ABSTRACT ALGEBRA

DUMMIT, FOOTE

Second Edition

My Own Notes + Exercises

J.B.

July 2025

Contents

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

(1) (Well Ordering of $\mathbb{Z}$) If A is any nonempty subset of $\mathbb{Z}^+$, there is some element $m \in A$ such that $m \leq a$, for all $a \in A$ (m is called a *minimal element* of A).

(2) If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say a *divides* b if there is an element $c \in \mathbb{Z}$ such that $b = ac$ (i.e., b/a is an integer). In this case we write $a \mid b$; if a does not divide b we write $a \nmid b$.

(3) If $a, b \in \mathbb{Z} \setminus \{0\}$, there is a unique positive integer d, called the *greatest common divisor* (gcd) of a and b, satisfying:

   (a) $d \mid a$ and $d \mid b$

   (b) if $e \mid a$ and $e \mid b$ then $e \mid d$.

   The gcd of a and b will be denoted (a, b). If $(a, b) = 1$, we say that a and b are *relatively prime*.

(4) If $a, b \in \mathbb{Z} \setminus \{0\}$, there is a unique positive integer l, called the *least common multiple* (lcm) of a and b, satisfying:

   (a) $a \mid l$ and $b \mid l$

   (b) if $a \mid m$ and $b \mid m$ then $l \mid m$.

   The connection between the gcd d and lcm l of any two such a, b is given by $dl = ab$.

(5) *The Division Algorithm*: if $a, b \in \mathbb{Z} \setminus \{0\}$, then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r, \quad 0 \leq r < |b|,$$

   where q is the *quotient* and r is the *remainder*.

(6) The *Euclidean Algorithm* is an important procedure which produces a greatest common divisor of two integers a and b by iterating the Division Algorithm: if $a, b \in \mathbb{Z} \setminus \{0\}$, then we obtain a sequence of quotients and remainders

$$\begin{aligned}
a &= q_0 b + r_0 && (0)\\
b &= q_1 r_0 + r_1 && (1)\\
r_0 &= q_2 r_1 + r_2 && (2)\\
r_1 &= q_3 r_2 + r_3 && (3)\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n && (n)\\
r_{n-1} &= q_{n+1} r_n \ (r_{n+1} = 0) && (n+1)
\end{aligned}$$

where r_n is the last nonzero remainder. Such an r_n exists since $|b| > |r_0| > |r_1| > \cdots > |r_n|$ is a decreasing sequence of strictly positive integers if the remainders are nonzero and such a sequence cannot continue indefinitely. Then r_n is the gcd (a, b) of a and b.

(7) One consequence of the Euclidean Algorithm: if $a, b \in \mathbb{Z} \setminus \{0\}$, then there exist $x, y \in \mathbb{Z}$ such that

$$(a, b) = ax + by.$$

(8) An element p of $\mathbb{Z}^+$ is called a *prime* if $p > 1$ and the only positive divisors of p are 1 and p. Elements of $\mathbb{Z}^+$ that are not prime are called *composite*.

(9) The *Fundamental Theorem of Arithmetic says*: if $n \in \mathbb{Z}_{>1}$, then n can be factored uniquely into the product of primes; i.e., there are distinct primes $p_1, p_2, \ldots, p_n$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}.$$

This factorization is unique. Suppose we have two positive integers a and b with the prime factorizations

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n},$$

and the p_i are unique and allow the $\alpha_i, \beta_i \geq 0$. Then the greatest common divisor of a and b is

$$(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \ldots p_n^{\min(\alpha_n,\beta_n)}.$$

Then similarly the least common multiple is obtained by taking each maximum instead of the minimum.

(10) The *Euler φ-function* is defined as follows: for $n \in \mathbb{Z}^+$, let $\varphi(n)$ be the number of positive integers $a \leq n$ with a relatively prime to n; i.e., $(a, n) = 1$. For primes p we have $\varphi(p) = p - 1$, and more generally for all $a \geq 1$ we have the formula

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1).$$

The function φ is *multiplicative* in the sense that

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{if } (a, b) = 1.$$

EXERCISES

1. For each of the following pairs of integers a and b, determine:
   - their greatest common divisor ($\gcd(a, b)$),
   - their least common multiple (lcm(a, b)),
   - and write their greatest common divisor in the form $ax + by$ for some integers x and y.

   (a) $a = 20, \quad b = 13$
   (b) $a = 69, \quad b = 372$
   (c) $a = 792, \quad b = 275$
   (d) $a = 11391, \quad b = 5673$
   (e) $a = 1761, \quad b = 1567$
   (f) $a = 507885, \quad b = 60808$

2. Prove that if the integer k divides the integers a and b, then k divides $as + bt$ for every pair of integers s and t.

3. Prove that if n is composite then there are integers a and b such that $n \mid ab$ but $n \nmid a$ and $n \nmid b$.

4. Let a, b, and N be fixed integers with a and b nonzero, and let $d = (a, b)$ be the greatest common divisor of a and b. Suppose x_0 and y_0 are particular solutions to $ax + by = N$ (i.e., $ax_0 + by_0 = N$). Prove that for any integer t, the integers
$$x = x_0 + \frac{b}{d}t \quad \text{and} \quad y = y_0 - \frac{a}{d}t$$
are also solutions to $ax + by = N$ (this is in fact the general solution).

5. Determine the value $\varphi(n)$ for each integer $n \leq 30$ where φ denotes the Euler φ function.

6. Prove the Well-Ordering Property of $\mathbb{Z}$ by induction and prove that the minimal element is unique.

7. If p is a prime, prove that there do not exist nonzero integers a and b such that $a^2 = pb^2$ (i.e., $\sqrt{p}$ is not a rational number).

8. Let p be a prime and $n \in \mathbb{Z}^+$. Find a formula for the largest power of p which divides $n! = n(n-1)(n-2) \cdots 2 \cdot 1$ (it involves the greatest integer function).

9. Write a computer program to determine the greatest common divisor (a, b) of two integers a and b and to express (a, b) in the form $ax + by$ for some integers x and y.

10. Prove that for any given positive integer N there exist only finitely many integers n with $\varphi(n) = N$ where φ denotes the Euler φ function. Conclude in particular that $\varphi(n)$ tends to infinity as n tends to infinity.

11. Prove that if d divides n then $\varphi(d)$ divides $\varphi(n)$ where φ denotes the Euler φ function.

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

abcdefg

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