

# Basic Algebra I

Second Edition

NATHAN JACOBSON

YALE UNIVERSITY



W. H. FREEMAN AND COMPANY  
New York

# Contents

Preface xi

Preface to the First Edition xiii

## INTRODUCTION: CONCEPTS FROM SET THEORY. THE INTEGERS 1

- 0.1 The power set of a set 3
- 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  $\mathbb{Z}$  22
- 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 36

- 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 54
- 1.9 Homomorphisms 58
- 1.10 Subgroups of a homomorphic image.  
Two basic isomorphism theorems 64
- 1.11 Free objects. Generators and relations 67
- 1.12 Groups acting on sets 71
- 1.13 Sylow's theorems 79

## 2 RINGS 85

- 2.1 Definition and elementary properties 86
- 2.2 Types of rings 90
- 2.3 Matrix rings 92
- 2.4 Quaternions 98
- 2.5 Ideals, quotient rings 101
- 2.6 Ideals and quotient rings for  $\mathbb{Z}$  103
- 2.7 Homomorphisms of rings. Basic theorems 106
- 2.8 Anti-isomorphisms 111
- 2.9 Field of fractions of a commutative domain 115
- 2.10 Polynomial rings 119
- 2.11 Some properties of polynomial rings and applications 127
- 2.12 Polynomial functions 134
- 2.13 Symmetric polynomials 138
- 2.14 Factorial monoids and rings 140
- 2.15 Principal ideal domains and Euclidean domains 147
- 2.16 Polynomial extensions of factorial domains 151
- 2.17 "Rngs" (rings without unit) 155

## 3 MODULES OVER A PRINCIPAL IDEAL DOMAIN 157

- 3.1 Ring of endomorphisms of an abelian group 158
- 3.2 Left and right modules 163
- 3.3 Fundamental concepts and results 166
- 3.4 Free modules and matrices 170
- 3.5 Direct sums of modules 175
- 3.6 Finitely generated modules over a p.i.d. Preliminary results 179
- 3.7 Equivalence of matrices with entries in a p.i.d. 181
- 3.8 Structure theorem for finitely generated modules over a p.i.d. 187
- 3.9 Torsion modules, primary components, invariance theorem 189
- 3.10 Applications to abelian groups and to linear transformations 194
- 3.11 The ring of endomorphisms of a finitely generated module  
over a p.i.d. 204

## 4 GALOIS THEORY OF EQUATIONS 210

- 4.1 Preliminary results, some old, some new 213
- 4.2 Construction with straight-edge and compass 216
- 4.3 Splitting field of a polynomial 224
- 4.4 Multiple roots 229
- 4.5 The Galois group. The fundamental Galois pairing 234
- 4.6 Some results on finite groups 244
- 4.7 Galois' criterion for solvability by radicals 251
- 4.8 The Galois group as permutation group of the roots 256
- 4.9 The general equation of the  $n$ th degree 262
- 4.10 Equations with rational coefficients and symmetric group as Galois group 267
- 4.11 Constructible regular  $n$ -gons. Cyclotomic fields over  $\mathbb{Q}$  271
- 4.12 Transcendence of  $e$  and  $\pi$ . The Lindemann-Weierstrass theorem 277
- 4.13 Finite fields 287
- 4.14 Special bases for finite dimensional extensions fields 290
- 4.15 Traces and norms 296
- 4.16 Mod  $p$  reduction 301

## 5 REAL POLYNOMIAL EQUATIONS AND INEQUALITIES 306

- 5.1 Ordered fields. Real closed fields 307
- 5.2 Sturm's theorem 311
- 5.3 Formalized Euclidean algorithm and Sturm's theorem 316
- 5.4 Elimination procedures. Resultants 322
- 5.5 Decision method for an algebraic curve 327
- 5.6 Tarski's theorem 335

## 6 METRIC VECTOR SPACES AND THE CLASSICAL GROUPS 342

- 6.1 Linear functions and bilinear forms 343
- 6.2 Alternate forms 349
- 6.3 Quadratic forms and symmetric bilinear forms 354
- 6.4 Basic concepts of orthogonal geometry 361
- 6.5 Witt's cancellation theorem 367
- 6.6 The theorem of Cartan-Dieudonné 371
- 6.7 Structure of the general linear group  $GL_n(F)$  375
- 6.8 Structure of orthogonal groups 382
- 6.9 Symplectic geometry. The symplectic group 391
- 6.10 Orders of orthogonal and symplectic groups over a finite field 398
- 6.11 Postscript on hermitian forms and unitary geometry 401

## 7 ALGEBRAS OVER A FIELD 405

- 7.1 Definition and examples of associative algebras 406
- 7.2 Exterior algebras. Application to determinants 411

- 7.3 Regular matrix representations of associative algebras.  
Norms and traces 422
- 7.4 Change of base field. Transitivity of trace and norm 426
- 7.5 Non-associative algebras. Lie and Jordan algebras 430
- 7.6 Hurwitz' problem. Composition algebras 438
- 7.7 Frobenius' and Wedderburn's theorems on associative  
division algebras 451

## 8 LATTICES AND BOOLEAN ALGEBRAS 455

- 8.1 Partially ordered sets and lattices 456
- 8.2 Distributivity and modularity 461
- 8.3 The theorem of Jordan-Hölder-Dedekind 466
- 8.4 The lattice of subspaces of a vector space.  
Fundamental theorem of projective geometry 468
- 8.5 Boolean algebras 474
- 8.6 The Möbius function of a partially ordered set 480

## Appendix 489

## Index 493