

Contents

Preface — VII

| | |
|----------|--|
| 1 | Sets, relations and functions — 1 |
| 1.1 | Sets and subsets — 1 |
| 1.2 | Relations, equivalence relations, partial orders — 4 |
| 1.3 | Functions — 9 |
| 1.4 | Cardinality — 13 |
| 2 | The integers — 17 |
| 2.1 | Well-ordering and mathematical induction — 17 |
| 2.2 | Division in the integers — 19 |
| 2.3 | Congruences — 24 |
| 3 | Introduction to groups — 31 |
| 3.1 | Permutations — 31 |
| 3.2 | Semigroups, monoids and groups — 40 |
| 3.3 | Groups and subgroups — 45 |
| 4 | Quotient groups and homomorphisms — 53 |
| 4.1 | Cosets and Lagrange's Theorem — 53 |
| 4.2 | Normal subgroups and quotient groups — 61 |
| 4.3 | Homomorphisms — 68 |
| 5 | Groups acting on sets — 79 |
| 5.1 | Group actions — 79 |
| 5.2 | Orbits and stabilizers — 82 |
| 5.3 | Applications to the structure of groups — 86 |
| 5.4 | Applications to combinatorics — 93 |
| 6 | Introduction to rings — 100 |
| 6.1 | Elementary properties of rings — 100 |
| 6.2 | Subrings and ideals — 104 |
| 6.3 | Integral domains, division rings and fields — 110 |
| 6.4 | Finiteness conditions on ideals — 117 |
| 7 | Division in commutative rings — 120 |
| 7.1 | Euclidean domains — 120 |
| 7.2 | Principal ideal domains — 123 |
| 7.3 | Unique factorization in integral domains — 126 |
| 7.4 | Roots of polynomials and splitting fields — 132 |

| | |
|-----------|--|
| 8 | Vector spaces — 139 |
| 8.1 | Vector spaces and subspaces — 139 |
| 8.2 | Linear independence, basis and dimension — 143 |
| 8.3 | Linear mappings — 152 |
| 8.4 | Eigenvalues and eigenvectors — 160 |
| 9 | Introduction to modules — 173 |
| 9.1 | Elements of module theory — 173 |
| 9.2 | Modules over principal ideal domains — 185 |
| 9.3 | Applications to linear operators — 197 |
| 10 | The Structure of groups — 206 |
| 10.1 | The Jordan–Hölder Theorem — 206 |
| 10.2 | Solvable and nilpotent groups — 214 |
| 10.3 | Theorems on finite solvable groups — 222 |
| 11 | The Theory of fields — 227 |
| 11.1 | Field extensions — 227 |
| 11.2 | Constructions with ruler and compass — 232 |
| 11.3 | Finite fields — 237 |
| 11.4 | Latin squares and Steiner triple systems — 241 |
| 12 | Galois Theory — 250 |
| 12.1 | Normal and separable extensions — 250 |
| 12.2 | Automorphisms of field extensions — 255 |
| 12.3 | The Fundamental Theorem of Galois theory — 263 |
| 12.4 | Solvability of equations by radicals — 269 |
| 13 | Tensor products — 276 |
| 13.1 | Definition of the tensor product — 276 |
| 13.2 | Properties of tensor products. — 281 |
| 13.3 | Extending the ring of operators. — 288 |
| 14 | Further topics — 293 |
| 14.1 | Zorn’s Lemma with applications — 293 |
| 14.2 | Roots of polynomials and discriminants — 299 |
| 14.3 | Presentations of groups — 302 |
| 14.4 | Introduction to error correcting codes — 313 |

Bibliography — 326

List of symbols — 327

Index — 329