

Contents

1	Sets, relations and functions	1
1.1	Sets and subsets	1
1.2	Relations, equivalence relations and 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 of a set	31
3.2	Binary operations: semigroups, monoids and groups	39
3.3	Groups and subgroups	44
4	Cosets, quotient groups and homomorphisms	52
4.1	Cosets and Lagrange's Theorem	52
4.2	Normal subgroups and quotient groups	60
4.3	Homomorphisms of groups	67
5	Groups acting on sets	78
5.1	Group actions and permutation representations	78
5.2	Orbits and stabilizers	81
5.3	Applications to the structure of groups	85
5.4	Applications to combinatorics – counting labellings and graphs	92
6	Introduction to rings	99
6.1	Definition and elementary properties of rings	99
6.2	Subrings and ideals	103
6.3	Integral domains, division rings and fields	107
7	Division in rings	115
7.1	Euclidean domains	115
7.2	Principal ideal domains	118
7.3	Unique factorization in integral domains	121
7.4	Roots of polynomials and splitting fields	127

8	Vector spaces	134
8.1	Vector spaces and subspaces	134
8.2	Linear independence, basis and dimension	138
8.3	Linear mappings	147
8.4	Orthogonality in vector spaces	155
9	The structure of groups	163
9.1	The Jordan–Hölder Theorem	163
9.2	Solvable and nilpotent groups	171
9.3	Theorems on finite solvable groups	178
10	Introduction to the theory of fields	185
10.1	Field extensions	185
10.2	Constructions with ruler and compass	190
10.3	Finite fields	195
10.4	Applications to latin squares and Steiner triple systems	199
11	Galois theory	208
11.1	Normal and separable extensions	208
11.2	Automorphisms of field extensions	213
11.3	The Fundamental Theorem of Galois Theory	221
11.4	Solvability of equations by radicals	228
12	Further topics	235
12.1	Zorn’s Lemma and its applications	235
12.2	More on roots of polynomials	240
12.3	Generators and relations for groups	243
12.4	An introduction to error correcting codes	254
	Bibliography	267
	Index of notation	269
	Index	273