations 400
- 7.5 Prime spectrum of a commutative ring 403
- 7.6 Integral dependence 408
- 7.7 Rank of projective modules 411
- 7.8 Projective class group 416
- 7.9 Noetherian rings 417
- 7.10 Commutative artinian rings 422
- 7.11 Affine algebraic varieties. The Hilbert Nullstellensatz 424
- 7.12 Primary decompositions 430
- 7.13 Artin-Rees lemma. Krull intersection theorem 437
- 7.14 Hilbert's polynomial for a graded module 440
- 7.15 The characteristic polynomial of a noetherian local ring 445
- 7.16 Krull dimension 447
- 7.17 I -adic topologies and completions 451

8 FIELD THEORY 459

- 8.1 Algebraic closure of a field 460
- 8.2 The Jacobson-Bourbaki correspondence 464
- 8.3 Finite Galois theory 467
- 8.4 Crossed products and the Brauer group 471
- 8.5 Cyclic algebras 480
- 8.6 Infinite Galois theory 482
- 8.7 Separability and normality 485
- 8.8 Separable splitting fields 491
- 8.9 Kummer extensions 494
- 8.10 Rings of Witt vectors 497
- 8.11 Abelian p -extensions 505
- 8.12 Transcendence bases 510
- 8.13 Luroth's theorem 513
- 8.14 Separability for arbitrary extension fields 517
- 8.15 Derivations 522
- 8.16 Galois theory for purely inseparable extensions of exponent one 533

9 VALUATION THEORY 537

- 9.1 Absolute values 538
- 9.2 The approximation theorem 542
- 9.3 Absolute values on \mathbb{Q} and $F(x)$ 544
- 9.4 Completion of a field 546
- 9.5 Finite dimensional extensions of complete fields.
The archimedean case 549
- 9.6 Valuations 554
- 9.7 Valuation rings and places 558
- 9.8 Extension of homomorphisms and valuations 561
- 9.9 Determination of the absolute values of a finite dimensional extension field 565
- 9.10 Ramification index and residue degree. Discrete valuations 568
- 9.11 Hensel's lemma 572
- 9.12 Local fields 575
- 9.13 Totally disconnected locally compact division rings 579
- 9.14 The Brauer group of a local field 588
- 9.15 Quadratic forms over local fields 591

10 DEDEKIND DOMAINS 599

- 10.1 Fractional ideals. Dedekind domains 600
- 10.2 Characterizations of Dedekind domains 605
- 10.3 Integral extensions of Dedekind domains 611
- 10.4 Connections with valuation theory 614
- 10.5 Ramified primes and the discriminant 619
- 10.6 Finitely generated modules over a Dedekind domain 623

11 FORMALLY REAL FIELDS 630

- 11.1 Formally real fields 631
- 11.2 Real closures 635
- 11.3 Totally positive elements 637
- 11.4 Hilbert's seventeenth problem 640
- 11.5 Pfister theory of quadratic forms 643
- 11.6 Sums of squares in $R(x_1, \dots, x_n)$, R a real closed field 649
- 11.7 Artin-Schreier characterization of real closed fields 654

INDEX 659

Contents of Basic Algebra I

INTRODUCTION: CONCEPTS FROM SET THEORY. THE INTEGERS 1

- 0.1 The power set of a set 2
- 0.2 The Cartesian product set. Maps 4
- 0.3 Equivalence relations. Factoring a map through an equivalence relation 10
- 0.4 The natural numbers 15
- 0.5 The number system \mathbb{Z} of integers 19
- 0.6 Some basic arithmetic facts about \mathbb{Z} 21
- 0.7 A word on cardinal numbers 24

1 MONOIDS AND GROUPS 26

- 1.1 Monoids of transformations and abstract monoids 28
- 1.2 Groups of transformations and abstract groups 31
- 1.3 Isomorphism. Cayley's theorem 37
- 1.4 Generalized associativity. Commutativity 39
- 1.5 Submonoids and subgroups generated by a subset.
Cyclic groups 42
- 1.6 Cycle decomposition of permutations 48
- 1.7 Orbits. Cosets of a subgroup 51
- 1.8 Congruences. Quotient monoids and groups 53
- 1.9 Homomorphisms 57
- 1.10 Subgroups of a homomorphic image.
Two basic isomorphism theorems 62
- 1.11 Free objects. Generators and relations 65
- 1.12 Groups acting on sets 69
- 1.13 Sylow's theorems 78

2 RINGS 83

- 2.1 Definition and elementary properties 84
- 2.2 Types of rings 87
- 2.3 Matrix rings 90
- 2.4 Quaternions 95
- 2.5 Ideals, quotient rings 98
- 2.6 Ideals and quotient rings for \mathbb{Z} 101
- 2.7 Homomorphisms of rings. Basic theorems 103
- 2.8 Anti-isomorphisms 108
- 2.9 Field of fractions of a commutative domain 111
- 2.10 Polynomial rings 116
- 2.11 Some properties of polynomial rings and applications 123
- 2.12 Polynomial functions 129
- 2.13 Symmetric polynomials 133
- 2.14 Factorial monoids and rings 135
- 2.15 Principal ideal domains and Euclidean domains 141
- 2.16 Polynomial extensions of factorial domains 146
- 2.17 "Rngs" (rings without unit) 149

3 MODULES OVER A PRINCIPAL IDEAL DOMAIN 152

- 3.1 Ring of endomorphisms of an abelian group 153
- 3.2 Left and right modules 158
- 3.3 Fundamental concepts and results 161
- 3.4 Free modules and matrices 164
- 3.5 Direct sums of modules 170
- 3.6 Finitely generated modules over a p.i.d.
Preliminary results 173
- 3.7 Equivalence of matrices with entries in a p.i.d. 175
- 3.8 Structure theorem for finitely generated modules
over a p.i.d. 181
- 3.9 Torsion modules, primary components, invariance
theorem 183
- 3.10 Applications to abelian groups and to linear
transformations 188
- 3.11 The ring of endomorphisms of a finitely generated
module over a p.i.d. 197

4 GALOIS THEORY OF EQUATIONS 204

- 4.1 Preliminary results, some old, some new 207
- 4.2 Construction with straight-edge and compass 210
- 4.3 Splitting field of a polynomial 218
- 4.4 Multiple roots 223
- 4.5 The Galois group. The fundamental Galois pairing 227
- 4.6 Some results on finite groups 237

- 4.7 Galois' criterion for solvability by radicals 243
- 4.8 The Galois group as permutation group of the roots 249
- 4.9 The general equation of the n th degree 255
- 4.10 Equations with rational coefficients and symmetric group as Galois group 260
- 4.11 Constructible regular n -gons 263
- 4.12 Transcendence of e and π . The Lindemann-Weierstrass theorem 268
- 4.13 Finite fields 277
- 4.14 Special bases for finite dimensional extension fields 278
- 4.15 Traces and norms 284

5 REAL POLYNOMIAL EQUATIONS AND INEQUALITIES 290

- 5.1 Ordered fields. Real closed fields 291
- 5.2 Sturm's theorem 295.
- 5.3 Formalized Euclidean algorithm and Sturm's theorem 300
- 5.4 Elimination procedures. Resultants 305
- 5.5 Decision method for an algebraic curve 311
- 5.6 Generalized Sturm's theorem. Tarski's principle 318

6 METRIC VECTOR SPACES AND THE CLASSICAL GROUPS 325

- 6.1 Linear functions and bilinear forms 326
- 6.2 Alternate forms 332
- 6.3 Quadratic forms and symmetric bilinear forms 336
- 6.4 Basic concepts of orthogonal geometry 343
- 6.5 Witt's cancellation theorem 348
- 6.6 The theorem of Cartan-Dieudonné 352
- 6.7 Structure of the linear group $L_n(F)$ 356
- 6.8 Structure of orthogonal groups 363
- 6.9 Symplectic geometry. The symplectic group 372
- 6.10 Orders of orthogonal and symplectic groups over a finite field 378
- 6.11 Postscript on hermitian forms and unitary geometry 381

7 ALGEBRAS OVER A FIELD 385

- 7.1 Definition and examples of associative algebras 387
- 7.2 Exterior algebras. Application to determinants 391
- 7.3 Regular matrix representations of associative algebras. Norms and traces 401
- 7.4 Change of base field. Transitivity of trace and norm 405
- 7.5 Non-associative algebras. Lie and Jordan algebras 409

- 7.6 Hurwitz' problem. Composition algebras 417
- 7.7 Frobenius' and Wedderburn's theorems on associative division algebras 429

8 LATTICES AND BOOLEAN ALGEBRAS 433

- 8.1 Partially ordered sets and lattices 434
- 8.2 Distributivity and modularity 439
- 8.3 The theorem of Jordan-Hölder-Dedekind 444
- 8.4 The lattice of subspaces of a vector space.
Fundamental theorem of projective geometry 446
- 8.5 Boolean algebras 452
- 8.6 The Möbius function of a partially ordered set 457

Introduction

In the Introduction to *Basic Algebra I* (abbreviated throughout as “BAI”) we gave an account of the set theoretic concepts that were needed for that volume. These included the power set $\mathcal{P}(S)$ of a set S , the Cartesian product $S_1 \times S_2$ of two sets S_1 and S_2 , maps (= functions), and equivalence relations. In the first volume we generally gave preference to constructive arguments and avoided transfinite methods altogether.

The results that are presented in this volume require more powerful tools, particularly for the proofs of certain existence theorems. Many of these proofs will be based on a result, called Zorn’s lemma, whose usefulness for proving such existence theorems was first noted by Max Zorn. We shall require also some results on the arithmetic of cardinal numbers. All of this fits into the framework of the Zermelo–Fraenkel axiomatization of set theory, including the axiom of choice (the so-called ZFC set theory). Two excellent texts that can be used to fill in the details omitted in our discussion are P. R. Halmos’ *Naive Set Theory* and the more substantial *Set Theory and the Continuum Hypothesis* by P. J. Cohen.

Classical mathematics deals almost exclusively with structures based on sets. On the other hand, category theory—which will be introduced in Chapter 1—

deals with collections of sets, such as all groups, that need to be treated differently from sets. Such collections are called classes. A brief indication of a suitable foundation for category theory is given in the last section of this Introduction.

0.1 ZORN'S LEMMA

We shall now formulate a maximum principle of set theory called Zorn's lemma. We state this first for subsets of a given set. We recall that a set C of subsets of a set S (that is, a subset of the power set $\mathcal{P}(S)$) is called a *chain* if C is totally ordered by inclusion, that is, for any $A, B \in C$ either $A \subset B$ or $B \subset A$. A set T of subsets of S is called *inductive* if the union $\bigcup A_\alpha$ of any chain $C = \{A_\alpha\} \subset T$ is a member of T . We can now state

ZORN'S LEMMA (First formulation). *Let T be a non-vacuous set of subsets of a set S . Assume T is inductive. Then T contains a maximal element, that is, there exists an $M \in T$ such that no $A \in T$ properly contains M .*

There is another formulation of Zorn's lemma in terms of partially ordered sets (BAI, p. 434). Let P, \geq be a partially ordered set. We call P, \geq (totally or linearly) ordered if for every $a, b \in P$ either $a \geq b$ or $b \geq a$. We call P inductive if every non-vacuous subset C of P that is (totally) ordered by \geq as defined in P has a least upper bound in P , that is, there exists a $u \in P$ such that $u \geq a$ for every $a \in C$ and if $v \geq a$ for every $a \in C$ then $v \geq u$. Then we have

ZORN'S LEMMA (Second formulation). *Let P, \geq be a partially ordered set that is inductive. Then P contains maximal elements, that is, there exists $m \in P$ such that no $a \in P$ satisfies $m < a$.*

It is easily seen that the two formulations of Zorn's lemma are equivalent, so there is no harm in referring to either as "Zorn's lemma." It can be shown that Zorn's lemma is equivalent to the

AXIOM OF CHOICE. *Let S be a set, $\mathcal{P}(S)^*$ the set of non-vacuous subsets of S . Then there exists a map f (a "choice function") of $\mathcal{P}(S)^*$ into S such that $f(A) \in A$ for every $A \in \mathcal{P}(S)^*$.*

This is equivalent also to the following: If $\{A_\alpha\}$ is a set of non-vacuous sets A_α , then the Cartesian product $\prod A_\alpha \neq \emptyset$.

The statement that the axiom of choice implies Zorn's lemma can be proved