

# Contents

<b>1</b>	<b>Prerequisites: Basics of Set Theory and Integers</b>	<b>1</b>
1.1	Sets: Introductory Concepts	2
1.2	Relations on Sets	8
1.2.1	Equivalence Relation	8
1.2.2	Partial Order Relations	12
1.2.3	Operations on Binary Relations	17
1.2.4	Functions or Mappings	18
1.3	Countability and Cardinality of Sets	25
1.3.1	Continuum Hypothesis	31
1.3.2	Exercises	36
1.4	Integers	39
1.5	Congruences	48
1.5.1	Exercises	52
1.6	Additional Reading	53
	References	53
<b>2</b>	<b>Groups: Introductory Concepts</b>	<b>55</b>
2.1	Binary Operations	55
2.2	Semigroups	58
2.2.1	Topological Semigroups	68
2.2.2	Fuzzy Ideals in a Semigroup	69
2.2.3	Exercises	70
2.3	Groups	72
2.4	Subgroups and Cyclic Groups	82
2.5	Lagrange's Theorem	89
2.6	Normal Subgroups, Quotient Groups and Homomorphism Theorems	92
2.7	Geometrical Applications	99
2.7.1	Symmetry Groups of Geometric Figures in Euclidean Plane	99
2.7.2	Group of Rotations of the Sphere	101

2.7.3	Clock Arithmetic . . . . .	102
2.8	Free Abelian Groups and Structure Theorem . . . . .	103
2.8.1	Exercises . . . . .	110
2.9	Topological Groups, Lie Groups and Hopf Groups . . . . .	112
2.9.1	Topological Groups . . . . .	112
2.9.2	Lie Groups . . . . .	113
2.9.3	Hopf's Groups or $H$ -Groups . . . . .	113
2.10	Fundamental Groups . . . . .	115
2.10.1	A Generalization of Fundamental Groups . . . . .	116
2.11	Exercises . . . . .	121
2.12	Exercises (Objective Type) . . . . .	129
2.13	Additional Reading . . . . .	135
	References . . . . .	135
<b>3</b>	<b>Actions of Groups, Topological Groups and Semigroups . . . . .</b>	<b>137</b>
3.1	Actions of Groups . . . . .	137
3.2	Group Actions to Counting and Sylow's Theorems . . . . .	142
3.2.1	$p$ -Groups and Cauchy's Theorem . . . . .	144
3.2.2	Class Equation and Sylow's Theorems . . . . .	145
3.2.3	Exercises . . . . .	149
3.3	Actions of Topological Groups and Lie Groups . . . . .	151
3.3.1	Exercises . . . . .	152
3.4	Actions of Semigroups and State Machines . . . . .	155
3.4.1	Exercises . . . . .	157
3.5	Additional Reading . . . . .	157
	References . . . . .	158
<b>4</b>	<b>Rings: Introductory Concepts . . . . .</b>	<b>159</b>
4.1	Introductory Concepts . . . . .	159
4.2	Subrings . . . . .	166
4.3	Characteristic of a Ring . . . . .	168
4.4	Embedding and Extension for Rings . . . . .	170
4.5	Power Series Rings and Polynomial Rings . . . . .	177
4.6	Rings of Continuous Functions . . . . .	184
4.7	Endomorphism Ring . . . . .	186
4.8	Problems and Supplementary Examples . . . . .	188
4.8.1	Exercises . . . . .	193
4.9	Additional Reading . . . . .	201
	References . . . . .	201
<b>5</b>	<b>Ideals of Rings: Introductory Concepts . . . . .</b>	<b>203</b>
5.1	Ideals: Introductory concepts . . . . .	203
5.2	Quotient Rings . . . . .	206
5.3	Prime Ideals and Maximal Ideals . . . . .	209
5.4	Local Rings . . . . .	213
5.5	Application to Algebraic Geometry . . . . .	214

5.5.1	Affine Algebraic Sets . . . . .	214
5.5.2	Ideal of a Set of Points in $K^n$ . . . . .	215
5.5.3	Affine Variety . . . . .	217
5.5.4	The Zariski Topology in $K^n$ . . . . .	217
5.6	Chinese Remainder Theorem . . . . .	220
5.7	Ideals of $C(X)$ . . . . .	222
5.8	Exercises . . . . .	227
5.9	Additional Reading . . . . .	235
	References . . . . .	235
<b>6</b>	<b>Factorization in Integral Domains and in Polynomial Rings</b> . . . .	237
6.1	Divisibility . . . . .	237
6.2	Euclidean Domains . . . . .	243
6.3	Factorization of Polynomials over a UFD . . . . .	246
6.4	Supplementary Examples (SE-I) . . . . .	249
6.5	Exercises . . . . .	251
6.6	Additional Reading . . . . .	255
	References . . . . .	255
<b>7</b>	<b>Rings with Chain Conditions</b> . . . . .	257
7.1	Noetherian and Artinian Rings . . . . .	257
7.2	An Application of Hilbert Basis Theorem to Algebraic Geometry . . . . .	267
7.3	An Application of Cohen's Theorem . . . . .	268
7.4	Supplementary Examples (SE-I) . . . . .	269
7.5	Exercises . . . . .	269
7.6	Additional Reading . . . . .	271
	References . . . . .	271
<b>8</b>	<b>Vector Spaces</b> . . . . .	273
8.1	Introductory Concepts . . . . .	273
8.2	Subspaces . . . . .	276
8.3	Quotient Spaces . . . . .	279
8.3.1	Geometrical Interpretation of Quotient Spaces . . . . .	279
8.4	Linear Independence and Bases . . . . .	280
8.4.1	Geometrical Interpretation . . . . .	282
8.4.2	Coordinate System . . . . .	288
8.4.3	Affine Set . . . . .	288
8.4.4	Exercises . . . . .	289
8.5	Linear Transformations and Associated Algebra . . . . .	290
8.5.1	Algebra over a Field . . . . .	300
8.6	Correspondence Between Linear Transformations and Matrices . . . . .	303
8.7	Eigenvalues and Eigenvectors . . . . .	310
8.8	The Cayley–Hamilton Theorem . . . . .	317
8.9	Jordan Canonical Form . . . . .	320
8.10	Inner Product Spaces . . . . .	326
8.10.1	Geometry in $\mathbf{R}^n$ and $\mathbf{C}^n$ . . . . .	326

8.10.2	Inner Product Spaces: Introductory Concepts . . . . .	326
8.11	Hilbert Spaces . . . . .	330
8.12	Quadratic Forms . . . . .	334
8.12.1	Quadratic Forms: Introductory Concepts . . . . .	335
8.13	Exercises . . . . .	340
8.14	Additional Reading . . . . .	353
	References . . . . .	353
<b>9</b>	<b>Modules . . . . .</b>	<b>355</b>
9.1	Introductory Concepts . . . . .	355
9.2	Submodules . . . . .	358
9.3	Module Homomorphisms . . . . .	366
9.4	Quotient Modules and Isomorphism Theorems . . . . .	370
9.5	Modules of Homomorphisms . . . . .	373
9.6	Free Modules, Modules over PID and Structure Theorems . . . . .	375
9.6.1	Free Modules . . . . .	375
9.6.2	Modules over PID . . . . .	380
9.6.3	Structure Theorems . . . . .	381
9.7	Exact Sequences . . . . .	385
9.8	Modules with Chain Conditions . . . . .	392
9.9	Representations . . . . .	394
9.10	Worked-Out Exercises . . . . .	395
9.10.1	Exercises . . . . .	399
9.11	Homology and Cohomology Modules . . . . .	406
9.11.1	Exercises . . . . .	409
9.12	Topology on Spectrum of Modules and Rings . . . . .	409
9.12.1	Spectrum of Modules . . . . .	409
9.12.2	Spectrum of Rings and Associated Schemes . . . . .	410
9.13	Additional Reading . . . . .	411
	References . . . . .	411
<b>10</b>	<b>Algebraic Aspects of Number Theory . . . . .</b>	<b>413</b>
10.1	A Brief History of Prime Numbers . . . . .	413
10.2	Some Properties of Prime Numbers . . . . .	416
10.2.1	Prime Number Theorem . . . . .	419
10.2.2	Twin Primes . . . . .	419
10.3	Multiplicative Functions . . . . .	420
10.3.1	Euler phi-Function . . . . .	421
10.3.2	Sum of Divisor Functions and Number of Divisor Functions . . . . .	423
10.4	Group of Units . . . . .	424
10.5	Quadratic Residues and Quadratic Reciprocity . . . . .	430
10.6	Fermat Numbers . . . . .	443
10.7	Perfect Numbers and Mersenne Numbers . . . . .	445
10.8	Analysis of the Complexity of Algorithms . . . . .	448
10.8.1	Asymptotic Notation . . . . .	448

10.8.2	Relational Properties Among the Asymptotic Notations	451
10.8.3	Poly-time and Exponential-Time Algorithms . . . . .	451
10.8.4	Notations for Algorithms . . . . .	452
10.8.5	Analysis of Few Important Number Theoretic Algorithms . . . . .	453
10.8.6	Euclidean and Extended Euclidean Algorithms . . . . .	456
10.8.7	Modular Arithmetic . . . . .	461
10.8.8	Square and Multiply Algorithm . . . . .	461
10.9	Primality Testing . . . . .	463
10.9.1	Deterministic Primality Testing . . . . .	463
10.9.2	AKS Algorithm . . . . .	465
10.10	Probabilistic or Randomized Primality Testing . . . . .	466
10.10.1	Solovay–Strassen Primality Testing . . . . .	467
10.10.2	Pseudo-primes and Primality Testing Based on Fermat’s Little Theorem . . . . .	469
10.10.3	Miller–Rabin Primality Testing . . . . .	474
10.11	Exercise . . . . .	483
10.12	Additional Reading . . . . .	485
	References . . . . .	486
<b>11</b>	<b>Algebraic Numbers</b> . . . . .	487
11.1	Field Extension . . . . .	487
11.1.1	Exercises . . . . .	496
11.2	Finite Fields . . . . .	498
11.2.1	Exercises . . . . .	499
11.3	Algebraic Numbers . . . . .	500
11.4	Exercises . . . . .	504
11.5	Algebraic Integers . . . . .	504
11.6	Gaussian Integers . . . . .	506
11.7	Algebraic Number Fields . . . . .	509
11.8	Quadratic Fields . . . . .	510
11.9	Exercises . . . . .	511
11.10	Additional Reading . . . . .	515
	References . . . . .	516
<b>12</b>	<b>Introduction to Mathematical Cryptography</b> . . . . .	517
12.1	Introduction to Cryptography . . . . .	517
12.2	Kerckhoffs’ Law . . . . .	519
12.3	Cryptanalysis . . . . .	519
12.3.1	Brute-Force Search . . . . .	521
12.4	Some Classical Cryptographic Schemes . . . . .	521
12.4.1	Caesarian Cipher or Shift Cipher . . . . .	522
12.4.2	Affine Cipher . . . . .	523
12.4.3	Substitution Cipher . . . . .	523
12.4.4	Vigenère Cipher . . . . .	525
12.4.5	Hill Cipher . . . . .	526

12.5	Introduction to Public-Key Cryptography . . . . .	527
12.5.1	Discrete Logarithm Problem (DLP) . . . . .	530
12.5.2	Diffie–Hellman Key Exchange . . . . .	530
12.6	RSA Public Key Cryptosystem . . . . .	532
12.6.1	Algorithm for RSA Cryptosystem (Rivest et al. 1978) . . . . .	533
12.6.2	Sketch of the Proof of the Decryption . . . . .	534
12.6.3	Some Attacks on RSA Cryptosystem . . . . .	534
12.7	ElGamal Cryptosystem . . . . .	536
12.7.1	Algorithm for ElGamal Cryptosystem . . . . .	537
12.8	Rabin Cryptosystem . . . . .	538
12.8.1	Square Roots Modulo $N$ . . . . .	538
12.8.2	Algorithm for a variant of Rabin Cryptosystem . . . . .	540
12.9	Digital Signature . . . . .	541
12.9.1	RSA Based Digital Signature Scheme . . . . .	543
12.10	Oblivious Transfer . . . . .	544
12.10.1	OT Based on RSA . . . . .	546
12.11	Secret Sharing . . . . .	547
12.11.1	Shamir’s Threshold Secret Sharing Scheme . . . . .	549
12.12	Visual Cryptography . . . . .	551
12.12.1	$(2, 2)$ -Visual Cryptographic Scheme . . . . .	552
12.12.2	Visual Threshold Schemes . . . . .	555
12.12.3	The Model for Black and White VCS . . . . .	555
12.12.4	Basis Matrices . . . . .	557
12.12.5	Share Distribution Algorithm . . . . .	557
12.12.6	$(2, n)$ -Threshold VCS . . . . .	557
12.12.7	Applications of Linear Algebra to Visual Cryptographic Schemes for $(n, n)$ -VCS . . . . .	558
12.12.8	Applications of Linear Algebra to Visual Cryptographic Schemes for General Access Structure . . . . .	560
12.13	Open-Source Software: SAGE . . . . .	565
12.13.1	Sage Implementation of RSA Cryptosystem . . . . .	567
12.13.2	SAGE Implementation of ElGamal Plulic Key Cryptosystem . . . . .	576
12.13.3	SAGE Implementation of Rabin Plulic Key Cryptosystem . . . . .	577
12.14	Exercises . . . . .	580
12.15	Additional Reading . . . . .	583
	References . . . . .	583
<b>Appendix A</b>	<b>Some Aspects of Semirings . . . . .</b>	<b>585</b>
A.1	Introductory Concepts . . . . .	585
A.2	More Results on Semirings . . . . .	588
A.3	Ring Congruences and Their Characterization . . . . .	591
A.4	$k$ -Regular Semirings . . . . .	593
A.5	The Ring Completion of a Semiring . . . . .	596

A.6	Structure Spaces of Semirings . . . . .	597
A.7	Worked-Out Exercises and Exercises . . . . .	601
A.8	Additional Reading . . . . .	603
	References . . . . .	604
<b>Appendix B</b>	<b>Category Theory . . . . .</b>	<b>605</b>
B.1	Categories . . . . .	605
B.2	Special Morphisms . . . . .	607
B.3	Functors . . . . .	608
B.4	Natural Transformations . . . . .	610
B.5	Presheaf and Sheaf . . . . .	614
B.6	Exercises . . . . .	616
B.7	Additional Reading . . . . .	618
	References . . . . .	619
<b>Appendix C</b>	<b>A Brief Historical Note . . . . .</b>	<b>621</b>
C.1	Additional Reading . . . . .	630
	References . . . . .	630
<b>Index</b>	<b>. . . . .</b>	<b>631</b>

<http://www.springer.com/978-81-322-1598-1>

Basic Modern Algebra with Applications

Adhikari, M.R.; Adhikari, A.

2014, XIX, 637 p. 48 illus., Hardcover

ISBN: 978-81-322-1598-1