

Contents

Preface	8
1 Number-theoretic preliminaries	12
1.1 Basic facts about the divisibility	12
1.2 The greatest common divisor	13
1.3 The least common multiple	17
1.4 The prime numbers	19
1.5 The relation of congruence modulo m	23
1.6 Euler's phi function	32
1.7 The number-of-positive-divisor function	39
2 The notion of a group	41
2.1 A binary operation on a set	41
2.2 The definition of a group and general remarks	45
2.3 Examples of groups	47
2.3.1 Groups related to geometry	54
2.3.2 Groups related to modular arithmetic	56
2.4 Arithmetic in groups	59
3 A subgroup of a group	64
3.1 The definition and basic properties	64
3.2 Cosets of a subgroup in a group	69
3.3 A normal subgroup and the quotient group of a group	72
3.4 The product of subgroups in a group	77
3.5 Subgroups generated by sets	79

4	Cyclic groups	84
4.1	The order of a group element	84
4.2	Properties of cyclic groups	89
4.2.1	The cyclic and non-cyclic subgroups of some particular groups	95
5	Homomorphisms of groups	101
5.1	Definitions and general properties	101
5.2	Isomorphism theorems for groups	114
5.3	Homomorphic images of cyclic groups	120
5.4	The classification of groups of order four	128
5.5	Direct product of groups	131
5.6	Cayley's theorem	134
6	Groups of permutations	137
6.1	General remarks and basic notions	137
6.2	Disjoint permutations	142
6.3	Cycles	145
6.4	The factorization of non-trivial permutations into the product of disjoint cycles	149
6.5	Possible orders of elements in S_n	153
7	The notion of a ring	155
7.1	Definitions and general remarks	155
7.2	Arithmetic in rings	157
7.3	Basic examples of rings	162
7.4	Direct product of rings	166
7.5	Zero divisors and regular elements of a ring	167
8	Subrings and ideals of rings	171
8.1	Subrings	171
8.2	Ideals	180
8.3	Quotient rings	184
8.3.1	Prime and maximal ideals	186
8.4	Principal ideal domains	190

9 Homomorphisms of rings	192
9.1 Definitions and basic properties	192
9.2 Isomorphism theorems for rings	197
9.3 Examples of ring homomorphisms	200
10 Rings of polynomials	207
10.1 Basic definitions and notations	207
10.2 Homomorphism related to polynomial rings and their consequences	212
10.3 Polynomial rings over integral domains	218
10.4 The Fundamental Theorem of Algebra and its proof . .	221
11 Dividing polynomials	231
11.1 General theory	231
11.2 Arithmetic in integral domains	245
12 Polynomials over \mathbb{Z} and \mathbb{Q}	254
12.1 Rational root theorem	254
12.2 Primitive polynomials	257
13 Unique factorization domains	265
13.1 Prime elements of integral domains	265
13.2 The notion of a unique factorization domain	273
14 Fields	277
14.1 Properties of fields	277
14.1.1 General remarks	277
14.1.2 The characteristic of a field	278
14.2 Subfields in a field	281
14.3 The field of fractions of an integral domain	293
14.4 Field extensions	297
14.4.1 A simple extension of a field	313
List of symbols	316
Index	319
Bibliography	324