

---

# CONTENTS\*

---

Chapter 16	The Fundamental Theorem of Symmetric Groups. Dihedral Groups. Fundamental Properties and Consequences.	157
Chapter 17	Permutations of a Finite Set. Cauchy's Theorem. Low Subgroups. Decomposition of Permutations into Cycles. Transpositions. Even and Odd Permutations. Alternating Groups.	180
Chapter 17	Rings: Definitions and Elementary Properties	90
	Preface	xi
Chapter 1	Why Abstract Algebra?	1
	History of Algebra. New Algebras. Algebraic Structures. Axioms and Axiomatic Algebra. Abstraction in Algebra.	
Chapter 2	Operations	19
	Operations on a Set. Properties of Operations.	
Chapter 3	The Definition of Groups	25
	Groups. Examples of Infinite and Finite Groups. Examples of Abelian and Nonabelian Groups. Group Tables.	
	<i>Theory of Coding: Maximum-Likelihood Decoding.</i>	
Chapter 4	Elementary Properties of Groups	36
	Uniqueness of Identity and Inverses. Properties of Inverses.	
	<i>Direct Product of Groups.</i>	
Chapter 5	Subgroups	44
	Definition of Subgroup. Generators and Defining Relations.	
	<i>Cayley Diagrams. Center of a Group. Group Codes; Hamming Code.</i>	

\* Italic headings indicate topics discussed in the exercise sections.

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

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

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

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

In an introductory chapter entitled *Why Abstract Algebra?*, as well as in numerous historical asides, concepts of abstract algebra are traced to the historic context in which they arose. I have attempted to show that they arose without artifice, as a natural response to particular needs, in the course of a natural process of evolution. Furthermore, I have endeavored to bring to light, explicitly, the intuitive content of the algebraic concepts used in this book. Concepts are more meaningful to students when the students are able to represent those concepts in their minds by clear and familiar mental images. Accordingly, the process of concrete concept-formation is developed with care throughout this book.

I have deliberately avoided a rigid conventional format, with its succession of *definition, theorem, proof, corollary, example*. In my experience, that kind of format encourages some students to believe that mathematical concepts have a merely conventional character, and may