

Contents

Preface	xv
0.1 A brief history of <i>Visual Algebra</i>	xv
0.2 Target audiences	xviii
0.3 A guide to teaching out of this book	xix
0.4 Additional resources and practical considerations	xxiii
0.5 An invitation to readers	xxv
1 Groups, intuitively	1
1.1 Symmetries and Cayley graphs	1
1.1.1 The rectangle symmetry group	1
1.1.2 The equilateral triangle symmetry group	5
1.1.3 Groups beyond geometric symmetry	8
1.2 Groups from puzzles	11
1.2.1 The Rubik's cube group	12
1.2.2 Groups from other puzzles	14
1.2.3 Groupoid puzzles	16
1.3 Group presentations	17
1.3.1 Unlabeled Cayley graphs	17
1.3.2 Labeling Cayley graphs with actions	18
1.3.3 Generators and relations	19
1.3.4 The word problem	22
1.4 Infinite symmetry groups	24
1.4.1 Frieze groups	24
1.4.2 Wallpaper and crystal groups	30
1.4.3 Braid groups	30
1.5 Cayley tables	33
1.5.1 Constructing Cayley tables	33
1.5.2 Recognizing structure in Cayley tables	36
1.6 The formal definition of a group	37
1.6.1 Binary operations	38
1.6.2 The group axioms	38
1.6.3 What can fail with our informal definition?	40
1.7 Exercises	43
2 Examples of groups	53
2.1 Overview and preliminaries	53
2.1.1 Families of groups	54
2.1.2 Roots of unity	56
2.1.3 Cyclotomic polynomials	59
2.1.4 Rotation and reflection matrices	60
2.2 Cyclic groups	61
2.2.1 Cyclic groups, multiplicatively	62
2.2.2 Cyclic groups, additively	63

2.2.3	Infinite cyclic groups	65
2.2.4	Cyclic subgroups and cycle graphs	66
2.3	Dihedral groups	68
2.3.1	Finite dihedral groups	68
2.3.2	The infinite dihedral group	69
2.4	Abelian groups	73
2.4.1	Finite abelian groups	73
2.4.2	Infinite abelian groups	77
2.4.3	Finitely generated abelian groups	79
2.5	Groups of permutations	79
2.5.1	Permutations of a set	80
2.5.2	Permutation matrices	83
2.5.3	Cayley's theorem	85
2.6	Symmetric and alternating groups	87
2.6.1	The symmetric group and permutahedra	87
2.6.2	Cayley graphs on polytopes	89
2.6.3	The alternating group	93
2.7	Quaternion and dicyclic groups	98
2.7.1	Generalizing the quaternion group	98
2.7.2	Dicyclic groups as matrices	100
2.7.3	Cycle graphs of dicyclic groups	101
2.7.4	Quotients of dicyclic groups	102
2.8	Diquaternion groups	102
2.8.1	Dihedralizing the quaternions	103
2.8.2	Generalized diquaternion groups	105
2.9	Semidihedral and semiabelian groups	106
2.9.1	Completing partial Cayley graphs	106
2.9.2	Semidihedral groups	107
2.9.3	Semiabelian groups	109
2.9.4	Comparing cycle graphs	110
2.9.5	Matrix representations and classification	111
2.10	Direct and semidirect products	113
2.10.1	Direct products	114
2.10.2	Automorphisms and rewirings	116
2.10.3	Semidirect products	118
2.10.4	Examples of semidirect products	121
2.10.5	Familiar groups as semidirect products	127
2.10.6	Hidden direct products	129
2.11	Groups of matrices	129
2.11.1	Coefficient rings and fields	130
2.11.2	Linear groups	130
2.11.3	Affine groups	134
2.12	The landscape of finite groups	134
2.12.1	Building blocks and p -groups	134
2.12.2	Small groups and group databases	136
2.13	Exercises	138
3	Group structure	163
3.1	Subgroups	163
3.1.1	A few small examples	164
3.1.2	Basic properties of subgroups	165
3.1.3	Groups of order 8	169
3.2	Cosets	174

3.2.1	Left and right cosets	174
3.2.2	Properties of cosets	177
3.2.3	Cosets in additive groups	180
3.2.4	The center of a group	181
3.3	Normality	182
3.3.1	Normal subgroups and normalizers	183
3.3.2	The degree of normality	184
3.3.3	Normalizers in Cayley graphs	187
3.4	Conjugate subgroups	188
3.4.1	Conjugation and normality	188
3.4.2	The number of conjugate subgroups	190
3.4.3	Conjugate subgroups in subgroup lattices	192
3.4.4	Conjugate subgroups, algebraically	201
3.4.5	Conjugate subgroups in Cayley graphs	202
3.5	Products of subgroups	205
3.5.1	Products and double cosets	205
3.5.2	When is a product a subgroup?	206
3.6	Quotients by subgroups	207
3.6.1	Quotient groups, visually	207
3.6.2	Quotient groups, algebraically	212
3.6.3	Examples and nonexamples of quotients	213
3.7	Conjugate elements	215
3.7.1	Basic properties of conjugacy classes	215
3.7.2	Conjugation in frieze groups	217
3.7.3	Conjugation in dihedral groups	218
3.7.4	Conjugation in symmetric groups	223
3.7.5	Centralizers	225
3.8	Exercises	230
4	Maps between groups	249
4.1	Homomorphisms	249
4.1.1	Embeddings and quotients	249
4.1.2	The formal definition	251
4.1.3	Group representations	257
4.2	Kernels and quotients	258
4.2.1	The kernel of a homomorphism	258
4.2.2	The fundamental homomorphism theorem	262
4.2.3	Applying the FHT	264
4.2.4	The quotient-embedding factorization	268
4.3	Subgroups of quotients	269
4.3.1	The correspondence theorem	269
4.3.2	Reading quotient lattices	272
4.3.3	The shoebox analogy	274
4.3.4	Proof of the correspondence theorem	276
4.4	Quotients of quotients	278
4.4.1	The fraction theorem	278
4.4.2	Proof of the fraction theorem	280
4.5	Subquotients	281
4.5.1	The diamond theorem	281
4.5.2	Proof of the diamond theorem	282
4.5.3	Applications of the diamond theorem	284
4.5.4	The butterfly lemma	286
4.6	Commutators and abelianization	288

4.6.1	The commutator subgroup and its quotient	288
4.6.2	Abelian quotients	289
4.7	Automorphisms	291
4.7.1	Automorphisms of noncyclic groups	292
4.7.2	Inner and outer automorphisms	296
4.7.3	Automorphisms of symmetric groups	300
4.8	External and internal products	301
4.8.1	External products	301
4.8.2	Internal direct products	304
4.8.3	Internal semidirect products	306
4.8.4	The holomorph of a group	310
4.8.5	Central products	310
4.9	Hidden homomorphisms	313
4.9.1	Linear algebra: systems of equations	313
4.9.2	Differential equations: solutions to inhomogeneous linear ODEs	313
4.9.3	Calculus: constants of integration	314
4.9.4	Precalculus: exponentials and logarithms	314
4.9.5	Trigonometry: angle addition formulas	314
4.10	Exercises	315
5	Actions of groups	331
5.1	Group actions and G -sets	331
5.1.1	Actions vs. configurations	331
5.1.2	Group switchboards and action graphs	332
5.1.3	G -sets and the choice of generators	334
5.1.4	Left vs. right actions	337
5.2	Five features of every action	339
5.2.1	Local features: orbits, stabilizers, and fixators	340
5.2.2	Global features: fixed points and kernels	343
5.3	Two theorems on orbits	344
5.3.1	The orbit-stabilizer theorem	344
5.3.2	The orbit-counting theorem	348
5.4	Examples of actions	349
5.4.1	Actions by multiplication	349
5.4.2	Actions by conjugation	350
5.4.3	Actions on subgroups	353
5.4.4	Actions on cosets	357
5.4.5	Subgroups of small index	360
5.4.6	Summary of our four actions	362
5.5	Actions by automorphisms	362
5.5.1	Actions of $\text{Aut}(G)$ on elements and conjugacy classes	362
5.5.2	Actions of $\text{Aut}(G)$ on subgroups	364
5.6	Action equivalence and G -set isomorphisms	365
5.6.1	The idea of action equivalence	365
5.6.2	Equivalence of left and right actions	368
5.6.3	Left and right actions of permutations	370
5.6.4	Isomorphisms of G -sets	372
5.7	Transitive actions	374
5.7.1	Free, transitive, and simply transitive actions	375
5.7.2	Classification of transitive G -sets	376
5.7.3	Conjugate subgroups and isomorphic G -sets	379
5.8	Simply transitive actions	381
5.8.1	Tilings, chambers, and group actions	381

5.8.2	Affine Weyl groups	383
5.8.3	Coxeter graphs and higher-dimensional tilings	386
5.8.4	Hyperbolic tilings and the modular group	388
5.9	Equivariance and G -set homomorphisms	391
5.9.1	Equivariant bijections and G -set isomorphisms	391
5.9.2	Equivariant surjections and G -set quotients	397
5.9.3	The fundamental homomorphism theorem for G -sets	400
5.10	p -groups	402
5.10.1	Actions of p -groups	403
5.10.2	Cauchy's theorem	403
5.10.3	Normalizers in p -groups	405
5.10.4	p -subgroups	406
5.11	Sylow theory	407
5.11.1	Goals of the Sylow theorems	408
5.11.2	The first Sylow theorem	409
5.11.3	The second Sylow theorem	411
5.11.4	The third Sylow theorem	415
5.11.5	Sylow theorems and simple groups	417
5.11.6	The Frattini argument	418
5.12	Exercises	419
6	Extensions of groups	441
6.1	Finite group structure	441
6.1.1	Finite abelian groups	441
6.1.2	Finite simple groups	444
6.1.3	Alternating groups: conjugacy and simplicity	448
6.2	Short exact sequences	452
6.2.1	Chopping off sublattices	452
6.2.2	Exactness	453
6.2.3	Iterative extensions	455
6.2.4	Extension equivalence	457
6.3	Split extensions and products	459
6.3.1	Right-split extensions and semidirect products	459
6.3.2	Left-split extensions and direct products	463
6.3.3	Abelian, central, and stem extensions	464
6.4	Simple extensions and composition series	466
6.4.1	Subnormal series and their factors	466
6.4.2	Ascending vs. descending subnormal series	468
6.4.3	The Jordan-Hölder theorem	470
6.4.4	Chief series	474
6.5	Abelian extensions and solvability	474
6.5.1	Maximal abelian descents	474
6.5.2	Commutator subgroups	476
6.5.3	Solvability of subgroups and quotients	479
6.5.4	Solvability and abelian extensions	481
6.6	Central extensions and nilpotency	483
6.6.1	Solvable vs. nilpotent groups	483
6.6.2	Central ascents and the ascending central series	483
6.6.3	Central descents	487
6.6.4	The descending central series	489
6.6.5	Comparing the two central series	491
6.6.6	Central series and central extensions	495
6.6.7	Alternate characterizations of nilpotent groups	499

6.7	Exercises	503
7	Universal constructions	517
7.1	Commutative diagrams	517
7.1.1	Factoring maps	517
7.1.2	Cancellation laws	521
7.1.3	Factoring non-homomorphisms	525
7.2	Universal and co-universal properties	526
7.2.1	The co-universal property of quotient groups	526
7.2.2	Other co-universal properties	529
7.2.3	Universal properties	531
7.3	Products and coproducts	533
7.3.1	Products and direct sums of vector spaces	533
7.3.2	Products and coproducts of groups	536
7.4	Basic category theory	538
7.4.1	Objects and morphisms	538
7.4.2	Functors	541
7.4.3	Initial, terminal, and zero objects	547
7.5	Free groups and free objects	551
7.5.1	Cayley graphs of free groups	551
7.5.2	Free semigroups	554
7.5.3	Constructing free groups from free semigroups	556
7.5.4	Free objects in categories	561
7.5.5	Free abelian groups	561
7.5.6	Free nilpotent groups	564
7.6	Formalizing group presentations	566
7.6.1	Relations and quotients	566
7.6.2	The co-universal property of presentations	568
7.6.3	Recognizing groups from presentations	571
7.7	Free products	573
7.7.1	Coproducts in Ab	573
7.7.2	Coproducts in Grp	574
7.8	Amalgamation	577
7.8.1	Amalgamated free products, pushouts, and pullbacks	578
7.8.2	The Seifert–van Kampen theorem	581
7.9	Exercises	584
8	Rings	597
8.1	Rings and their substructures	597
8.1.1	Subgroups, subrings, and ideals	598
8.1.2	Ideals generated by sets	601
8.1.3	Ideals and units	605
8.1.4	Sums and intersections of substructures	607
8.2	Examples of rings	608
8.2.1	Finite rings	608
8.2.2	Infinite rings	615
8.2.3	Fields, domains, and unity	617
8.3	Maps between rings	620
8.3.1	Quotient rings	620
8.3.2	Ring homomorphisms	621
8.3.3	The ring isomorphism theorems	622
8.3.4	The fundamental homomorphism theorem	623
8.3.5	The correspondence theorem	624

8.3.6	The fraction theorem	628
8.3.7	The diamond theorem	629
8.3.8	The quotient-embedding factorization	631
8.4	Maximal ideals and fields	633
8.4.1	Maximal structures: normal subgroups vs. ideals	633
8.4.2	Ordinals, transfinite recursion, and Zorn's lemma	635
8.4.3	Fields as quotients	638
8.5	Finite fields	639
8.5.1	Constructing finite fields	640
8.5.2	Subfields of finite fields	642
8.5.3	Properties of finite fields	644
8.6	Prime and primary ideals	646
8.6.1	Prime numbers and prime ideals	646
8.6.2	Primary ideals	649
8.7	Radicals of rings	649
8.7.1	Nilpotent elements and subdirect products	650
8.7.2	The Jacobson radical of a ring	651
8.7.3	The nilradical of a ring	653
8.8	Radicals of ideals	656
8.8.1	The nilradical of an ideal	656
8.8.2	The Jacobson radical of an ideal	659
8.9	Rings of fractions	659
8.9.1	The field of fractions of an integral domain	661
8.9.2	Rings of fractions and localization	663
8.9.3	Localization with zero divisors	665
8.10	Exercises	665
9	Domains	681
9.1	Divisibility	681
9.1.1	Divisibility via ideals	681
9.1.2	Primes and irreducibles	684
9.1.3	GCD and LCM	687
9.2	Factorization	691
9.2.1	Atomic domains	691
9.2.2	Noetherian rings	692
9.2.3	Unique factorization domains	693
9.3	Sunzi's remainder theorem	695
9.3.1	Four versions of the Sunzi remainder theorem	695
9.3.2	Idempotents	699
9.3.3	A group-theoretic analogue of the Sunzi remainder theorem	700
9.4	Quadratic number fields and integer rings	701
9.4.1	Algebraic integers	701
9.4.2	Quadratic fields and their rings of integers	702
9.4.3	The field norms	703
9.5	The Gaussian integers	705
9.5.1	Gaussian primes	705
9.5.2	Quotients of the Gaussian integers	709
9.6	The Eisenstein integers	714
9.6.1	Eisenstein primes	715
9.6.2	Quotients of Eisenstein integers	718
9.7	The ring $\mathbb{Z}[\sqrt{-5}]$	720
9.7.1	Primes in $\mathbb{Z}[\sqrt{-5}]$	721
9.7.2	Non-prime irreducibles	722

9.7.3	Ideal factorization	724
9.7.4	Quotients in $\mathbb{Z}[\sqrt{-5}]$	728
9.8	The division algorithm and Euclidean domains	730
9.8.1	The division and Euclidean algorithms in the integers	730
9.8.2	Euclidean domains	733
9.9	Norm-Euclidean domains	735
9.9.1	The division algorithm, visually	735
9.9.2	Failure of the division algorithm, visually	737
9.9.3	Norm-Euclidean quadratic integer rings	738
9.10	Dedekind-Hasse norms	743
9.10.1	A norm characterization of PIDs	743
9.10.2	Dedekind-Hasse covers and non-Euclidean PIDs	745
9.11	Ideals and factorization in $\mathbb{Z}[x]$	749
9.11.1	Ideals in $\mathbb{Z}[x]$	750
9.11.2	Factorization in $\mathbb{Z}[x]$	750
9.11.3	Prime ideals in $\mathbb{Z}[x]$	752
9.11.4	Maximal ideals in $\mathbb{Z}[x]$	754
9.12	Divisibility and factorization in polynomial rings	755
9.12.1	Content and Gauss's lemma	755
9.12.2	Irreducibility criteria and factorization	759
9.13	Ideals in polynomial rings	762
9.13.1	Extension, contraction, and reduction	762
9.13.2	Prime ideals in polynomial rings	765
9.13.3	Maximal ideals in polynomial rings	767
9.14	Multivariate polynomial rings	770
9.14.1	Constructing polynomial rings in several variables	770
9.14.2	Hilbert's basis theorem	771
9.15	Exercises	774
Bibliography		793