
Contents

1	Forward	1
2	In the Beginning	5
2.1	Prologue	5
2.2	Integers, rational numbers, real numbers	6
2.2.1	Operations and relations	7
2.2.2	Manipulating equations and inequalities	10
2.2.3	Exponentiation (VERY important)	10
2.3	Test yourself	11
3	Complex Numbers	13
3.1	The origin of complex numbers	13
3.1.1	A number that can't be real (and we can prove it!) . .	13
3.1.2	Unreal, but unavoidable	16
3.1.3	A mathematical revolution	18
3.2	Arithmetic with complex numbers	22
3.2.1	Complex arithmetic	22
3.2.2	Comparison of integer, rational, real and complex addition properties	27
3.2.3	Comparison of integer, rational, real and complex multiplication properties	28

3.2.4	Modulus and complex conjugate	29
3.3	Alternative representations of complex numbers	33
3.3.1	Cartesian representation of complex numbers	33
3.3.2	Vector representation of complex numbers	34
3.3.3	Polar representation of complex numbers	35
3.3.4	Converting between rectangular and polar form	35
3.3.5	Multiplication and powers in complex polar form	39
3.3.6	A Remark on representations of complex numbers	45
3.4	Applications of complex numbers	47
3.4.1	General remarks on the usefulness of complex numbers	47
3.4.2	Complex numbers, sine and cosine waves, and phasors	47
3.4.3	Roots of unity and regular polygons	53
3.4.4	Arbitrary n th roots	59
3.5	Complex roots of polynomial equations	61
4	Modular Arithmetic	64
4.1	Introductory examples	64
4.2	Modular equivalence and modular arithmetic	66
4.3	Modular equations	74
4.3.1	More uses of modular arithmetic	74
4.3.2	Solving modular equations	77
4.4	The integers mod n (also known as $\mathbb{Z}_n$)	84
4.4.1	Arithmetic with remainders	84
4.4.2	Cayley tables for $\mathbb{Z}_n$	87
4.4.3	Closure properties of $\mathbb{Z}_n$	89
4.4.4	Identities and inverses in $\mathbb{Z}_n$	91
4.4.5	Inverses in $\mathbb{Z}_n$	92
4.4.6	Other arithmetic properties of $\oplus$ and $\odot$	94
4.4.7	Definition of a group	95
4.5	Modular division	96

4.5.1	A sticky problem	96
4.5.2	Greatest common divisors	101
4.5.3	Computer stuff	105
4.5.4	Diophantine equations	106
4.5.5	Multiplicative inverse for modular arithmetic	114
4.5.6	Chinese remainder theorem	116
5	Introduction to Cryptography	120
5.1	Private key cryptography	121
5.1.1	Shift codes	121
5.1.2	Affine codes	124
5.1.3	Monoalphabetic codes	128
5.1.4	Polyalphabetic codes	128
5.1.5	Spreadsheet exercises	132
5.2	Public key cryptography	137
5.2.1	The RSA cryptosystem	137
5.2.2	Message verification	140
5.2.3	RSA exercises	140
5.2.4	Additional exercises: identifying prime numbers	143
5.3	References and suggested readings	150
6	Set Theory	152
6.1	Set Basics	152
6.1.1	What's a set? (mathematically speaking, that is)	152
6.1.2	How to specify sets	152
6.1.3	Important sets of numbers	155
6.1.4	Operations on sets	157
6.2	Properties of set operations	164
6.3	Do the subsets of a set form a group?	169

7	Functions: basic concepts	173
7.1	The Cartesian product: a different type of set operation . . .	173
7.2	Introduction to functions	176
7.2.1	Informal look at functions	176
7.2.2	Official definition of functions	183
7.2.3	Summary of basic function concepts	187
7.3	One-to-one functions	187
7.3.1	Concept and definition	187
7.3.2	Proving that a function is one-to-one	190
7.4	Onto functions	195
7.4.1	Concept and definition	195
7.4.2	Proving that a function is onto	197
7.5	Bijections	201
7.5.1	Concept and definition	201
7.5.2	Proving that a function is a bijection	203
7.6	Composition of functions	206
7.6.1	Concept and definition	206
7.6.2	Proofs involving function composition	210
7.7	Inverse functions	213
7.7.1	Concept and definition	213
7.7.2	Which functions have inverses?	215
8	Equivalence Relations and Equivalence Classes	218
8.1	Binary relations	218
8.2	Definition and basic properties of equivalence relations	228
8.3	Equivalence classes	232
8.4	Modular arithmetic redux	235
8.4.1	The integers modulo 3	236
8.4.2	The integers modulo n	238
8.4.3	Something we have swept under the rug	239
8.5	Partitions	242

9	Symmetries of Plane Figures	247
9.1	Definition and examples	247
9.2	Composition of symmetries	253
9.3	Do the symmetries of an object form a group?	256
9.4	The dihedral groups	262
9.5	For further investigation	271
9.6	An unexplained miracle	272
10	Permutations	275
10.1	Introduction to permutations	276
10.2	Permutation groups and other generalizations	277
10.2.1	The symmetric group of n letters	278
10.2.2	Isomorphic groups	280
10.2.3	Subgroups and permutation groups	281
10.3	Cycle notation	283
10.3.1	Tableaus and cycles	283
10.3.2	Composition (a.k.a. product) of cycles	287
10.3.3	Product of disjoint cycles	290
10.3.4	Products of permutations using cycle notation	294
10.3.5	Cycle structure of permutations	296
10.4	Algebraic properties of cycles	299
10.4.1	Powers of cycles: definition of order	299
10.4.2	Powers and orders of permutations in general	303
10.4.3	Transpositions and inverses	307
10.5	“Switchyard” and generators of the permutation group	310
10.6	Other groups of permutations 	316
10.6.1	Even and odd permutations	316
10.6.2	The alternating group	320
10.7	Additional exercises	323

11 Abstract Groups: Definitions and Basic Properties	325
11.1 Formal definition of a group	326
11.2 Examples	328
11.2.1 The group of units of $\mathbb{Z}_n$	334
11.2.2 Groups of matrices	336
11.3 Basic properties of groups	337
11.4 Subgroups	347
11.5 Cyclic groups	352
11.5.1 Cyclic groups	352
11.5.2 Cyclic subgroups	355
11.5.3 Subgroups of cyclic groups	359
11.6 Additional group and subgroup exercises	360
12 Cosets and Factor Groups	364
12.1 Definition of cosets	365
12.2 Cosets and partitions of groups	369
12.3 Lagrange's theorem, and some consequences	373
12.3.1 Lagrange's theorem	373
12.3.2 Orders of elements, Euler's theorem, Fermat's little theorem, and prime order	375
12.4 Factor groups and normal subgroups	378
12.4.1 Normal subgroups	378
12.4.2 Factor groups	380
12.5 The simplicity of the alternating group	384
13 Group Actions	392
13.1 Basic definitions	392
13.2 Group actions on regular polyhedra	394
13.2.1 G-equivalence and orbits	394
13.2.2 Stabilizers, stabilizer subgroups, and fixed point sets	397

13.2.3	Counting formula for the order of polyhedral rotational symmetry groups	399
13.2.4	Representing G in terms of stabilizer subgroups	401
13.3	Examples of other regular polyhedral rotation groups	403
13.3.1	The tetrahedron	403
13.3.2	The octahedron	406
13.3.3	The dodecahedron	409
13.3.4	Soccer ball	412
13.4	Euler's formula for regular polyhedra	413
13.5	Closing comments on polyhedral symmetry groups	415
13.6	Group actions on subgroups and cosets	415
13.7	Conjugation	421
14	Algebraic Coding	432
14.1	Error-Detecting and Correcting Codes	432
14.1.1	Maximum-Likelihood Decoding	435
14.1.2	Block Codes	438
14.2	Group codes and linear codes	444
14.3	Linear Block Codes	446
14.4	Code words and encoding in block linear codes	450
14.4.1	Canonical Parity-check matrices	450
14.4.2	Standard Generator Matrices	452
14.4.3	Error detection and correction	456
14.5	Efficient Decoding	459
14.5.1	Decoding using syndromes	459
14.5.2	Coset Decoding	461
14.6	Additional algebraic coding exercises	464
14.7	References and Suggested Readings	466

15 Isomorphisms of Groups	468
15.1 Preliminary examples	468
15.2 Formal definition and basic properties of isomorphisms	472
15.3 More Examples	474
15.4 More properties of isomorphisms	482
15.5 Classification up to isomorphism	484
15.5.1 Classifying cyclic groups	484
15.5.2 Characterizing all finite groups: Cayley's theorem . . .	486
15.6 Direct Products	489
15.6.1 External Direct Products	489
15.6.2 Classifying abelian groups by factorization	492
15.6.3 Internal Direct Products	495
16 Homomorphisms of Groups	500
16.1 Preliminary examples	500
16.2 Definition and several more examples	506
16.3 Proofs of homomorphism properties	511
16.4 The First Isomorphism Theorem	514
17 Sigma Notation	517
17.1 Lots of examples	517
17.2 Sigma notation properties	519
17.3 Nested Sigmas	522
17.4 Common Sums	524
17.5 Sigma notation in linear algebra	527
17.5.1 Applications to matrices	527
17.5.2 Levi-Civita symbols	533
17.6 Summation by parts	545

18 Polynomials	548
18.1 Polynomials of various stripes	548
18.2 Polynomial rings	551
18.3 The Division Algorithm for Polynomials	561
18.4 Polynomial roots	564
18.5 Proof that $U(p)$ is cyclic	566
19 Polynomials and Matrices	568
19.1 Definition of vector space	568
19.2 Polynomials are vectors	570
19.3 Ring isomorphism between polynomials and banded lower-triangular matrices	571
20 Appendix: Induction proofs—patterns and examples	583
20.1 Basic examples of induction proofs	583
20.2 Advice on writing up induction proofs	584
20.3 Induction proof patterns & practice problems	585
20.4 Strong Induction, with applications	590
20.5 More advice on induction and strong induction proofs	592
20.6 Common mistakes	593
20.7 Strong induction practice problems	594
20.8 Non-formula induction proofs.	596
20.9 Practice problems for non-formula induction	597
20.10 Fallacies and pitfalls	597
21 Hints	601
21.1 Hints for “Complex Numbers” exercises	601
21.2 Hints for “Modular Arithmetic” exercises	602
21.3 Hints for “Introduction to Cryptography” exercises	603
21.4 Hints for “Set Theory” exercises	604
21.5 Hints for “Functions: basic concepts” exercises	604

21.6 Hints for “Equivalence Relations and Equivalence Classes” exercises	604
21.7 Hints for “Symmetries of Plane Figures” exercises	605
21.8 Hints for “Permutations” exercises	605
21.9 Hints for “Abstract Groups: Definitions and Basic Proper- ties” exercises	606
21.10 Hints for “Cosets” exercises	607
21.11 Hints for “Group Actions” exercises	607
21.12 Hints for “Algebraic Coding” exercises	608
21.13 Hints for “Isomorphisms” exercises	608
21.14 Hints for “Homomorphism” exercises	609
21.15 Hints for “Sigma Notation” exercises	609
21.16 Hints for “Polynomial Rings” exercises	610
21.17 Hints for “Polynomials and Matrices” exercises	610
GNU Free Documentation License	611
Index	620