

Contents

1	The integers	1
1.1	Unique factorization	1
1.2	Irrationalities	5
1.3	\mathbb{Z}/m , the integers mod m	6
1.4	Fermat's Little Theorem	8
1.5	Sun-Ze's theorem	11
1.6	Worked examples	12
2	Groups I	17
2.1	Groups	17
2.2	Subgroups, Lagrange's theorem	19
2.3	Homomorphisms, kernels, normal subgroups	22
2.4	Cyclic groups	24
2.5	Quotient groups	26
2.6	Groups acting on sets	28
2.7	The Sylow theorem	31
2.8	Trying to classify finite groups, part I	34
2.9	Worked examples	42
3	The players: rings, fields, etc.	47
3.1	Rings, fields	47
3.2	Ring homomorphisms	50
3.3	Vectorspaces, modules, algebras	52
3.4	Polynomial rings I	54
4	Commutative rings I	61
4.1	Divisibility and ideals	61
4.2	Polynomials in one variable over a field	62
4.3	Ideals and quotients	65
4.4	Ideals and quotient rings	68
4.5	Maximal ideals and fields	69
4.6	Prime ideals and integral domains	69
4.7	Fermat-Euler on sums of two squares	71
4.8	Worked examples	73
5	Linear Algebra I: Dimension	79
5.1	Some simple results	79
5.2	Bases and dimension	80
5.3	Homomorphisms and dimension	82

6	Fields I	85
6.1	Adjoining things	85
6.2	Fields of fractions, fields of rational functions	88
6.3	Characteristics, finite fields	90
6.4	Algebraic field extensions	92
6.5	Algebraic closures	96
7	Some Irreducible Polynomials	99
7.1	Irreducibles over a finite field	99
7.2	Worked examples	102
8	Cyclotomic polynomials	105
8.1	Multiple factors in polynomials	105
8.2	Cyclotomic polynomials	107
8.3	Examples	110
8.4	Finite subgroups of fields	113
8.5	Infinitude of primes $p = 1 \pmod n$	113
8.6	Worked examples	114
9	Finite fields	119
9.1	Uniqueness	119
9.2	Frobenius automorphisms	120
9.3	Counting irreducibles	123
10	Modules over PIDs	125
10.1	The structure theorem	125
10.2	Variations	126
10.3	Finitely-generated abelian groups	128
10.4	Jordan canonical form	130
10.5	Conjugacy versus $k[x]$ -module isomorphism	134
10.6	Worked examples	141
11	Finitely-generated modules	151
11.1	Free modules	151
11.2	Finitely-generated modules over a domain	155
11.3	PIDs are UFDs	158
11.4	Structure theorem, again	159
11.5	Recovering the earlier structure theorem	161
11.6	Submodules of free modules	161
12	Polynomials over UFDs	165
12.1	Gauss' lemma	165
12.2	Fields of fractions	167
12.3	Worked examples	169
13	Symmetric groups	175
13.1	Cycles, disjoint cycle decompositions	175
13.2	Transpositions	176
13.3	Worked examples	176

14 Naive Set Theory	181
14.1 Sets	181
14.2 Posets, ordinals	183
14.3 Transfinite induction	187
14.4 Finiteness, infiniteness	188
14.5 Comparison of infinities	188
14.6 Example: transfinite Lagrange replacement	190
14.7 Equivalents of the Axiom of Choice	191
15 Symmetric polynomials	193
15.1 The theorem	193
15.2 First examples	194
15.3 A variant: discriminants	196
16 Eisenstein's criterion	199
16.1 Eisenstein's irreducibility criterion	199
16.2 Examples	200
17 Vandermonde determinants	203
17.1 Vandermonde determinants	203
17.2 Worked examples	206
18 Cyclotomic polynomials II	211
18.1 Cyclotomic polynomials over \mathbb{Z}	211
18.2 Worked examples	213
19 Roots of unity	219
19.1 Another proof of cyclicity	219
19.2 Roots of unity	220
19.3 \mathbb{Q} with roots of unity adjoined	220
19.4 Solution in radicals, Lagrange resolvents	227
19.5 Quadratic fields, quadratic reciprocity	230
19.6 Worked examples	234
20 Cyclotomic III	243
20.1 Prime-power cyclotomic polynomials over \mathbb{Q}	243
20.2 Irreducibility of cyclotomic polynomials over \mathbb{Q}	245
20.3 Factoring $\Phi_n(x)$ in $\mathbb{F}_p[x]$ with $p n$	246
20.4 Worked examples	246
21 Primes in arithmetic progressions	261
21.1 Euler's theorem and the zeta function	261
21.2 Dirichlet's theorem	263
21.3 Dual groups of abelian groups	266
21.4 Non-vanishing on $\operatorname{Re}(s) = 1$	268
21.5 Analytic continuations	269
21.6 Dirichlet series with positive coefficients	270

22	Galois theory	273
22.1	Field extensions, imbeddings, automorphisms	274
22.2	Separable field extensions	275
22.3	Primitive elements	277
22.4	Normal field extensions	278
22.5	The main theorem	280
22.6	Conjugates, trace, norm	282
22.7	Basic examples	282
22.8	Worked examples	283
23	Solving equations by radicals	293
23.1	Galois' criterion	293
23.2	Composition series, Jordan-Hölder theorem	295
23.3	Solving cubics by radicals	295
23.4	Worked examples	298
24	Eigenvectors, Spectral Theorems	303
24.1	Eigenvectors, eigenvalues	303
24.2	Diagonalizability, semi-simplicity	306
24.3	Commuting endomorphisms $ST = TS$	308
24.4	Inner product spaces	309
24.5	Projections without coordinates	314
24.6	Unitary operators	314
24.7	Spectral theorems	315
24.8	Corollaries of the spectral theorem	316
24.9	Worked examples	318
25	Duals, naturality, bilinear forms	325
25.1	Dual vectorspaces	325
25.2	First example of naturality	329
25.3	Bilinear forms	330
25.4	Worked examples	333
26	Determinants I	341
26.1	Prehistory	341
26.2	Definitions	343
26.3	Uniqueness and other properties	344
26.4	Existence	348
27	Tensor products	351
27.1	Desiderata	351
27.2	Definitions, uniqueness, existence	352
27.3	First examples	356
27.4	Tensor products $f \otimes g$ of maps	359
27.5	Extension of scalars, functoriality, naturality	360
27.6	Worked examples	363

28 Exterior powers	375
28.1 Desiderata	375
28.2 Definitions, uniqueness, existence	376
28.3 Some elementary facts	379
28.4 Exterior powers $\bigwedge^n f$ of maps	380
28.5 Exterior powers of free modules	381
28.6 Determinants revisited	384
28.7 Minors of matrices	385
28.8 Uniqueness in the structure theorem	386
28.9 Cartan's lemma	387
28.10 Cayley-Hamilton theorem	389
28.11 Worked examples	393