ABSTRACT ALGEBRA

DUMMIT, FOOTE

Second Edition

My Own Notes + Exercises

J.B.

July 2025

Contents

Preliminaries 1
0.1 Basics 1
0.2 Properties of the Integers 4
0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n 4

I GROUP THEORY 5

Chapter 1 Introduction to Groups 7
1.1 Basic Axioms and Examples 7
1.2 Dihedral Groups 7
1.3 Symmetric Groups 7
1.4 Matrix Groups 7
1.5 The Quaternion Group 7
1.6 Homomorphisms and Isomorphisms 7
1.7 Group Actions 7

Chapter 2 Subgroups 9
2.1 Definition and Examples 9
2.2 Centralizers and Normalizers, Stabilizers and Kernels 9
2.3 Cyclic Groups and Cyclic Subgroups 9
2.4 Subgroups Generated by Subsets of a Group 9
2.5 The Lattice of Subgroups of a Group 9

Chapter 3 Quotient Groups and Homomorphisms 11
3.1 Definitions and Examples 11
3.2 More on Cosets and Lagrange's Theorem 11
3.3 The Isomorphism Theorems 11
3.4 Composition Series and the Hölder Program 11
3.5 Transpositions and the Alternating Group 11

Chapter 4 Group Actions 13
4.1 Group Actions and Permutation Representations 13
4.2 Groups Acting on Themselves by Left Multiplication—Cayley's Theorem 13
4.3 Groups Acting on Themselves by Conjugation—The Class Equation 13
4.4 Automorphisms 13
4.5 The Sylow Theorems 13
4.6 The Simplicity of A_n 13

Chapter 5 Direct and Semidirect Products and Abelian Groups 15
5.1 Direct Products 15
5.2 The Fundamental Theorem of Finitely Generated Abelian Groups 15
5.3 Table of Groups of Small Order 15
5.4 Recognizing Direct Products 15
5.5 Semidirect Products 15

Chapter 6 Further Topics in Group Theory 17
6.1 p-groups, Nilpotent Groups, and Solvable Groups 17
6.2 Applications in Groups of Medium Order 17
6.3 A Word on Free Groups 17

II RING THEORY 19

Chapter 7 Introduction to Rings 21
7.1 Basic Definitions and Examples 21
7.2 Examples: Polynomial Rings, Matrix Rings, and Group Rings 21
7.3 Ring Homomorphisms and Quotient Rings 21
7.4 Properties of Ideals 21
7.5 Rings of Fractions 21
7.6 The Chinese Remainder Theorem 21

Chapter 8 Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains 23
8.1 Euclidean Domains 23
8.2 Principal Ideal Domains (P.I.D.s) 23
8.3 Unique Factorization Domains (U.F.D.s) 23

Chapter 9 Polynomial Rings 25
9.1 Definitions and Basic Properties 25
9.2 Polynomial Rings over Fields I 25
9.3 Polynomial Rings that are Unique Factorization Domains 25
9.4 Irreducibility Criteria 25
9.5 Polynomial Rings over Fields II 25

III MODULES AND VECTOR SPACES 27

Chapter 10 Introduction to Module Theory 29
10.1 Basic Definitions and Examples 29
10.2 Quotient Modules and Module Homomorphisms 29
10.3 Generation of Modules, Direct Sums, and Free Modules 29
10.4 Tensor Products of Modules 29
10.5 Exact Sequences—Projective, Injective, and Flat Modules 29

Chapter 11 Vector Spaces 31
11.1 Definitions and Basic Theory 31
11.2 The Matrix of a Linear Transformation 31
11.3 Dual Vector Spaces 31

11.4 Determinants 31
11.5 Tensor Algebras, Symmetric and Exterior Algebras 31

Chapter 12 Modules over Principal Ideal Domains 33
12.1 The Basic Theory 33
12.2 The Rational Canonical Form 33
12.3 The Jordan Canonical Form 33

IV FIELD THEORY AND GALOIS THEORY 35

Chapter 13 Field Theory 37
13.1 Basic Theory of Field Extensions 37
13.2 Algebraic Extensions 37
13.3 Classical Straightedge and Compass Constructions 37
13.4 Splitting Fields and Algebraic Closures 37
13.5 Separable and Inseparable Extensions 37
13.6 Cyclotomic Polynomials and Extensions 37

Chapter 14 Galois Theory 39
14.1 Basic Definitions 39
14.2 The Fundamental Theorem of Galois Theory 39
14.3 Finite Fields 39
14.4 Composite Extensions and Simple Extensions 39
14.5 Cyclotomic Extensions and Abelian Extensions over $\mathbb{Q}$ 39
14.6 Galois Groups of Polynomials 39
14.7 Solvable and Radical Extensions: Insolvability of the Quintic 39
14.8 Computation of Galois Groups over $\mathbb{Q}$ 39
14.9 Transcendental Extensions, Inseparable Extensions, Infinite Galois Groups 39

V AN INTRODUCTION TO COMMUTATIVE RINGS, ALGEBRAIC GEOMETRY, AND HOMOLOGICAL ALGEBRA 41

Chapter 15 Commutative Rings and Algebraic Geometry 43
15.1 Noetherian Rings and Affine Algebraic Sets 43
15.2 Radicals and Affine Varieties 43
15.3 Integral Extensions and Hilbert's Nullstellensatz 43
15.4 Localization 43
15.5 The Prime Spectrum of a Ring 43

Chapter 16 Artinian Rings, Discrete Valuation Rings, and Dedekind Domains 45
16.1 Artinian Rings 45
16.2 Discrete Valuation Rings 45
16.3 Dedekind Domains 45

Chapter 17 Introduction to Homological Algebra and Group Cohomology 47
17.1 Introduction to Homological Algebra—Ext and Tor 47
17.2 The Cohomology of Groups 47
17.3 Crossed Homomorphisms and $H^1(G, A)$ 47

17.4 Group Extensions, Factor Sets, and $H^2(G, A)$ 47

VI INTRODUCTION TO THE REPRESENTATION THEORY OF FINITE GROUPS 49

Chapter 18 Representation Theory and Character Theory 51
18.1 Linear Actions and Modules over Group Rings 51
18.2 Wedderburn's Theorem and Some Consequences 51
18.3 Character Theory and the Orthogonality Relations 51

Chapter 19 Examples and Applications of Character Theory 53
19.1 Characters of Groups of Small Order 53
19.2 Theorems of Burnside and Hall 53
19.3 Introduction to the Theory of Induced Characters 53

Appendix I: Cartesian Products and Zorn's Lemma 55

Appendix II: Category Theory 57

Preliminaries

0.1 Basics

The set

$$f(A) = \{b \in B \mid b \in f(a), \text{ for some } a \in A\},$$

is a subset of B, called the *range* or *image* of f. For each subset C of B the set

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}$$

consisting of the elements of A mapping into C under f is called the *preimage* or *inverse image* of C under f. For each $b \in B$, the preimage of $\{b\}$ under f is called the *fiber* of f over b.

Let $f : A \to B$.

(1) f is *injective* or is an *injection* if whenever $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.

(2) f is *surjective* or is an *surjection* if for all $b \in B$ there is some $a \in A$ such that $f(a) = b$; i.e., the image of f is all of B. (The codomain of f is B, while the range/image of f is the subset $f(A) := \{b \in B : b = f(a), \text{ for some } a \in A\}$)

(3) f is *bijective* or is an *bijection* if it is both injective and surjective.

(4) f has a *left inverse* if there is a function $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on A; i.e., $(g \circ f)(a) = a$, for all $a \in A$.

(5) f has a *right inverse* if there is a function $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B; i.e., $(f \circ h)(b) = b$, for all $b \in B$.

Proposition 1. *Let $f : A \to B$.*

(1) The map f is injective iff f has a left inverse.

(2) The map f is surjective iff f has a right inverse.

(3) The map f is a bijection iff there exists $g : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A. (The map g is necessarily unique and we say g is the 2-sided inverse of f)

(4) If A and B are finite sets with the same number of elements ($|A| = |B|$), then $f : A \to B$ is bijective iff f is injective iff f is surjective.

Proof. (1) Suppose f is injective. Now, note that by definition of image of f, for all $c \in f(A)$, there exists $a \in A$ s.t. $c = f(a)$. Thus for all such c, we may define the function $g : f(A) \to A$ by $g(f(a)) = g(c) := a$. Note that g is well-defined as a function because each unique $c \in B$ corresponds to a unique $a \in A$ ($c_1 = f(a_1) = f(a_2) = c_2$ implies $g(c_1) = a_1 = a_2 = g(c_2)$). We may extend g to all of B arbitrarily. On the other hand, suppose f has a left inverse. Consider any $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$. Then $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$.

(2) Suppose f is surjective. Then for any $b \in B$, there exists some $a \in A$ such that $f(a) = b$. Thus it is well-defined to define the function $h : B \to A$ such that $h(b) = a$, and we have $f(h(b)) = f(a) = b$. On the other hand, suppose f has a right inverse. Consider any $b \in B$. Then $f(h(b)) = b$, with $a = h(b) \in A$

(3) Suppose f is a bijection. Then by (1) and (2), there exists a left inverse g and a right inverse h. Fix any $b \in B$. Then by surjectivity of f, there exists $a \in A$ such that $b = f(a)$. But then $g(b) = g(f(a)) = a = h(b)$, and $g \equiv h$ is the inverse of f.

(4) Bijective implies injective and surjective by definition. Now suppose f is injective. Suppose that for all $a \in A$ there does not exist $b \in B$ whence $f(a) = b$. But by the pidgeonhole principle there must be (distinct) $a_1 \neq a_2 \in A$ that map to the same element in B; i.e., $f(a_1) = f(a_2)$, and this is a contradiction to the injectivity. On the other hand suppose f is surjective. Suppose that there exists $a_1 \neq a_2 \in A$ but $f(a_1) = f(a_2)$. Again by the pidgeonhole principle there must be a $b \in B$ that is not mapped to, which is a contradiction. □

Let A be a nonempty set.

(1) A binary relation on a set A is a subset R of $A \times A$ and we write $a \sim b$ if $(a, b) \in R$.

(2) The relation $\sim$ on A is said to be:

- *(a) reflexive if $a \sim a$ for all $a \in A$,*
- *(b) symmetric if $a \sim b$ implies $b \sim a$ for all $a, b \in A$,*
- *(c) transitive if $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$.*

A relation is an equivalence relation if it is reflexive, symmetric, and transitive.

(3) If $\sim$ defines an equivalence relation on A, then the equivalence class of $a \in A$ is defined to be $\{x \in A \mid x \sim a\}$. Elements of the equivalence class of a are said to be equivalent to a. If C is an equivalence class, any element of C is called a representative of the class C.

(4) A partition of A is any collection $\{A_i \mid i \in I\}$ of nonempty subsets of A (I some indexing set) such that

- *(a) $A = \cup_{i \in I} A_i$, and*
- *(b) $A_i \cap A_j = \emptyset$, for all $i, j \in I$ with $i \neq j$.*

Preposition 2. *Let A be a nonempty set.*

(1) If $\sim$ defines an equivalence relation on A then the set of equivalence classes of $\sim$ form a partition of A.

(2) If $\{A_i \mid i \in I\}$ is a partition of A then there is an equivalence relation on A whose equivalence classes are precisely the sets $A_i, i \in I$.

EXERCISES

In exercises 1 to 4 let $\mathcal{A}$ be the set of 2×2 matrices with real number entries. Recall that matrix multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{pmatrix}.$$

Let

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let

$$\mathcal{B} := \{X \in \mathcal{A} \mid MX = XM\}.$$

1. Determine which of the following elements of $\mathcal{A}$ lie in $\mathcal{B}$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

   The first is trivially yes. The second is no:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

   The third is trivially yes. The fourth is no:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

   The fifth is yes (identity). The sixth is no:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

2. Prove that if $P, Q \in \mathcal{B}$, then $P + Q \in \mathcal{B}$.

$$(P+Q)M = PM + QM = MP + MQ = M(P+Q)$$

3. Prove that if $P, Q \in \mathcal{B}$, then $P \cdot Q \in \mathcal{B}$.

$$(PQ)M = P(QM) = P(MQ) = (PM)Q = (MP)Q = M(PQ)$$

4. Find conditions on p, q, r, s which determine precisely when $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathcal{B}$.

$$\begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix}$$

   Thus we have

$$\begin{cases} p = p + r \\ r = r \\ p + q = q + s \\ r + s = s \end{cases} \implies \begin{cases} 0 = r \\ p = s \end{cases}$$

5. Determine whether the following functions f are well-defined:

   (a) $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(a/b) = a$;
   Yes, because the rational numbers are defined to be $\{a/b : a, b \in \mathbb{Z}, b \neq 0\}$.

   (b) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$;
   Yes, because $a, b \in \mathbb{Z} \implies a^2, b^2 \in \mathbb{Z}$, and $b \neq 0 \implies b^2 \neq 0$.

6. Determine whether the function $f : \mathbb{R}^+ \to \mathbb{Z}$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well defined.

   False: see $0.0\overline{9} = 0.1$, but $0 = f(0.0\overline{9}) = f(0.1) = 1$, and f is not a function.

7. Let $f : A \to B$ be a surjective map of sets. Prove that the relation

$$a \sim b \iff f(a) = f(b)$$

   is an equivalence relation whose equivalence classes are the fibers of f.

   See that $f(a) = f(a)$, and $f(a) = f(b)$ implies $f(b) = f(a)$, and $f(a) = f(b)$ and $f(b) = f(c)$ implies $f(a) = f(b) = f(c)$. Also see that

$$f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\}.$$

0.2 Properties of the Integers

0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

Part I

GROUP THEORY

Chapter 1

Introduction to Groups

1.1 Basic Axioms and Examples

EXERCISES

1.2 Dihedral Groups

EXERCISES

1.3 Symmetric Groups

EXERCISES

1.4 Matrix Groups

EXERCISES

1.5 The Quaternion Group

EXERCISES

1.6 Homomorphisms and Isomorphisms

EXERCISES

1.7 Group Actions

EXERCISES

Chapter 2

Subgroups

2.1 Definition and Examples

EXERCISES

2.2 Centralizers and Normalizers, Stabilizers and Kernels

EXERCISES

2.3 Cyclic Groups and Cyclic Subgroups

EXERCISES

2.4 Subgroups Generated by Subsets of a Group

EXERCISES

2.5 The Lattice of Subgroups of a Group

EXERCISES

Chapter 3

Quotient Groups and Homomorphisms

3.1 Definitions and Examples

EXERCISES

3.2 More on Cosets and Lagrange's Theorem

EXERCISES

3.3 The Isomorphism Theorems

EXERCISES

3.4 Composition Series and the Hölder Program

EXERCISES

3.5 Transpositions and the Alternating Group

EXERCISES

Chapter 4

Group Actions

4.1 Group Actions and Permutation Representations

4.2 Groups Acting on Themselves by Left Multiplication—Cayley's Theorem

4.3 Groups Acting on Themselves by Conjugation—The Class Equation

4.4 Automorphisms

4.5 The Sylow Theorems

4.6 The Simplicity of A_n

Chapter 5

Direct and Semidirect Products and Abelian Groups

5.1 Direct Products

5.2 The Fundamental Theorem of Finitely Generated Abelian Groups

5.3 Table of Groups of Small Order

5.4 Recognizing Direct Products

5.5 Semidirect Products

Chapter 6

Further Topics in Group Theory

6.1 p-groups, Nilpotent Groups, and Solvable Groups

6.2 Applications in Groups of Medium Order

6.3 A Word on Free Groups

Part II

RING THEORY

Chapter 7

Introduction to Rings

7.1 Basic Definitions and Examples

7.2 Examples: Polynomial Rings, Matrix Rings, and Group Rings

7.3 Ring Homomorphisms and Quotient Rings

7.4 Properties of Ideals

7.5 Rings of Fractions

7.6 The Chinese Remainder Theorem

Chapter 8

Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

8.1 Euclidean Domains

8.2 Principal Ideal Domains (P.I.D.s)

8.3 Unique Factorization Domains (U.F.D.s)

Chapter 9

Polynomial Rings

9.1 Definitions and Basic Properties

9.2 Polynomial Rings over Fields I

9.3 Polynomial Rings that are Unique Factorization Domains

9.4 Irreducibility Criteria

9.5 Polynomial Rings over Fields II

Part III

MODULES AND VECTOR SPACES

Chapter 10

Introduction to Module Theory

10.1 Basic Definitions and Examples

10.2 Quotient Modules and Module Homomorphisms

10.3 Generation of Modules, Direct Sums, and Free Modules

10.4 Tensor Products of Modules

10.5 Exact Sequences—Projective, Injective, and Flat Modules

Chapter 11

Vector Spaces

11.1 Definitions and Basic Theory

11.2 The Matrix of a Linear Transformation

11.3 Dual Vector Spaces

11.4 Determinants

11.5 Tensor Algebras, Symmetric and Exterior Algebras

Chapter 12

Modules over Principal Ideal Domains

12.1 The Basic Theory

12.2 The Rational Canonical Form

12.3 The Jordan Canonical Form

Part IV

FIELD THEORY AND GALOIS THEORY

Chapter 13

Field Theory

13.1 Basic Theory of Field Extensions

13.2 Algebraic Extensions

13.3 Classical Straightedge and Compass Constructions

13.4 Splitting Fields and Algebraic Closures

13.5 Separable and Inseparable Extensions

13.6 Cyclotomic Polynomials and Extensions

Chapter 14

Galois Theory

14.1 Basic Definitions

14.2 The Fundamental Theorem of Galois Theory

14.3 Finite Fields

14.4 Composite Extensions and Simple Extensions

14.5 Cyclotomic Extensions and Abelian Extensions over $\mathbb{Q}$

14.6 Galois Groups of Polynomials

14.7 Solvable and Radical Extensions: Insolvability of the Quintic

14.8 Computation of Galois Groups over $\mathbb{Q}$

14.9 Transcendental Extensions, Inseparable Extensions, Infinite Galois Groups

Part V

AN INTRODUCTION TO COMMUTATIVE RINGS, ALGEBRAIC GEOMETRY, AND HOMOLOGICAL ALGEBRA

Chapter 15

Commutative Rings and Algebraic Geometry

15.1 Noetherian Rings and Affine Algebraic Sets

15.2 Radicals and Affine Varieties

15.3 Integral Extensions and Hilbert's Nullstellensatz

15.4 Localization

15.5 The Prime Spectrum of a Ring

Chapter 16

Artinian Rings, Discrete Valuation Rings, and Dedekind Domains

16.1 Artinian Rings

16.2 Discrete Valuation Rings

16.3 Dedekind Domains

Chapter 17

Introduction to Homological Algebra and Group Cohomology

17.1 Introduction to Homological Algebra—Ext and Tor

17.2 The Cohomology of Groups

17.3 Crossed Homomorphisms and $H^1(G, A)$

17.4 Group Extensions, Factor Sets, and $H^2(G, A)$

Part VI

INTRODUCTION TO THE REPRESENTATION THEORY OF FINITE GROUPS

Chapter 18

Representation Theory and Character Theory

18.1 Linear Actions and Modules over Group Rings

18.2 Wedderburn's Theorem and Some Consequences

18.3 Character Theory and the Orthogonality Relations

Chapter 19

Examples and Applications of Character Theory

19.1 Characters of Groups of Small Order

19.2 Theorems of Burnside and Hall

19.3 Introduction to the Theory of Induced Characters

Appendix I: Cartesian Products and Zorn's Lemma

Appendix II: Category Theory