
CONTENTS*

	Preface	xv
Chapter 1	Why Abstract Algebra? History of Algebra. New Algebras. Algebraic Structures. Axioms and Axiomatic Algebra. Abstraction in Algebra.	1
Chapter 2	Operations Operations on a Set. Properties of Operations.	19
Chapter 3	The Definition of Groups Groups. Examples of Infinite and Finite Groups. Examples of Abelian and Nonabelian Groups. Group Tables. <i>Theory of Coding: Maximum-Likelihood Decoding.</i>	25
Chapter 4	Elementary Properties of Groups Uniqueness of Identity and Inverses. Properties of Inverses. <i>Direct Product of Groups.</i>	36
Chapter 5	Subgroups Definition of Subgroup. Generators and Defining Relations. <i>Cayley Diagrams. Center of a Group. Group Codes; Hamming Code.</i>	44

* Italic headings indicate topics discussed in the exercise sections.

Chapter 6	Functions Injective, Surjective, Bijective Function. Composite and Inverse of Functions. <i>Finite-State Machines. Automata and Their Semigroups.</i>	56
Chapter 7	Groups of Permutations Symmetric Groups. Dihedral Groups. <i>An Application of Groups to Anthropology.</i>	69
Chapter 8	Permutations of a Finite Set Decomposition of Permutations into Cycles. Transpositions. Even and Odd Permutations. Alternating Groups.	80
Chapter 9	Isomorphism The Concept of Isomorphism in Mathematics. Isomorphic and Nonisomorphic Groups. Cayley's Theorem. <i>Group Automorphisms.</i>	90
Chapter 10	Order of Group Elements Powers/Multiples of Group Elements. Laws of Exponents. Properties of the Order of Group Elements.	103
Chapter 11	Cyclic Groups Finite and Infinite Cyclic Groups. Isomorphism of Cyclic Groups. Subgroups of Cyclic Groups.	112
Chapter 12	Partitions and Equivalence Relations	119
Chapter 13	Counting Cosets Lagrange's Theorem and Elementary Consequences. <i>Survey of Groups of Order ≤ 10. Number of Conjugate Elements. Group Acting on a Set.</i>	126
Chapter 14	Homomorphisms Elementary Properties of Homomorphisms. Normal Subgroups. Kernel and Range. <i>Inner Direct Products. Conjugate Subgroups.</i>	136

Chapter 15	Quotient Groups	147
	Quotient Group Construction. Examples and Applications. <i>The Class Equation. Induction on the Order of a Group.</i>	
Chapter 16	The Fundamental Homomorphism Theorem	157
	Fundamental Homomorphism Theorem and Some Consequences. <i>The Isomorphism Theorems. The Correspondence Theorem. Cauchy's Theorem. Sylow Subgroups. Sylow's Theorem. Decomposition Theorem for Finite Abelian Groups.</i>	
Chapter 17	Rings: Definitions and Elementary Properties	169
	Commutative Rings. Unity. Invertibles and Zero-Divisors. Integral Domain. Field.	
Chapter 18	Ideals and Homomorphisms	181
Chapter 19	Quotient Rings	190
	Construction of Quotient Rings. Examples. Fundamental Homomorphism Theorem and Some Consequences. Properties of Prime and Maximal Ideals.	
Chapter 20	Integral Domains	200
	Characteristic of an Integral Domain. Properties of the Characteristic. Finite Fields. Construction of the Field of Quotients.	
Chapter 21	The Integers	208
	Ordered Integral Domains. Well-ordering. Characterization of \mathbb{Z} Up to Isomorphism. Mathematical Induction. Division Algorithm.	
Chapter 22	Factoring into Primes	217
	Ideals of \mathbb{Z} . Properties of the GCD. Relatively Prime Integers. Primes. Euclid's Lemma. Unique Factorization.	

Chapter 23	Elements of Number Theory (Optional)	226
	Properties of Congruence. Theorems of Fermat and Euler. Solutions of Linear Congruences. Chinese Remainder Theorem.	
	<i>Wilson's Theorem and Consequences. Quadratic Residues. The Legendre Symbol. Primitive Roots.</i>	
Chapter 24	Rings of Polynomials	240
	Motivation and Definitions. Domain of Polynomials over a Field. Division Algorithm.	
	<i>Polynomials in Several Variables. Fields of Polynomial Quotients.</i>	
Chapter 25	Factoring Polynomials	251
	Ideals of $F[x]$. Properties of the GCD. Irreducible Polynomials. Unique factorization.	
	<i>Euclidean Algorithm.</i>	
Chapter 26	Substitution in Polynomials	258
	Roots and Factors. Polynomial Functions. Polynomials over \mathbb{Q} . Eisenstein's Irreducibility Criterion. Polynomials over the Reals. Polynomial Interpolation.	
Chapter 27	Extensions of Fields	270
	Algebraic and Transcendental Elements. The Minimum Polynomial. Basic Theorem on Field Extensions.	
Chapter 28	Vector Spaces	282
	Elementary Properties of Vector Spaces. Linear Independence. Basis. Dimension. Linear Transformations.	
Chapter 29	Degrees of Field Extensions	292
	Simple and Iterated Extensions. Degree of an Iterated Extension.	
	<i>Fields of Algebraic Elements. Algebraic Numbers. Algebraic Closure.</i>	

Chapter 30	Ruler and Compass	301
	Constructible Points and Numbers. Impossible Constructions. <i>Constructible Angles and Polygons.</i>	
Chapter 31	Galois Theory: Preamble	311
	Multiple Roots. Root Field. Extension of a Field. Isomorphism. <i>Roots of Unity. Separable Polynomials. Normal Extensions.</i>	
Chapter 32	Galois Theory: The Heart of the Matter	323
	Field Automorphisms. The Galois Group. The Galois Correspondence. Fundamental Theorem of Galois Theory. <i>Computing Galois Groups.</i>	
Chapter 33	Solving Equations by Radicals	334
	Radical Extensions. Abelian Extensions. Solvable Groups. Insolvability of the Quintic.	
Appendix A	Review of Set Theory	345
Appendix B	Review of the Integers	349
Appendix C	Review of Mathematical Induction	
	Answers to Selected Exercises	353
	Index	381