

Contents

1	Set-Theoretic and Combinatorial Background	1
1.1	Sets and Maps	1
1.1.1	Sets	1
1.1.2	Maps	2
1.1.3	Fibers of Maps	3
1.2	Equivalence Classes	7
1.2.1	Equivalence Relations	7
1.2.2	Implicitly Defined Equivalences	9
1.3	Compositions of Maps	10
1.3.1	Composition Versus Multiplication	10
1.3.2	Right Inverse Map and the Axiom of Choice	11
1.3.3	Invertible Maps	12
1.3.4	Transformation Groups	12
1.4	Posets	13
1.4.1	Partial Order Relations	13
1.4.2	Well-Ordered Sets	15
1.4.3	Zorn's Lemma	15
	Problems for Independent Solution to Chap. 1	16
2	Integers and Residues	19
2.1	Fields, Rings, and Abelian Groups	19
2.1.1	Definition of a Field	19
2.1.2	Commutative Rings	21
2.1.3	Abelian Groups	21
2.1.4	Subtraction and Division	23
2.2	The Ring of Integers	24
2.2.1	Divisibility	24
2.2.2	The Equation $ax + by = k$ and the Greatest Common Divisor in \mathbb{Z}	24
2.2.3	The Euclidean Algorithm	25
2.3	Coprime Elements	26

2.4	Rings of Residues	27
2.4.1	Residue Classes Modulo n	27
2.4.2	Zero Divisors and Nilpotents	28
2.4.3	Invertible Elements in Residue Rings	28
2.4.4	Residue Fields	29
2.5	Direct Products of Commutative Groups and Rings	30
2.6	Homomorphisms	31
2.6.1	Homomorphisms of Abelian Groups	31
2.6.2	Kernel of a Homomorphism	32
2.6.3	Group of Homomorphisms	32
2.6.4	Homomorphisms of Commutative Rings	33
2.6.5	Homomorphisms of Fields	34
2.7	Chinese Remainder Theorem	34
2.8	Characteristic	35
2.8.1	Prime Subfield	35
2.8.2	Frobenius Endomorphism	36
	Problems for Independent Solution to Chap. 2	37
3	Polynomials and Simple Field Extensions	41
3.1	Formal Power Series	41
3.1.1	Rings of Formal Power Series	41
3.1.2	Algebraic Operations on Power Series	42
3.1.3	Polynomials	43
3.1.4	Differential Calculus	44
3.2	Polynomial Rings	46
3.2.1	Division	46
3.2.2	Coprime Polynomials	48
3.2.3	Euclidean Algorithm	48
3.3	Roots of Polynomials	50
3.3.1	Common Roots	50
3.3.2	Multiple Roots	51
3.3.3	Separable Polynomials	51
3.4	Adjunction of Roots	52
3.4.1	Residue Class Rings	52
3.4.2	Algebraic Elements	54
3.4.3	Algebraic Closure	55
3.5	The Field of Complex Numbers	55
3.5.1	The Complex Plane	55
3.5.2	Complex Conjugation	58
3.5.3	Trigonometry	58
3.5.4	Roots of Unity and Cyclotomic Polynomials	60
3.5.5	The Gaussian Integers	62
3.6	Finite Fields	62
3.6.1	Finite Multiplicative Subgroups in Fields	62
3.6.2	Description of All Finite Fields	63

3.6.3	Quadratic Residues	65
	Problems for Independent Solution to Chap. 3	66
4	Elementary Functions and Power Series Expansions	73
4.1	Rings of Fractions	73
4.1.1	Localization	73
4.1.2	Field of Fractions of an Integral Domain	75
4.2	Field of Rational Functions	76
4.2.1	Simplified Fractions	76
4.2.2	Partial Fraction Expansion	77
4.2.3	Power Series Expansions of Rational Functions	79
4.2.4	Linear Recurrence Relations	80
4.3	Logarithm and Exponential	82
4.3.1	The Logarithm	83
4.3.2	The Exponential	83
4.3.3	Power Function and Binomial Formula	84
4.4	Todd's Series and Bernoulli Numbers	88
4.4.1	Action of $\mathbb{Q}[[d/dt]]$ on $\mathbb{Q}[t]$	88
4.4.2	Bernoulli Numbers	91
4.5	Fractional Power Series	92
4.5.1	Puiseux Series	92
4.5.2	Newton's Method	96
	Problems for Independent Solution to Chap. 4	100
5	Ideals, Quotient Rings, and Factorization	103
5.1	Ideals	103
5.1.1	Definition and Examples	103
5.1.2	Noetherian Rings	104
5.2	Quotient Rings	106
5.2.1	Factorization Homomorphism	106
5.2.2	Maximal Ideals and Evaluation Maps	107
5.2.3	Prime Ideals and Ring Homomorphisms to Fields	108
5.2.4	Finitely Generated Commutative Algebras	109
5.3	Principal Ideal Domains	109
5.3.1	Euclidean Domains	109
5.3.2	Greatest Common Divisor	110
5.3.3	Coprime Elements	111
5.3.4	Irreducible Elements	111
5.4	Unique Factorization Domains	112
5.4.1	Irreducible Factorization	112
5.4.2	Prime Elements	114
5.4.3	GCD in Unique Factorization Domains	115
5.4.4	Polynomials over Unique Factorization Domains	116

5.5	Factorization of Polynomials with Rational Coefficients	118
5.5.1	Reduction of Coefficients	118
5.5.2	Kronecker's Algorithm	119
	Problems for Independent Solution to Chap. 5	120
6	Vectors	123
6.1	Vector Spaces and Modules	123
6.1.1	Definitions and Examples	123
6.1.2	Linear Maps	124
6.1.3	Proportional Vectors	125
6.2	Bases and Dimension	127
6.2.1	Linear Combinations	127
6.2.2	Linear Dependence	130
6.2.3	Basis of a Vector Space	132
6.2.4	Infinite-Dimensional Vector Spaces	134
6.3	Space of Linear Maps	135
6.3.1	Kernel and Image	135
6.3.2	Matrix of a Linear Map	136
6.4	Vector Subspaces	138
6.4.1	Codimension	138
6.4.2	Linear Spans	138
6.4.3	Sum of Subspaces	139
6.4.4	Transversal Subspaces	140
6.4.5	Direct Sums and Direct Products	141
6.5	Affine Spaces	142
6.5.1	Definition and Examples	142
6.5.2	Affinization and Vectorization	143
6.5.3	Center of Mass	143
6.5.4	Affine Subspaces	145
6.5.5	Affine Maps	148
6.5.6	Affine Groups	148
6.6	Quotient Spaces	149
6.6.1	Quotient by a Subspace	149
6.6.2	Quotient Groups of Abelian Groups	150
	Problems for Independent Solution to Chap. 6	151
7	Duality	155
7.1	Dual Spaces	155
7.1.1	Covectors	155
7.1.2	Canonical Inclusion $V \hookrightarrow V^{**}$	158
7.1.3	Dual Bases	158
7.1.4	Pairings	160
7.2	Annihilators	161

7.3	Dual Linear Maps	164
7.3.1	Pullback of Linear Forms	164
7.3.2	Rank of a Matrix	165
	Problems for Independent Solution to Chap. 7	167
8	Matrices	173
8.1	Associative Algebras over a Field	173
8.1.1	Definition of Associative Algebra	173
8.1.2	Invertible Elements	174
8.1.3	Algebraic and Transcendental Elements	175
8.2	Matrix Algebras	175
8.2.1	Multiplication of Matrices	175
8.2.2	Invertible Matrices	179
8.3	Transition Matrices	180
8.4	Gaussian Elimination	182
8.4.1	Elimination by Row Operations	182
8.4.2	Location of a Subspace with Respect to a Basis	190
8.4.3	Gaussian Method for Inverting Matrices	192
8.5	Matrices over Noncommutative Rings	195
	Problems for Independent Solution to Chap. 8	199
9	Determinants	205
9.1	Volume Forms	205
9.1.1	Volume of an n -Dimensional Parallelepiped	205
9.1.2	Skew-Symmetric Multilinear Forms	207
9.2	Digression on Parities of Permutations	208
9.3	Determinants	210
9.3.1	Basic Properties of Determinants	211
9.3.2	Determinant of a Linear Endomorphism	214
9.4	Grassmannian Polynomials	215
9.4.1	Polynomials in Skew-Commuting Variables	215
9.4.2	Linear Change of Grassmannian Variables	216
9.5	Laplace Relations	217
9.6	Adjunct Matrix	220
9.6.1	Row and Column Cofactor Expansions	220
9.6.2	Matrix Inversion	221
9.6.3	Cayley–Hamilton Identity	222
9.6.4	Cramer’s Rules	223
	Problems for Independent Solution to Chap. 9	225
10	Euclidean Spaces	229
10.1	Inner Product	229
10.1.1	Euclidean Structure	229
10.1.2	Length of a Vector	230
10.1.3	Orthogonality	230

10.2	Gramians	233
10.2.1	Gram Matrices	233
10.2.2	Euclidean Volume	234
10.2.3	Orientation	234
10.2.4	Cauchy–Bunyakovsky–Schwarz Inequality	235
10.3	Duality	235
10.3.1	Isomorphism $V \simeq V^*$ Provided by Euclidean Structure	235
10.3.2	Orthogonal Complement and Orthogonal Projection	236
10.4	Metric Geometry	238
10.4.1	Euclidean Metric	238
10.4.2	Angles	242
10.5	Orthogonal Group	244
10.5.1	Euclidean Isometries	244
10.5.2	Orthogonal Matrices	244
	Problems for Independent Solution to Chap. 10	248
11	Projective Spaces	253
11.1	Projectivization	253
11.1.1	Points and Charts	253
11.1.2	Global Homogeneous Coordinates	254
11.1.3	Local Affine Coordinates	255
11.2	Polynomials Revisited	258
11.2.1	Polynomial Functions on a Vector Space	258
11.2.2	Symmetric Algebra of a Vector Space	258
11.2.3	Polynomial Functions on an Affine Space	262
11.2.4	Affine Algebraic Varieties	262
11.3	Projective Algebraic Varieties	263
11.3.1	Homogeneous Equations	263
11.3.2	Projective Closure of an Affine Hypersurface	264
11.3.3	Space of Hypersurfaces	265
11.3.4	Linear Systems of Hypersurfaces	266
11.4	Complementary Subspaces and Projections	268
11.5	Linear Projective Isomorphisms	270
11.5.1	Action of a Linear Isomorphism on Projective Space	270
11.5.2	Linear Projective Group	271
11.6	Cross Ratio	272
11.6.1	Action of the Permutation Group S_4	272
11.6.2	Special Quadruples of Points	273
11.6.3	Harmonic Pairs of Points	274
	Problems for Independent Solution to Chap. 11	275
12	Groups	279
12.1	Definition and First Examples	279

12.2	Cycles	280
12.2.1	Cyclic Subgroups	280
12.2.2	Cyclic Groups	281
12.2.3	Cyclic Type of Permutation	281
12.3	Groups of Figures	283
12.4	Homomorphisms of Groups	289
12.5	Group Actions	294
12.5.1	Definitions and Terminology	294
12.5.2	Orbits and Stabilizers	295
12.5.3	Enumeration of Orbits	298
12.6	Factorization of Groups	300
12.6.1	Cosets	300
12.6.2	Normal Subgroups	300
12.6.3	Quotient Groups	301
	Problems for Independent Solution to Chap. 12	303
13	Descriptions of Groups	309
13.1	Generators and Relations	309
13.1.1	Free Groups	309
13.1.2	Presentation of a Group by Generators and Relators	310
13.1.3	Presentations for the Dihedral Groups	312
13.1.4	Presentations of the Groups of Platonic Solids	313
13.2	Presentation of the Symmetric Group	318
13.2.1	Complete Group of a Regular Simplex	318
13.2.2	Bruhat Order	321
13.3	Simple Groups and Composition Series	324
13.3.1	Jordan–Hölder Series	324
13.3.2	Finite Simple Groups	326
13.4	Semidirect Products	328
13.4.1	Semidirect Product of Subgroups	328
13.4.2	Semidirect Product of Groups	329
13.5	p -Groups and Sylow’s Theorems	330
13.5.1	p -Groups in Action	330
13.5.2	Sylow Subgroups	331
	Problems for Independent Solution to Chap. 13	332
14	Modules over a Principal Ideal Domain	335
14.1	Modules over Commutative Rings Revisited	335
14.1.1	Free Modules	336
14.1.2	Generators and Relations	337
14.1.3	Linear Maps	338
14.1.4	Matrices of Linear Maps	339
14.1.5	Torsion	341
14.1.6	Quotient of a Module by an Ideal	341
14.1.7	Direct Sum Decompositions	341
14.1.8	Semisimplicity	343

14.2	Invariant Factors	344
14.2.1	Submodules of Finitely Generated Free Modules	344
14.2.2	Deduction of the Invariant Factors Theorem from the Smith Normal Form Theorem	345
14.2.3	Uniqueness of the Smith Normal Form	346
14.2.4	Gaussian Elimination over a Principal Ideal Domain	346
14.3	Elementary Divisors	351
14.3.1	Elementary Divisors Versus Invariant Factors	351
14.3.2	Existence of the Canonical Decomposition	353
14.3.3	Splitting Off Torsion	353
14.3.4	Splitting Off p -Torsion	353
14.3.5	Invariance of p -Torsion Exponents	354
14.4	Description of Finitely Generated Abelian Groups	355
14.4.1	Canonical Form of a Finitely Generated Abelian Group	355
14.4.2	Abelian Groups Presented by Generators and Relations	356
	Problems for Independent Solution to Chap. 14	356
15	Linear Operators	361
15.1	Classification of Operators	361
15.1.1	Spaces with Operators	361
15.1.2	Invariant Subspaces and Decomposability	361
15.1.3	Space with Operator as a $\mathbb{k}[t]$ -Module	362
15.1.4	Elementary Divisors	363
15.1.5	Minimal Polynomial	365
15.1.6	Characteristic Polynomial	366
15.2	Operators of Special Types	367
15.2.1	Nilpotent Operators	367
15.2.2	Semisimple Operators	368
15.2.3	Cyclic Vectors and Cyclic Operators	370
15.2.4	Eigenvectors and Eigenvalues	371
15.2.5	Eigenspaces	372
15.2.6	Diagonalizable Operators	372
15.2.7	Annihilating Polynomials	373
15.3	Jordan Decomposition	375
15.3.1	Jordan Normal Form	375
15.3.2	Root Decomposition	376
15.3.3	Commuting Operators	377
15.3.4	Nilpotent and Diagonalizable Components	378
15.4	Functions of Operators	379
15.4.1	Evaluation of Functions on an Operator	379
15.4.2	Interpolating Polynomial	381
15.4.3	Comparison with Analytic Approaches	383
	Problems for Independent Solution to Chap. 15	384

16	Bilinear Forms	387
16.1	Bilinear Forms and Correlations	387
16.1.1	Space with Bilinear Form	387
16.1.2	Gramians	388
16.1.3	Left Correlation	389
16.1.4	Nondegeneracy	390
16.1.5	Kernels	390
16.1.6	Nonsymmetric and (Skew)-Symmetric Forms	391
16.1.7	Characteristic Polynomial and Characteristic Values	392
16.2	Nondegenerate Forms	395
16.2.1	Dual Bases	395
16.2.2	Isotropic Subspaces	395
16.2.3	Isometry Group	396
16.2.4	Correspondence Between Forms and Operators	396
16.2.5	Canonical Operator	397
16.3	Adjoint Operators	399
16.3.1	Reflexive Operators	400
16.4	Orthogonals and Orthogonal Projections	403
16.4.1	Orthogonal Projections	403
16.4.2	Biorthogonal Direct Sums	405
16.4.3	Classification of Nondegenerate Forms	405
16.5	Symmetric and Skew-Symmetric Forms	408
16.5.1	Orthogonals and Kernel	409
16.5.2	Orthogonal Projections	409
16.5.3	Adjoint Operators	411
16.5.4	Form–Operator Correspondence	411
16.6	Symplectic Spaces	411
16.6.1	Symplectic Group	412
16.6.2	Lagrangian Subspaces	413
16.6.3	Pfaffian	414
	Problems for Independent Solution to Chap. 16	416
17	Quadratic Forms and Quadrics	421
17.1	Quadratic Forms and Their Polarizations	421
17.1.1	Space with a Quadratic Form	421
17.1.2	Gramian and Gram Determinant	422
17.1.3	Kernel and Rank	423
17.1.4	Sums of Squares	423
17.1.5	Isotropic and Anisotropic Subspaces	424
17.1.6	Hyperbolic Forms	425
17.2	Orthogonal Geometry of Nonsingular Forms	427
17.2.1	Isometries	427
17.2.2	Reflections	428

17.3	Quadratic Forms over Real and Simple Finite Fields.....	431
17.3.1	Quadratic Forms over $\mathbb{F}_p = \mathbb{Z}/(p)$	432
17.3.2	Real Quadratic Forms.....	433
17.3.3	How to Find the Signature of a Real Form.....	434
17.4	Projective Quadrics.....	435
17.4.1	Geometric Properties of Projective Quadrics.....	435
17.4.2	Smooth Quadrics.....	440
17.4.3	Polarities.....	443
17.5	Affine Quadrics.....	444
17.5.1	Projective Enhancement of Affine Quadrics.....	444
17.5.2	Smooth Central Quadrics.....	447
17.5.3	Paraboloids.....	448
17.5.4	Simple Cones.....	449
17.5.5	Cylinders.....	450
	Problems for Independent Solution to Chap. 17.....	454
18	Real Versus Complex	459
18.1	Realification.....	459
18.1.1	Realification of a Complex Vector Space.....	459
18.1.2	Comparison of Linear Groups.....	459
18.2	Complexification.....	462
18.2.1	Complexification of a Real Vector Space.....	462
18.2.2	Complex Conjugation.....	463
18.2.3	Complexification of Linear Maps.....	463
18.2.4	Complex Eigenvectors.....	464
18.2.5	Complexification of the Dual Space.....	465
18.2.6	Complexification of a Bilinear Form.....	465
18.3	Real Structures.....	466
18.4	Complex Structures.....	467
18.5	Hermitian Enhancement of Euclidean Structure.....	469
18.5.1	Hermitian Structure.....	469
18.5.2	Kähler Triples.....	471
18.5.3	Completing Kähler Triples for a Given Euclidean Structure.....	472
18.6	Hermitian Enhancement of Symplectic Structure.....	473
18.6.1	Completing Kähler Triples for a Given Symplectic Structure.....	473
18.6.2	Siegel Upper Half-Space and Riemann Relations.....	476
	Problems for Independent Solution to Chap. 18.....	478
19	Hermitian Spaces	481
19.1	Hermitian Geometry.....	481
19.1.1	Gramians.....	482
19.1.2	Gram–Schmidt Orthogonalization Procedure.....	482
19.1.3	Cauchy–Schwarz Inequality.....	483
19.1.4	Unitary Group.....	483

19.1.5	Hermitian Volume	484
19.1.6	Hermitian Correlation	484
19.1.7	Orthogonal Projections	485
19.1.8	Angle Between Two Lines	486
19.2	Adjoint Linear Maps	487
19.2.1	Hermitian Adjunction	487
19.2.2	Adjoint Endomorphisms	488
19.2.3	Euclidean Adjunction	489
19.3	Normal Operators	491
19.3.1	Orthogonal Diagonalization	491
19.3.2	Normal Operators in Euclidean Space	492
19.4	Polar and Singular Value Decompositions	495
19.4.1	Polar Decomposition	495
19.4.2	Exponential Cover of the Unitary Group	496
19.4.3	Singular Value Decomposition	497
	Problems for Independent Solution to Chap. 19	499
20	Quaternions and Spinors	503
20.1	Complex 2×2 Matrices and Quaternions	503
20.1.1	$\text{Mat}_2(\mathbb{C})$ as the Complexification of Euclidean \mathbb{R}^4	503
20.1.2	Algebra of Quaternions	505
20.1.3	Real and Pure Imaginary Quaternions	506
20.1.4	Quaternionic Norm	506
20.1.5	Division	507
20.2	Geometry of Quaternions	507
20.2.1	Universal Covering $S^3 = \text{SU}_2 \rightarrow \text{SO}_3(\mathbb{R})$	509
20.2.2	Topological Comment	510
20.2.3	Two Pencils of Hermitian Structures	512
20.3	Spinors	513
20.3.1	Geometry of Hermitian Enhancements of Euclidean \mathbb{R}^4	513
20.3.2	Explicit Formulas	514
20.3.3	Hopf Bundle	515
	Problems for Independent Solution to Chap. 20	516
	Hints to Selected Exercises	519
	References	545
	Index	547

Algebra I

Textbook for Students of Mathematics

Gorodentsev, A.L.

2016, XX, 564 p. 79 illus., 42 illus. in color., Hardcover

ISBN: 978-3-319-45284-5