8640

JACOBSON

Basic Algebra I

Basic Algebra I

NATHAN JACOBSON
YALE UNIVERSITY

W. H. FREEMAN AND COMPANY
San Francisco

Contents

Preface xi

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 ℤ of integers 19
0.6 Some basic arithmetic facts about 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 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

Index 467