

# Contents

<b>1</b>	<b>Preliminaries</b>	<b>1</b>
1.1	Sets and Mappings	1
1.1.1	Binary operations	2
1.1.2	Equivalence relations and equivalence classes	4
1.2	Some Elementary Combinatorics	6
1.2.1	Mathematical induction	7
1.2.2	The Binomial Theorem	8
<b>2</b>	<b>Groups and Fields: The Two Fundamental Notions of Algebra</b>	<b>11</b>
2.1	Groups and homomorphisms	11
2.1.1	The Definition of a Group	12
2.1.2	Some basic properties of groups	13
2.1.3	The symmetric groups $S(n)$	14
2.1.4	Cyclic groups	15
2.1.5	Dihedral groups: generators and relations	16
2.1.6	Subgroups	18
2.1.7	Homomorphisms and Cayley's Theorem	19
2.2	The Cosets of a Subgroup and Lagrange's Theorem	23
2.2.1	The definition of a coset	23
2.2.2	Lagrange's Theorem	25
2.3	Normal Subgroups and Quotient Groups	29
2.3.1	Normal subgroups	29
2.3.2	Constructing the quotient group $G/H$	30
2.3.3	Euler's Theorem via quotient groups	32
2.3.4	The First Isomorphism Theorem	34
2.4	Fields	36
2.4.1	The definition of a field	36
2.4.2	Arbitrary sums and products	38
2.5	The Basic Number Fields $\mathbb{Q}$ , $\mathbb{R}$ , and $\mathbb{C}$	40
2.5.1	The rational numbers $\mathbb{Q}$	40

2.5.2	The real numbers $\mathbb{R}$ . . . . .	40
2.5.3	The complex numbers $\mathbb{C}$ . . . . .	41
2.5.4	The geometry of $\mathbb{C}$ . . . . .	43
2.5.5	The Fundamental Theorem of Algebra . . . . .	45
2.6	Galois fields . . . . .	47
2.6.1	The prime fields $\mathbb{F}_p$ . . . . .	47
2.6.2	A four-element field . . . . .	48
2.6.3	The characteristic of a field . . . . .	49
2.6.4	Appendix: polynomials over a field. . . . .	51
<b>3</b>	<b>Matrices</b> . . . . .	<b>57</b>
3.1	Introduction to matrices and matrix algebra . . . . .	57
3.1.1	What is a matrix? . . . . .	58
3.1.2	Matrix addition . . . . .	59
3.1.3	Examples: matrices over $\mathbb{F}_2$ . . . . .	60
3.1.4	Matrix multiplication . . . . .	61
3.1.5	The Algebra of Matrix Multiplication . . . . .	63
3.1.6	The transpose of a matrix . . . . .	64
3.1.7	Matrices and linear mappings . . . . .	65
3.2	Reduced Row Echelon Form . . . . .	68
3.2.1	Reduced row echelon form and row operations. . . . .	68
3.2.2	Elementary matrices and row operations . . . . .	70
3.2.3	The row space and uniqueness of reduced row echelon form . . . . .	72
3.3	Linear Systems . . . . .	77
3.3.1	The coefficient matrix of a linear system. . . . .	77
3.3.2	Writing the solutions: the homogeneous case . . . . .	78
3.3.3	The inhomogeneous case. . . . .	79
3.3.4	A useful identity . . . . .	82
<b>4</b>	<b>Matrix Inverses, Matrix Groups and the <i>LPDU</i> Decomposition</b> . . .	<b>85</b>
4.1	The Inverse of a Square Matrix . . . . .	85
4.1.1	The definition of the inverse . . . . .	85
4.1.2	Results on Inverses . . . . .	86
4.1.3	Computing inverses. . . . .	88
4.2	Matrix Groups . . . . .	93
4.2.1	The definition of a matrix group . . . . .	93
4.2.2	Examples of matrix groups . . . . .	94
4.2.3	The group of permutation matrices . . . . .	95
4.3	The <i>LPDU</i> Factorization. . . . .	100
4.3.1	The basic ingredients: <i>L</i> , <i>P</i> , <i>D</i> , and <i>U</i> . . . . .	100
4.3.2	The main result . . . . .	102
4.3.3	Matrices with an <i>LDU</i> decomposition. . . . .	105
4.3.4	The Symmetric <i>LDU</i> Decomposition. . . . .	107

4.3.5	The Ranks of $A$ and $A^T$ . . . . .	108
<b>5</b>	<b>An Introduction to the Theory of Determinants</b> . . . . .	113
5.1	An Introduction to the Determinant Function . . . . .	114
5.1.1	The main theorem . . . . .	114
5.1.2	The computation of a determinant . . . . .	115
5.2	The Definition of the Determinant . . . . .	119
5.2.1	The signature of a permutation . . . . .	119
5.2.2	The determinant via Leibniz's Formula . . . . .	121
5.2.3	Consequences of the definition . . . . .	122
5.2.4	The effect of row operations on the determinant . . . . .	123
5.2.5	The proof of the main theorem . . . . .	125
5.2.6	Determinants and <i>LPDU</i> . . . . .	125
5.2.7	A beautiful formula: Lewis Carroll's identity . . . . .	126
5.3	Appendix: Further Results on Determinants . . . . .	130
5.3.1	The Laplace expansion . . . . .	130
5.3.2	Cramer's Rule . . . . .	132
5.3.3	The inverse of a matrix over $\mathbb{Z}$ . . . . .	134
<b>6</b>	<b>Vector Spaces</b> . . . . .	135
6.1	The Definition of a Vector Space and Examples . . . . .	136
6.1.1	The vector space axioms . . . . .	136
6.1.2	Examples . . . . .	138
6.2	Subspaces and Spanning Sets . . . . .	141
6.2.1	Spanning sets . . . . .	142
6.3	Linear Independence and Bases . . . . .	145
6.3.1	The definition of linear independence . . . . .	145
6.3.2	The definition of a basis . . . . .	147
6.4	Bases and Dimension . . . . .	151
6.4.1	The definition of dimension . . . . .	151
6.4.2	Some examples . . . . .	152
6.4.3	The Dimension Theorem . . . . .	153
6.4.4	Finding a basis of the column space . . . . .	156
6.4.5	A Galois field application . . . . .	157
6.5	The Grassmann Intersection Formula . . . . .	162
6.5.1	Intersections and sums of subspaces . . . . .	162
6.5.2	Proof of the Grassmann intersection formula . . . . .	163
6.5.3	Direct sums of subspaces . . . . .	165
6.5.4	External direct sums . . . . .	167
6.6	Inner Product Spaces . . . . .	169
6.6.1	The definition of an inner product . . . . .	169
6.6.2	Orthogonality . . . . .	170
6.6.3	Hermitian inner products . . . . .	173
6.6.4	Orthonormal bases . . . . .	174

6.6.5	The existence of orthonormal bases . . . . .	175
6.6.6	Fourier coefficients . . . . .	176
6.6.7	The orthogonal complement of a subspace . . . . .	177
6.6.8	Hermitian inner product spaces . . . . .	178
6.7	Vector Space Quotients . . . . .	183
6.7.1	Cosets of a subspace . . . . .	183
6.7.2	The quotient $V/W$ and the dimension formula . . . . .	184
6.8	Appendix: Linear Coding Theory . . . . .	187
6.8.1	The notion of a code . . . . .	187
6.8.2	Generating matrices . . . . .	188
6.8.3	Hamming distance . . . . .	188
6.8.4	Error-correcting codes . . . . .	190
6.8.5	Cosets and perfect codes . . . . .	192
6.8.6	The hat problem . . . . .	193
<b>7</b>	<b>Linear Mappings</b> . . . . .	<b>197</b>
7.1	Definitions and Examples . . . . .	197
7.1.1	Mappings . . . . .	197
7.1.2	The definition of a linear mapping . . . . .	198
7.1.3	Examples . . . . .	198
7.1.4	Matrix linear mappings . . . . .	200
7.1.5	An Application: rotations of the plane . . . . .	201
7.2	Theorems on Linear Mappings . . . . .	205
7.2.1	The kernel and image of a linear mapping . . . . .	205
7.2.2	The Rank–Nullity Theorem . . . . .	206
7.2.3	An existence theorem . . . . .	206
7.2.4	Vector space isomorphisms . . . . .	207
7.3	Isometries and Orthogonal Mappings . . . . .	211
7.3.1	Isometries and orthogonal linear mappings . . . . .	211
7.3.2	Orthogonal linear mappings on $\mathbb{R}^n$ . . . . .	212
7.3.3	Projections . . . . .	213
7.3.4	Reflections . . . . .	213
7.3.5	Projections on a general subspace . . . . .	215
7.3.6	Dimension two and the $O(2, \mathbb{R})$ -dichotomy . . . . .	216
7.3.7	The dihedral group as a subgroup of $O(2, \mathbb{R})$ . . . . .	218
7.3.8	The finite subgroups of $O(2, \mathbb{R})$ . . . . .	219
7.4	Coordinates with Respect to a Basis and Matrices of Linear Mappings . . . . .	222
7.4.1	Coordinates with respect to a basis . . . . .	222
7.4.2	The change of basis matrix . . . . .	223
7.4.3	The matrix of a linear mapping . . . . .	225
7.4.4	The Case $V = W$ . . . . .	226
7.4.5	Similar matrices . . . . .	228
7.4.6	The matrix of a composition $T \circ S$ . . . . .	228

7.4.7	The determinant of a linear mapping . . . . .	228
7.5	Further Results on Mappings . . . . .	232
7.5.1	The space $L(V, W)$ . . . . .	232
7.5.2	The dual space . . . . .	232
7.5.3	Multilinear maps . . . . .	234
7.5.4	A characterization of the determinant . . . . .	235
<b>8</b>	<b>Eigentheory</b> . . . . .	239
8.1	The Eigenvalue Problem and the Characteristic Polynomial . . . . .	239
8.1.1	First considerations: the eigenvalue problem for matrices . . . . .	240
8.1.2	The characteristic polynomial . . . . .	241
8.1.3	The characteristic polynomial of a $2 \times 2$ matrix . . . . .	243
8.1.4	A general formula for the characteristic polynomial . . . . .	244
8.2	Basic Results on Eigentheory . . . . .	251
8.2.1	Eigenpairs for linear mappings . . . . .	251
8.2.2	Diagonalizable matrices . . . . .	252
8.2.3	A criterion for diagonalizability . . . . .	254
8.2.4	The powers of a diagonalizable matrix . . . . .	255
8.2.5	The Fibonacci sequence as a dynamical system . . . . .	256
8.3	Two Characterizations of Diagonalizability . . . . .	259
8.3.1	Diagonalization via eigenspace decomposition . . . . .	259
8.3.2	A test for diagonalizability . . . . .	261
8.4	The Cayley–Hamilton Theorem . . . . .	268
8.4.1	Statement of the theorem . . . . .	268
8.4.2	The real and complex cases . . . . .	268
8.4.3	Nilpotent matrices . . . . .	269
8.4.4	A proof of the Cayley–Hamilton theorem . . . . .	269
8.4.5	The minimal polynomial of a linear mapping . . . . .	271
8.5	Self Adjoint Mappings and the Principal Axis Theorem . . . . .	274
8.5.1	The notion of self-adjointness . . . . .	274
8.5.2	Principal Axis Theorem for self-adjoint linear mappings . . . . .	275
8.5.3	Examples of self-adjoint linear mappings . . . . .	277
8.5.4	A projection formula for symmetric matrices . . . . .	278
8.6	The Group of Rotations of $\mathbb{R}^3$ and the Platonic Solids . . . . .	283
8.6.1	Rotations of $\mathbb{R}^3$ . . . . .	283
8.6.2	The Platonic solids . . . . .	286
8.6.3	The rotation group of a Platonic solid . . . . .	287
8.6.4	The cube and the octahedron . . . . .	288
8.6.5	Symmetry groups . . . . .	290
8.7	An Appendix on Field Extensions . . . . .	294

<b>9</b>	<b>Unitary Diagonalization and Quadratic Forms</b>	297
9.1	Schur Triangularization and the Normal Matrix Theorem	297
9.1.1	Upper triangularization via the unitary group	298
9.1.2	The normal matrix theorem	299
9.1.3	The Principal axis theorem: the short proof	300
9.1.4	Other examples of normal matrices	301
9.2	Quadratic Forms	305
9.2.1	Quadratic forms and congruence	305
9.2.2	Diagonalization of quadratic forms	306
9.2.3	Diagonalization in the real case	307
9.2.4	Hermitian forms	308
9.2.5	Positive definite matrices	308
9.2.6	The positive semidefinite case	310
9.3	Sylvester's Law of Inertia and Polar Decomposition	313
9.3.1	The law of inertia	313
9.3.2	The polar decomposition of a complex linear mapping	315
<b>10</b>	<b>The Structure Theory of Linear Mappings</b>	319
10.1	The Jordan–Chevalley Theorem	320
10.1.1	The statement of the theorem	320
10.1.2	The multiplicative Jordan–Chevalley decomposition	322
10.1.3	The proof of the Jordan–Chevalley theorem	323
10.1.4	An example	324
10.1.5	The Lie bracket	326
10.2	The Jordan Canonical Form	328
10.2.1	Jordan blocks and string bases	328
10.2.2	Jordan canonical form	329
10.2.3	String bases and nilpotent endomorphisms	330
10.2.4	Jordan canonical form and the minimal polynomial	333
10.2.5	The conjugacy class of a nilpotent matrix	334
<b>11</b>	<b>Theorems on Group Theory</b>	337
11.1	Group Actions and the Orbit Stabilizer Theorem	338
11.1.1	Group actions and $G$ -sets	338
11.1.2	The orbit stabilizer theorem	341
11.1.3	Cauchy's theorem	341
11.1.4	Conjugacy classes	343
11.1.5	Remarks on the center	344
11.1.6	A fixed-point theorem for $p$ -groups	344
11.1.7	Conjugacy classes in the symmetric group	345
11.2	The Finite Subgroups of $SO(3, \mathbb{R})$	349
11.2.1	The order of a finite subgroup of $SO(3, \mathbb{R})$	349

11.2.2	The order of a stabilizer $Gp$ . . . . .	351
11.3	The Sylow Theorems . . . . .	354
11.3.1	The first Sylow theorem . . . . .	354
11.3.2	The second Sylow theorem . . . . .	355
11.3.3	The third Sylow theorem. . . . .	355
11.3.4	Groups of order 12, 15, and 24. . . . .	356
11.4	The Structure of Finite Abelian Groups . . . . .	359
11.4.1	Direct products . . . . .	359
11.4.2	The structure theorem for finite abelian groups . . . . .	361
11.4.3	The Chinese Remainder Theorem . . . . .	362
11.5	Solvable Groups and Simple Groups . . . . .	364
11.5.1	The definition of a solvable group. . . . .	364
11.5.2	The commutator subgroup. . . . .	366
11.5.3	An example: $A(5)$ is simple. . . . .	367
11.5.4	Simple groups and the Jordan–Hölder theorem . . . . .	369
11.5.5	A few brief remarks on Galois theory . . . . .	370
11.6	Appendix: $S(n)$ , Cryptography, and the Enigma. . . . .	374
11.6.1	Substitution ciphers via $S(26)$ . . . . .	374
11.6.2	The Enigma. . . . .	375
11.6.3	Rejewski’s theorem on idempotents in $S(n)$ . . . . .	377
11.7	Breaking the Enigma . . . . .	379
<b>12</b>	<b>Linear Algebraic Groups: an Introduction</b> . . . . .	<b>383</b>
12.1	Linear Algebraic Groups. . . . .	383
12.1.1	Reductive and semisimple groups . . . . .	385
12.1.2	The classical groups . . . . .	386
12.1.3	Algebraic tori . . . . .	386
12.1.4	The Weyl group . . . . .	388
12.1.5	Borel subgroups. . . . .	390
12.1.6	The conjugacy of Borel subgroups . . . . .	391
12.1.7	The flag variety of a linear algebraic group. . . . .	392
12.1.8	The Bruhat decomposition of $GL(n, \mathbb{F})$ . . . . .	393
12.1.9	The Bruhat decomposition of a reductive group . . . . .	395
12.1.10	Parabolic subgroups. . . . .	396
12.2	Linearly reductive groups . . . . .	398
12.2.1	Invariant subspaces . . . . .	398
12.2.2	Maschke’s theorem . . . . .	398
12.2.3	Reductive groups. . . . .	399
12.2.4	Invariant theory . . . . .	400
	<b>Bibliography</b> . . . . .	<b>403</b>
	<b>Index</b> . . . . .	<b>407</b>



<http://www.springer.com/978-0-387-79427-3>

Groups, Matrices, and Vector Spaces

A Group Theoretic Approach to Linear Algebra

Carrell, J.B.

2017, XVII, 410 p., Hardcover

ISBN: 978-0-387-79427-3