Linear Algebra

Comprehensive Course Notes with Exercises

Undergraduate Level: 1st–2nd Year

For Mathematics and Engineering Students

Course Notes

February 2026

Contents

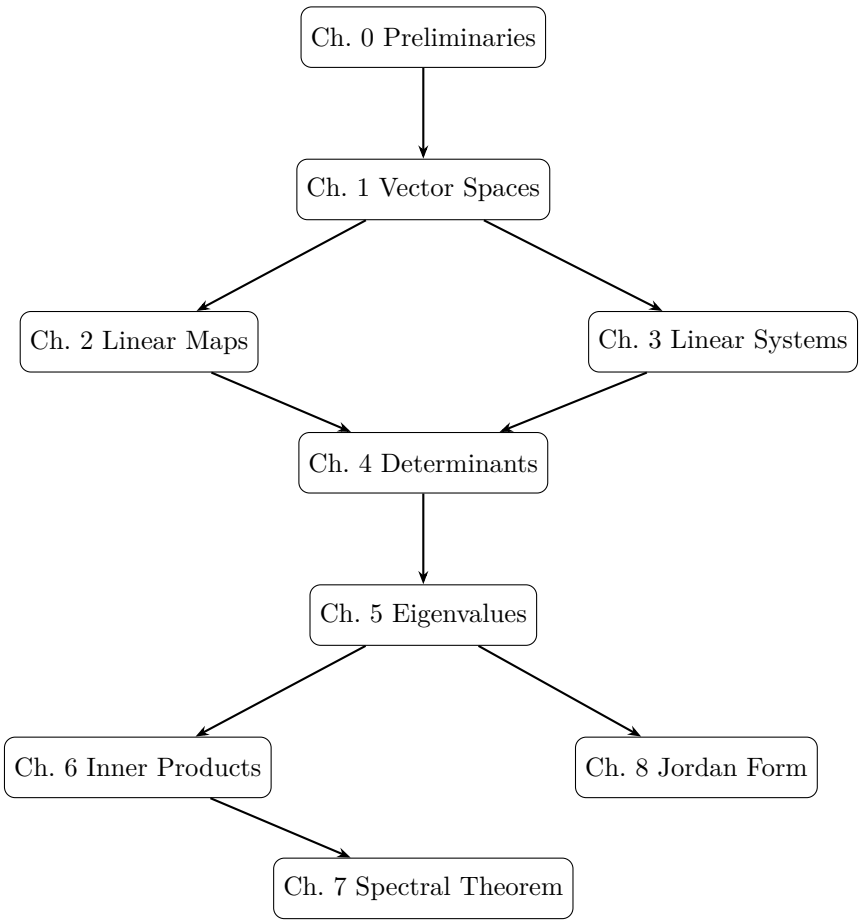
Preface

Linear algebra is one of the most fundamental and pervasive branches of modern mathematics. Its core concepts — vector spaces, linear maps, matrices, determinants, eigenvalues — form the foundation upon which vast areas of analysis, geometry, physics, computer science, and engineering are built.

These course notes are intended for first- and second-year undergraduate students in mathematics or engineering programs. They assume a solid background in high-school mathematics (calculus, functions, trigonometry) as well as elementary notions of set theory and logic.

Philosophy. We have striven to maintain a constant balance between *algebraic rigor* and *geometric intuition*. Every abstract concept is illustrated with concrete examples, figures, and applications. All proofs are complete: we believe that learning to read and write proofs is just as important as mastering computational techniques.

Organization. The notes consist of nine chapters, whose logical dependencies are shown below:



Chapter 0 (Preliminaries) may be skimmed quickly by students already familiar with the basic concepts. Chapter 8 (Jordan Normal Form) is an advanced chapter, intended for students

who wish to explore the subject in greater depth.

Exercises. Each chapter concludes with a set of exercises graded by difficulty:

- — basic exercises (direct verification of definitions),
- — intermediate exercises (applications of theorems),
- — challenging exercises (synthesis problems, open-ended questions).

Historical note. Linear algebra, as we know it today, developed gradually from the 18th to the 20th century. Major contributions include: Gauss's work on elimination (1809), Cauchy's theory of determinants (1815), the discovery of eigenvalues by Cauchy and Sylvester, Jordan's canonical forms (1870), and the axiomatic formalization of vector spaces by Peano (1888) and Banach (1920).

February 2026

Notation

We collect here the notation used throughout these notes. The reader is encouraged to refer back to this section as needed.

Symbol	Meaning
Number sets	
$\mathbb{N}$	Natural numbers $\{0, 1, 2, ...\}$
$\mathbb{Z}$	Integers
$\mathbb{Q}$	Rational numbers
$\mathbb{R}$	Real numbers
$\mathbb{C}$	Complex numbers
$\mathbb{K}$	Base field (usually $\mathbb{R}$ or $\mathbb{C}$)
$\mathbb{F}_p$	Finite field with p elements
Spaces and structures	
$\mathbb{K}^n$	Space of n-tuples over $\mathbb{K}$
$\mathcal{M}_{n,p}(\mathbb{K})$	Space of $n \times p$ matrices with entries in $\mathbb{K}$
$\mathcal{M}_n(\mathbb{K})$	Square matrices of size $n \times n$
$\mathrm{GL}_n(\mathbb{K})$	General linear group (invertible matrices)
$\mathcal{P}_n(\mathbb{K})$	Space of polynomials of degree $\leq n$
$\mathcal{L}(E, F)$	Space of linear maps from E to F
$\mathrm{End}(E)$	Endomorphisms of E $(= \mathcal{L}(E, E))$
Linear maps and matrices	
$\mathrm{Ker}\, f$	Kernel of f
$\mathrm{Im}\, f$	Image (range) of f
$\mathrm{rank}(f)$, $\mathrm{rank}(A)$	Rank of a linear map or matrix
Id, I_n	Identity map, $n \times n$ identity matrix
A^T	Transpose of A
A^*	Conjugate transpose (adjoint) of A
A^{-1}	Inverse of A
$\mathrm{tr}(A)$	Trace of A
$\det(A)$	Determinant of A
Vector spaces	
$\mathrm{Span}(v_1, \dots, v_k)$	Subspace spanned by $v_1, \dots, v_k$
$\dim E$	Dimension of E
$\mathrm{codim}\, F$	Codimension of F in E
$E \oplus F$	Direct sum
E/F	Quotient space
E^*	Dual of E

Symbol	Meaning
$\mathcal{B} = (e_1, \dots, e_n)$	Basis of E
Inner products and norms	
$\langle u, v \rangle$	Inner product of u and v
$\|v\|$	Norm of v
$u \perp v$	u and v are orthogonal
$F^\perp$	Orthogonal complement of F
Eigenvalues	
$\mathrm{Spec}(f)$	Spectrum of f (set of eigenvalues)
E_λ	Eigenspace associated with λ
$\chi_f(\lambda)$	Characteristic polynomial of f
$\mu_f(\lambda)$	Minimal polynomial of f
Miscellaneous	
$:=$	Equality by definition
δ_{ij}	Kronecker delta
$\mathrm{sgn}(\sigma)$	Sign of a permutation σ
$\mathfrak{S}_n$	Symmetric group on $\{1, \dots, n\}$

Chapter 1

Preliminaries

Linear algebra does not exist in a vacuum. It rests upon a small but essential toolkit from set theory, logic, and abstract algebra. The purpose of this chapter is to establish that toolkit clearly and concisely so that the rest of the course may proceed without interruption.

Most of the material here should be familiar from earlier courses. We therefore adopt a brisk pace: definitions are stated precisely, key examples are worked through, and proofs are included only when they illuminate a technique that will recur later. The reader who is comfortable with all five sections may safely skip ahead to Chapter 2; the reader who is not should work through the exercises at the end before continuing.

1.1 Sets

Definition 1 (Set)

A *set* is a collection of distinct objects, called its *elements*. We write $x \in A$ to mean that x is an element of A, and $x \notin A$ otherwise.

We recall the standard number sets that will pervade every chapter:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Here $\mathbb{N} = \{0, 1, 2, \ldots\}$ includes zero by convention.

Definition 2 (Subset and set equality)

Let A and B be sets.

(i) A is a *subset* of B, written $A \subseteq B$, if every element of A belongs to B.

(ii) $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

(iii) A is a *proper subset* of B, written $A \subsetneq B$, if $A \subseteq B$ and $A \neq B$.

Definition 3 (Set operations)

Let A and B be subsets of a universal set U.

(i) **Union:** $A \cup B := \{\, x \in U \mid x \in A \text{ or } x \in B \,\}$.

(ii) **Intersection:** $A \cap B := \{\, x \in U \mid x \in A \text{ and } x \in B \,\}$.

(iii) **Difference:** $A \setminus B := \{\, x \in U \mid x \in A \text{ and } x \notin B \,\}$.

(iv) **Complement:** $A^c := U \setminus A$.

(v) **Cartesian product:** $A \times B := \{\, (a,b) \mid a \in A,\ b \in B \,\}$.

(vi) **Power set:** $\mathcal{P}(A) := \{\, S \mid S \subseteq A \,\}$.

Example 4 (Cartesian products)

$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the Euclidean plane. More generally, $\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n}$ is the set of all n-tuples of real numbers, the primary setting for Chapters 1–3.

1.2 Mappings (functions)

Definition 5 (Mapping)

A *mapping* (or *function*) from a set A to a set B is a rule $f\colon A \to B$ that assigns to each element $a \in A$ exactly one element $f(a) \in B$. The set A is the *domain* and B is the *codomain*.

Definition 6 (Image and preimage)

Let $f\colon A \to B$ be a mapping.

(i) The *image* of a subset $S \subseteq A$ is $f(S) := \{\, f(a) \mid a \in S \,\}$.

(ii) The *image* (or *range*) of f is $\operatorname{Im} f := f(A)$.

(iii) The *preimage* of a subset $T \subseteq B$ is $f^{-1}(T) := \{\, a \in A \mid f(a) \in T \,\}$.

Definition 7 (Injectivity, surjectivity, bijectivity)

Let $f\colon A \to B$.

(i) f is *injective* (one-to-one) if $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

(ii) f is *surjective* (onto) if $\operatorname{Im} f = B$, i.e. for every $b \in B$ there exists $a \in A$ with $f(a) = b$.

(iii) f is *bijective* if it is both injective and surjective. In this case f has an *inverse* $f^{-1}\colon B \to A$ satisfying $f^{-1} \circ f = \mathrm{Id}_A$ and $f \circ f^{-1} = \mathrm{Id}_B$.

Example 8 (A classical injection and surjection)

(a) The map $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, is neither injective (since $f(-1) = f(1) = 1$) nor surjective (since $-1 \notin \operatorname{Im} f$).

(b) Restricting the domain and codomain: the map $g\colon [0,\infty) \to [0,\infty)$, $g(x) = x^2$, is bijective, with inverse $g^{-1}(y) = \sqrt{y}$.

Definition 9 (Composition)

If $f\colon A \to B$ and $g\colon B \to C$, their *composition* is the mapping $g \circ f\colon A \to C$ defined by $(g \circ f)(a) := g(f(a))$. Composition is associative: $h \circ (g \circ f) = (h \circ g) \circ f$.

Proposition 10 (Composition preserves injectivity and surjectivity)

Let $f\colon A \to B$ and $g\colon B \to C$.

(i) If f and g are injective, then $g \circ f$ is injective.

(ii) If f and g are surjective, then $g \circ f$ is surjective.

(iii) If $g \circ f$ is injective, then f is injective.

(iv) If $g \circ f$ is surjective, then g is surjective.

Proof. We prove (i); the others are similar exercises (see Exercise 42).

Suppose f and g are injective and $(g \circ f)(a_1) = (g \circ f)(a_2)$. Then $g(f(a_1)) = g(f(a_2))$. Since g is injective, $f(a_1) = f(a_2)$. Since f is injective, $a_1 = a_2$. □

1.3 Relations

Definition 11 (Binary relation)

A *binary relation* on a set A is a subset $\mathcal{R} \subseteq A \times A$. We write $a \mathcal{R} b$ to mean $(a, b) \in \mathcal{R}$.

1.3.1 Equivalence relations

Definition 12 (Equivalence relation)

A binary relation $\sim$ on A is an *equivalence relation* if it is:

(i) **Reflexive:** $a \sim a$ for all $a \in A$.

(ii) **Symmetric:** $a \sim b$ implies $b \sim a$.

(iii) **Transitive:** $a \sim b$ and $b \sim c$ imply $a \sim c$.

Definition 13 (Equivalence class and quotient set)

Let $\sim$ be an equivalence relation on A. The *equivalence class* of $a \in A$ is

$$[a] := \{\, b \in A \mid b \sim a \,\}.$$

The *quotient set* is $A/\!\sim \;:= \{\, [a] \mid a \in A \,\}$.

Example 14 (Congruence modulo n)

Fix an integer $n \geq 1$. On $\mathbb{Z}$, define $a \sim b$ if and only if $n \mid (a - b)$ (i.e. $a \equiv b \pmod{n}$). This is an equivalence relation with n equivalence classes: $[0], [1], \ldots, [n-1]$. The quotient set is denoted $\mathbb{Z}/n\mathbb{Z}$ (or simply $\mathbb{Z}_n$).

For $n = 3$: $[0] = \{\dots, -6, -3, 0, 3, 6, \dots\}$, $[1] = \{\dots, -5, -2, 1, 4, 7, \dots\}$, $[2] = \{\dots, -4, -1, 2, 5, 8, \dots\}$.

Remark 15 (Equivalence classes partition the set)

The equivalence classes of any equivalence relation on A form a *partition* of A: they are nonempty, pairwise disjoint, and their union is A. Conversely, every partition of A defines an equivalence relation. This fundamental observation will reappear when we study quotient vector spaces in Chapter 3.

1.3.2 Order relations

Definition 16 (Partial order)

A binary relation $\leq$ on A is a *partial order* if it is:

(i) **Reflexive:** $a \leq a$ for all $a \in A$.

(ii) **Antisymmetric:** $a \leq b$ and $b \leq a$ imply $a = b$.

(iii) **Transitive:** $a \leq b$ and $b \leq c$ imply $a \leq c$.

If in addition every two elements are comparable ($a \leq b$ or $b \leq a$ for all $a, b \in A$), then $\leq$ is a *total order*.

Example 17 (Orders on familiar sets)

(a) $(\mathbb{R}, \leq)$ is totally ordered.

(b) $(\mathcal{P}(S), \subseteq)$ is partially ordered for any set S, but not totally ordered when $|S| \geq 2$ (e.g. $\{1\}$ and $\{2\}$ are incomparable in $\mathcal{P}(\{1, 2\})$).

(c) Divisibility on $\mathbb{N}^*$: $a \mid b$ defines a partial order.

1.4 Algebraic structures

In this section we introduce the hierarchy *group* $\to$ *ring* $\to$ *field*. The central notion for this course is that of a *field*, since linear algebra is the study of vector spaces *over a field*. However, groups and rings appear naturally in the theory (symmetry groups, polynomial rings, matrix rings), so a brief treatment is warranted.

1.4.1 Groups

Definition 18 (Group)

A *group* is a pair $(G, \star)$ where G is a nonempty set and $\star \colon G \times G \to G$ is a binary operation satisfying:

G1. Associativity: $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$.

G2. Identity: there exists $e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$.

G3. Inverses: for each $a \in G$ there exists $a' \in G$ such that $a \star a' = a' \star a = e$.

If in addition $a \star b = b \star a$ for all $a, b \in G$, the group is called *abelian* (or *commutative*).

Example 19 (Basic examples of groups)

(a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are abelian groups with identity 0 and inverse $-a$.

(b) $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ are abelian groups with identity 1 and inverse $1/a$. (Here $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, etc.)

(c) $(\mathrm{GL}_n(\mathbb{R}), \times)$, the set of invertible $n \times n$ real matrices under matrix multiplication, is a group (non-abelian for $n \geq 2$). This group will play a central role starting from Chapter 5.

(d) $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group of order n.

Proposition 20 (Uniqueness of identity and inverses)

In any group $(G, \star)$:

(i) The identity element is unique.

(ii) Each element has a unique inverse.

Proof. (i) Suppose e and e' are both identities. Then $e = e \star e' = e'$.

(ii) Suppose a' and a'' are both inverses of a. Then $a' = a' \star e = a' \star (a \star a'') = (a' \star a) \star a'' = e \star a'' = a''$. □

1.4.2 Rings

Definition 21 (Ring)

A *ring* is a triple $(R, +, \cdot)$ where:

R1. $(R, +)$ is an abelian group (with identity 0_R).

R2. Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

R3. There exists a multiplicative identity 1_R with $1_R \cdot a = a \cdot 1_R = a$ for all a.

R4. Distributivity: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

If $a \cdot b = b \cdot a$ for all $a, b \in R$, the ring is *commutative*.

Example 22 (Rings)

(a) $(\mathbb{Z}, +, \times)$ is a commutative ring.

(b) The polynomial ring $\mathbb{R}[X]$ is a commutative ring.

(c) $(\mathcal{M}_n(\mathbb{R}), +, \times)$, the set of $n \times n$ real matrices, is a ring that is *not* commutative for $n \geq 2$.

(d) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ is a commutative ring.

1.4.3 Fields

The field axioms are the single most important algebraic prerequisite for this course. A field is, roughly speaking, a set where one can add, subtract, multiply, and divide (except by zero) and where all the usual algebraic rules hold.

Definition 23 (Field)

A *field* is a triple $(\mathbb{K}, +, \cdot)$ satisfying the following axioms. Let a, b, c denote arbitrary elements of $\mathbb{K}$.

Addition axioms:

A1. Closure: $a + b \in \mathbb{K}$.

A2. Associativity: $(a + b) + c = a + (b + c)$.

A3. Commutativity: $a + b = b + a$.

A4. Identity: there exists $0 \in \mathbb{K}$ with $a + 0 = a$.

A5. Inverses: for each a there exists $-a \in \mathbb{K}$ with $a + (-a) = 0$.

Multiplication axioms:

M1. Closure: $a \cdot b \in \mathbb{K}$.

M2. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

M3. Commutativity: $a \cdot b = b \cdot a$.

M4. Identity: there exists $1 \in \mathbb{K}$, $1 \neq 0$, with $a \cdot 1 = a$.

M5. Inverses: for each $a \neq 0$ there exists $a^{-1} \in \mathbb{K}$ with $a \cdot a^{-1} = 1$.

Distributive law:

D1. $a \cdot (b + c) = a \cdot b + a \cdot c$.

Remark 24 (Field = commutative division ring)

Equivalently, a field is a commutative ring in which every nonzero element has a multiplicative inverse. The requirement $1 \neq 0$ ensures that the field has at least two elements.

Proposition 25 (Elementary consequences of the field axioms)

Let $\mathbb{K}$ be a field and $a, b \in \mathbb{K}$. Then:

(i) $a \cdot 0 = 0$.

(ii) $(-1) \cdot a = -a$.

(iii) $a \cdot b = 0$ implies $a = 0$ or $b = 0$ (a field has no zero divisors).

Proof. (i) $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Adding $-(a \cdot 0)$ to both sides gives $0 = a \cdot 0$.

(ii) $a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0$, so $(-1) \cdot a$ is the additive inverse of a.

(iii) If $a \neq 0$, multiply both sides of $ab = 0$ by a^{-1}: $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$. □

We now examine the three families of fields that appear most frequently in linear algebra.

Example 26 (The real numbers $\mathbb{R}$)

$(\mathbb{R}, +, \times)$ is the prototypical field, and the default setting for most of undergraduate linear algebra. In addition to the field axioms, $\mathbb{R}$ carries a total order compatible with the field operations and satisfies the *completeness axiom* (every nonempty bounded-above subset has a least upper bound). These extra properties are not required by the field axioms and are not shared by all fields.

Example 27 (The complex numbers $\mathbb{C}$)

Define $\mathbb{C} := \{\, a + bi \mid a, b \in \mathbb{R} \,\}$ where $i^2 = -1$. Addition and multiplication are given by:

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

The additive identity is 0, the multiplicative identity is 1, and the inverse of $a + bi \neq 0$ is

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\, i.$$

A key advantage of $\mathbb{C}$ over $\mathbb{R}$ is that every polynomial of degree $n \geq 1$ has exactly n roots (counted with multiplicity) — this is the *Fundamental Theorem of Algebra*. As a consequence, eigenvalue theory is cleaner over $\mathbb{C}$, as we shall see in Chapters 6 and 8.

Example 28 (Finite fields $\mathbb{F}_p$)

Let p be a prime number. On $\mathbb{Z}/p\mathbb{Z} = \{[0], [1], \ldots, [p-1]\}$, define addition and multiplication by:

$$[a] + [b] := [a + b], \qquad [a] \cdot [b] := [a \cdot b],$$

where the operations on the right are performed in $\mathbb{Z}$ and the result is reduced modulo p. These operations are well-defined (independent of the choice of representatives) and make $\mathbb{Z}/p\mathbb{Z}$ into a field, denoted $\mathbb{F}_p$.
The key point is that p being prime guarantees the existence of multiplicative inverses: if $[a] \neq [0]$, then $\gcd(a, p) = 1$, so by Bézout's identity there exist $u, v \in \mathbb{Z}$ with $au + pv = 1$, and hence $[a] \cdot [u] = [1]$.

Multiplication table of $\mathbb{F}_5$:

$\times$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

From the table we read off: $[2]^{-1} = [3]$, $[3]^{-1} = [2]$, $[4]^{-1} = [4]$.

Remark 29 (Why primality matters)

If n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is *not* a field. For instance, in $\mathbb{Z}/6\mathbb{Z}$ we have $[2]\cdot[3]=[0]$ with $[2]\neq[0]$ and $[3]\neq[0]$, violating the no-zero-divisors property. More generally, finite fields of order q exist if and only if q is a prime power p^k; the construction for $k\geq 2$ requires quotient rings of polynomial rings and is beyond our scope.

Definition 30 (Characteristic of a field)

The *characteristic* of a field $\mathbb{K}$, denoted $\operatorname{char}(\mathbb{K})$, is the smallest positive integer p such that $\underbrace{1+1+\cdots+1}_{p}=0$ in $\mathbb{K}$. If no such integer exists, we set $\operatorname{char}(\mathbb{K})=0$.

Example 31 (Characteristics)

$\operatorname{char}(\mathbb{Q})=\operatorname{char}(\mathbb{R})=\operatorname{char}(\mathbb{C})=0$, while $\operatorname{char}(\mathbb{F}_p)=p$. Throughout this course, *unless otherwise stated, $\mathbb{K}$ denotes a field of characteristic zero* (typically $\mathbb{R}$ or $\mathbb{C}$).

Remark 32 (Convention: the symbol $\mathbb{K}$)

In these notes, the letter $\mathbb{K}$ always denotes the base field. Most results in Chapters 1–5 hold over an arbitrary field; we shall explicitly note when additional hypotheses on $\mathbb{K}$ (such as $\operatorname{char}(\mathbb{K})=0$, or algebraic closure) are needed.

1.5 Proof techniques

Proofs are the backbone of mathematics. In this section we review the principal strategies. The reader should view these not as abstract logical rules but as practical tools that will be used repeatedly throughout the course.

1.5.1 Direct proof

To prove "if P then Q", assume P is true and deduce Q through a chain of logical steps.

Example 33 (A direct proof)

Claim: If n is an even integer, then n^2 is even.
Proof: Assume n is even. Then $n=2k$ for some $k\in\mathbb{Z}$. Hence $n^2=4k^2=2(2k^2)$, which is even. □

1.5.2 Proof by contrapositive

The statement "if P then Q" is logically equivalent to "if $\neg Q$ then $\neg P$". Sometimes the contrapositive is easier to prove.

Example 34 (A contrapositive proof)

Claim: If n^2 is odd, then n is odd.
Proof (contrapositive): We prove: if n is even, then n^2 is even. This is exactly the statement proved in Example 33. □

1.5.3 Proof by contradiction

To prove a statement P, assume $\neg P$ and derive a logical contradiction.

Example 35 (Irrationality of $\sqrt{2}$)

Claim: $\sqrt{2} \notin \mathbb{Q}$.
Proof: Suppose for contradiction that $\sqrt{2} = a/b$ with $a, b \in \mathbb{Z}$, $b \neq 0$, and $\gcd(a, b) = 1$. Then $2b^2 = a^2$, so a^2 is even, hence a is even: $a = 2k$. Then $2b^2 = 4k^2$, so $b^2 = 2k^2$, hence b is even. But then $\gcd(a, b) \geq 2$, contradicting $\gcd(a, b) = 1$. □

1.5.4 Proof by induction

Definition 36 (Principle of mathematical induction)

Let $P(n)$ be a statement depending on $n \in \mathbb{N}$. If

(i) **Base case:** $P(n_0)$ is true for some $n_0 \in \mathbb{N}$, and

(ii) **Inductive step:** for every $n \geq n_0$, $P(n)$ implies $P(n+1)$,

then $P(n)$ is true for all $n \geq n_0$.

Remark 37 (Strong induction)

In the *strong* form of induction, the inductive hypothesis in step (ii) is strengthened: one assumes $P(k)$ for all $n_0 \leq k \leq n$ and deduces $P(n+1)$. The two forms are logically equivalent.

Example 38 (Sum of the first n integers)

Claim: For all $n \geq 1$, $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof by induction.

Base case ($n = 1$): $\displaystyle\sum_{k=1}^{1} k = 1 = \frac{1 \cdot 2}{2}$.

Inductive step: Assume the formula holds for some $n \geq 1$. Then

$$\sum_{k=1}^{n+1} k = \left(\sum_{k=1}^{n} k\right) + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

This is the formula with n replaced by $n+1$. □

Example 39 (A preview: dimension of a subspace)

Induction is the primary tool for proving results about finite-dimensional vector spaces. For instance, one proves by induction on $\dim V$ that every subspace of a finite-dimensional vector space is itself finite-dimensional (see Chapter 2). The base case is $\dim V = 0$ (the trivial space), and the inductive step reduces a space of dimension $n+1$ to one of dimension n.

1.5.5 Proof by double inclusion

To show that two sets A and B are equal, one proves $A \subseteq B$ and $B \subseteq A$ separately. This technique is used constantly in linear algebra (e.g. showing that $\operatorname{Ker} f = \{\mathbf{0}\}$).

1.5.6 Proof by double counting / dimension argument

Later in the course, a powerful and characteristically linear-algebraic proof technique will emerge: the *dimension argument*. To show that two subspaces U and W are equal, one often shows $U \subseteq W$ (or $W \subseteq U$) and $\dim U = \dim W$. This will be formalized in Chapter 2.

1.6 Exercises

Exercise 40 (Set operations)

Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{3, 4, 5, 6, 7\}$. Compute $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, and $A \times \{0, 1\}$.

Exercise 41 (Injectivity and surjectivity)

For each of the following mappings, determine whether it is injective, surjective, bijective, or none.

(a) $f \colon \mathbb{Z} \to \mathbb{Z}$, $f(n) = 2n$.

(b) $g \colon \mathbb{Z} \to \mathbb{Z}$, $g(n) = n + 3$.

(c) $h \colon \mathbb{R} \to \mathbb{R}$, $h(x) = x^3 - x$.

(d) $\varphi \colon \mathbb{R} \to \mathbb{R}_{>0}$, $\varphi(x) = e^x$.

Exercise 42 (Composition and invertibility)

Prove parts (ii)–(iv) of Proposition 10.

Exercise 43 (Equivalence relations)

On $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, define $(a, b) \sim (c, d)$ if and only if $ad = bc$. Verify that $\sim$ is an equivalence relation. What familiar set does the quotient $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\!\sim$ represent?

Exercise 44 (Verifying group axioms)

Verify that $(\mathbb{Z}/5\mathbb{Z} \setminus \{[0]\}, \times)$ is an abelian group. What is the inverse of $[3]$?

Exercise 45 (Why $\mathbb{Z}$ is not a field)

Which field axiom fails for $(\mathbb{Z}, +, \times)$? Give a specific counterexample.

Exercise 46 (Arithmetic in $\mathbb{F}_7$)

(a) Write out the complete multiplication table of $\mathbb{F}_7$.

(b) Find $[3]^{-1}$, $[5]^{-1}$, and $[6]^{-1}$ in $\mathbb{F}_7$.

(c) Solve the equation $[3]x + [2] = [5]$ in $\mathbb{F}_7$.

Exercise 47 (Complex arithmetic)

Let $z = 3 + 4i$ and $w = 1 - 2i$. Compute $z + w$, zw, $|z|$, z^{-1}, and z/w.

Exercise 48 (Field of four elements)

We know $\mathbb{F}_p$ exists for every prime p. A field of order 4 also exists, but it is *not* $\mathbb{Z}/4\mathbb{Z}$ (which has zero divisors). Consider the set $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$ with the rule $\alpha^2+\alpha+1 = 0$ (i.e. $\alpha^2 = \alpha + 1$) and characteristic 2 (so $1 + 1 = 0$, and $x = -x$ for all x).

(a) Write out the complete addition and multiplication tables for $\mathbb{F}_4$.

(b) Verify that $\mathbb{F}_4$ is indeed a field.

Exercise 49 (Induction: sum of squares)

Prove by induction that for all $n \geq 1$:

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Exercise 50 (Induction: divisibility)

Prove by induction that $3^{2n} - 1$ is divisible by 8 for all $n \geq 1$.

Exercise 51 (Proof strategies)

Prove each of the following statements using the most appropriate proof technique. State which technique you use.

(a) If $a, b \in \mathbb{R}$ and $a + b$ is irrational, then at least one of a, b is irrational.

(b) For every $n \in \mathbb{N}$, $n^2 + n$ is even.

(c) There is no smallest positive rational number.

(d) For all $n \geq 1$, $\displaystyle\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$.

Chapter summary

- A **set** is a collection of distinct objects. The standard operations are union, intersection, difference, and Cartesian product. The number sets $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ form the foundation for all that follows.

- A **mapping** $f\colon A \to B$ assigns to each element of A exactly one element of B. The fundamental classification is into injective, surjective, and bijective maps.
- An **equivalence relation** partitions a set into equivalence classes. An **order relation** provides a way to compare elements.
- A **group** $(G, \star)$ captures the idea of a reversible operation. A **ring** $(R, +, \cdot)$ has two compatible operations. A **field** $(\mathbb{K}, +, \cdot)$ is a commutative ring in which every nonzero element has a multiplicative inverse.
- The principal fields in this course are $\mathbb{R}$ (the reals), $\mathbb{C}$ (the complex numbers), and $\mathbb{F}_p$ (finite fields of prime order).
- The main proof techniques are: direct proof, contrapositive, contradiction, mathematical induction, and double inclusion. Mastering these is essential for the remainder of the course.

Chapter 2

Vector Spaces and Subspaces

The concept of a *vector space* is the central object of linear algebra. It abstracts the familiar geometry of arrows in the plane and in space into a framework that encompasses polynomials, matrices, functions, and solutions of differential equations — all governed by the same structural rules.

In the previous chapter we established the notion of a field $\mathbb{K}$. A vector space is, in essence, a set whose elements (called *vectors*) can be added together and scaled by elements of $\mathbb{K}$, subject to axioms that generalize the intuitive properties of $\mathbb{R}^2$ and $\mathbb{R}^3$.

Why abstract? The reader may wonder why we bother with axioms when we could simply work in $\mathbb{R}^n$. The answer is twofold. First, many naturally occurring mathematical objects—polynomial spaces, function spaces, solution sets of linear systems—share the same algebraic structure as $\mathbb{R}^n$, and it is both economical and illuminating to develop the theory once, in the abstract, rather than repeat arguments for each concrete example. Second, the abstract framework reveals *which properties matter*: the dimension of a space, for instance, is a far more fundamental invariant than the specific nature of its elements.

We begin with the motivating example of $\mathbb{R}^2$ and $\mathbb{R}^3$, then give the full axiomatic definition and a rich collection of examples. The bulk of the chapter develops the core structural theory: subspaces, linear combinations, linear independence, bases, and dimension, culminating in the Grassmann formula.

Throughout this chapter, $\mathbb{K}$ denotes a field (typically $\mathbb{R}$ or $\mathbb{C}$).

2.1 Geometric motivation

Before plunging into axioms, let us recall the geometric picture that motivates the entire theory.

In the Euclidean plane $\mathbb{R}^2$, a vector $\mathbf{v} = (v_1, v_2)$ can be visualized as an arrow from the origin to the point (v_1, v_2). Two fundamental operations are available:

- **Addition:** $(v_1, v_2) + (w_1, w_2) = (v_1 + w_1, v_2 + w_2)$, which corresponds to the parallelogram rule.
- **Scalar multiplication:** $\lambda(v_1, v_2) = (\lambda v_1, \lambda v_2)$, which stretches or compresses the arrow (and reverses it if $\lambda < 0$).

These operations satisfy many natural properties: addition is commutative and associative, there is a zero vector $(0, 0)$, every vector has an additive inverse, scalar multiplication distributes over addition, and so on. The exact list of these properties constitutes the axioms of a vector space.

The same picture extends to $\mathbb{R}^3$, where vectors are triples (v_1, v_2, v_3) and the operations are defined componentwise. But what about $\mathbb{R}^n$ for $n \geq 4$, where geometric visualization fails? And

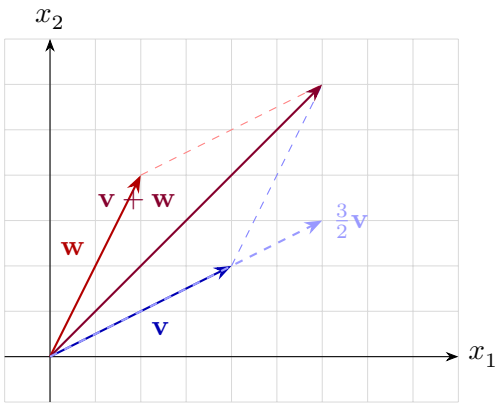


Figure 2.1: Vector addition (parallelogram rule) and scalar multiplication in $\mathbb{R}^2$.

what about objects like polynomials or matrices, which can also be added and scaled? The axioms of a vector space capture exactly the common structure.

2.2 Definition of a vector space

Definition 1 (Vector space)

A *vector space over* $\mathbb{K}$ (or $\mathbb{K}$*-vector space*) is a set E equipped with two operations:

- **Addition:** a map $+\colon E \times E \to E$, $(u, v) \mapsto u + v$.
- **Scalar multiplication:** a map $\cdot\colon \mathbb{K} \times E \to E$, $(\lambda, v) \mapsto \lambda \cdot v$ (usually written λv).

These operations satisfy the following axioms for all $u, v, w \in E$ and all $\lambda, \mu \in \mathbb{K}$:

Addition axioms:

(V1) Associativity: $(u + v) + w = u + (v + w)$.

(V2) Commutativity: $u + v = v + u$.

(V3) Zero vector: there exists $\mathbf{0} \in E$ such that $v + \mathbf{0} = v$ for all $v \in E$.

(V4) Additive inverse: for each $v \in E$ there exists $-v \in E$ such that $v + (-v) = \mathbf{0}$.

Scalar multiplication axioms:

(V5) Compatibility: $\lambda(\mu v) = (\lambda\mu)v$.

(V6) Unit: $1_{\mathbb{K}}\, v = v$.

(V7) Distributivity over vector addition: $\lambda(u + v) = \lambda u + \lambda v$.

(V8) Distributivity over scalar addition: $(\lambda + \mu)v = \lambda v + \mu v$.

The elements of E are called *vectors* and the elements of $\mathbb{K}$ are called *scalars*.

Remark 2 (Notation)

When the field $\mathbb{K}$ is clear from context we simply say "vector space" rather than "$\mathbb{K}$-vector space". We write $\mathbf{0}$ for the zero vector and 0 for the zero scalar, relying on context to distinguish them.

Proposition 3 (Elementary properties)

Let E be a $\mathbb{K}$-vector space. For all $v \in E$ and $\lambda \in \mathbb{K}$:

(i) The zero vector $\mathbf{0}$ is unique.

(ii) The additive inverse $-v$ is unique.

(iii) $0_{\mathbb{K}}\, v = \mathbf{0}$.

(iv) $\lambda\, \mathbf{0} = \mathbf{0}$.

(v) $(-1)v = -v$.

(vi) $\lambda v = \mathbf{0}$ implies $\lambda = 0$ or $v = \mathbf{0}$.

Proof. (i) Suppose $\mathbf{0}$ and $\mathbf{0}'$ are both zero vectors. Then $\mathbf{0} = \mathbf{0} + \mathbf{0}' = \mathbf{0}'$, using the zero-vector property of $\mathbf{0}'$ and then of $\mathbf{0}$.

(ii) Suppose w and w' are both additive inverses of v. Then $w = w + \mathbf{0} = w + (v + w') = (w + v) + w' = \mathbf{0} + w' = w'$.

(iii) $0_{\mathbb{K}}\, v = (0_{\mathbb{K}} + 0_{\mathbb{K}})v = 0_{\mathbb{K}}\, v + 0_{\mathbb{K}}\, v$ by **(V8)**. Adding $-(0_{\mathbb{K}}\, v)$ to both sides gives $\mathbf{0} = 0_{\mathbb{K}}\, v$.

(iv) $\lambda\, \mathbf{0} = \lambda(\mathbf{0} + \mathbf{0}) = \lambda\, \mathbf{0} + \lambda\, \mathbf{0}$ by **(V7)**. Adding $-(\lambda\, \mathbf{0})$ yields $\mathbf{0} = \lambda\, \mathbf{0}$.

(v) $v + (-1)v = 1 \cdot v + (-1)v = (1 + (-1))v = 0_{\mathbb{K}}\, v = \mathbf{0}$ by **(V8)** and (iii). By uniqueness of inverses, $(-1)v = -v$.

(vi) If $\lambda \neq 0$, then λ^{-1} exists in $\mathbb{K}$ and $v = 1 \cdot v = (\lambda^{-1}\lambda)v = \lambda^{-1}(\lambda v) = \lambda^{-1}\mathbf{0} = \mathbf{0}$ by (iv). □

2.3 Key examples of vector spaces

We now present a gallery of examples that will accoSpany us throughout the course. The reader is encouraged to verify the axioms in each case (at least mentally).

Example 4 (The space $\mathbb{K}^n$)

For any positive integer n, the set

$$\mathbb{K}^n = \{\, (x_1, \dots, x_n) \mid x_1, \dots, x_n \in \mathbb{K} \,\}$$

equipped with componentwise addition and scalar multiplication:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n),$$
$$\lambda(x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n),$$

is a $\mathbb{K}$-vector space. The zero vector is $\mathbf{0} = (0, \dots, 0)$.
When $\mathbb{K} = \mathbb{R}$, the cases $n = 1, 2, 3$ correspond to the real line, the plane, and three-dimensional space, respectively.

Example 5 (The space $\mathcal{M}_{n,p}(\mathbb{K})$)

The set $\mathcal{M}_{n,p}(\mathbb{K})$ of all $n \times p$ matrices with entries in $\mathbb{K}$ is a $\mathbb{K}$-vector space under the usual matrix addition and scalar multiplication. The zero vector is the $n \times p$ zero matrix.
By identifying an $n \times p$ matrix with an element of $\mathbb{K}^{np}$ (by listing entries row by row), we see that $\mathcal{M}_{n,p}(\mathbb{K})$ and $\mathbb{K}^{np}$ have the "same" structure; this will be made precise by the notion of *isomorphism* in Chapter 3.

Example 6 (Polynomial spaces)

The set $\mathbb{K}[X]$ of all polynomials with coefficients in $\mathbb{K}$ is a $\mathbb{K}$-vector space under the usual addition and scalar multiplication of polynomials. The zero vector is the zero polynomial. For each $n \in \mathbb{N}$, the subset

$$\mathbb{K}_n[X] := \{\, P \in \mathbb{K}[X] \mid \deg P \leq n \,\} \cup \{0\}$$

of polynomials of degree at most n (together with the zero polynomial) is also a $\mathbb{K}$-vector space.

Example 7 (Function spaces)

Let S be a nonempty set. The set $\mathbb{K}^S := \{\, f \mid f\colon S \to \mathbb{K} \,\}$ of all functions from S to $\mathbb{K}$ is a $\mathbb{K}$-vector space under pointwise operations:

$$(f+g)(s) := f(s) + g(s),$$
$$(\lambda f)(s) := \lambda \cdot f(s),$$

for all $s \in S$, $\lambda \in \mathbb{K}$. The zero vector is the constant function $s \mapsto 0$.
Important special cases include:

- $\mathcal{C}^0([a,b], \mathbb{R})$: the space of continuous real-valued functions on $[a,b]$.
- $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$: the space of infinitely differentiable functions.
- The space of sequences ($\mathbb{K}^{\mathbb{N}}$): functions from $\mathbb{N}$ to $\mathbb{K}$.

Example 8 (Solution space of a homogeneous linear system)

Let $A \in \mathcal{M}_{n,p}(\mathbb{K})$. The set of solutions

$$\mathcal{S} = \{\, X \in \mathbb{K}^p \mid AX = \mathbf{0} \,\}$$

of the homogeneous system $AX = \mathbf{0}$ is a $\mathbb{K}$-vector space (a subspace of $\mathbb{K}^p$, as we shall see in Section 2.4).
Indeed, if $AX_1 = \mathbf{0}$ and $AX_2 = \mathbf{0}$, then $A(X_1 + X_2) = AX_1 + AX_2 = \mathbf{0}$ and $A(\lambda X_1) = \lambda A X_1 = \lambda \mathbf{0} = \mathbf{0}$.
Warning: The solution set of a *non*-homogeneous system $AX = B$ (with $B \neq \mathbf{0}$) is *not* a vector space, since it does not contain $\mathbf{0}$ (unless $B = \mathbf{0}$).

Example 9 (The trivial vector space)

The set $\{\mathbf{0}\}$, consisting of a single element, is a $\mathbb{K}$-vector space (the only possibility for the operations being $\mathbf{0}+\mathbf{0}=\mathbf{0}$ and $\lambda\,\mathbf{0}=\mathbf{0}$). It is called the *trivial* or *zero* vector space.

Remark 10 (The field $\mathbb{K}$ is a vector space over itself)

The field $\mathbb{K}$ is itself a $\mathbb{K}$-vector space (with field multiplication playing the role of scalar multiplication). More generally, $\mathbb{C}$ is an $\mathbb{R}$-vector space (of dimension 2, as we shall see).

2.4 Subspaces

A subspace is a subset of a vector space that is itself a vector space (with the inherited operations). Rather than checking all eight axioms, the following characterization provides a convenient shortcut.

Definition 11 (Vector subspace)

Let E be a $\mathbb{K}$-vector space. A subset $F \subseteq E$ is a *vector subspace* (or simply *subspace*) of E if:

(i) F is nonempty (equivalently, $\mathbf{0} \in F$).

(ii) F is closed under addition: $u+v \in F$ for all $u, v \in F$.

(iii) F is closed under scalar multiplication: $\lambda v \in F$ for all $\lambda \in \mathbb{K}$ and $v \in F$.

Proposition 12 (Subspace characterization)

A subset $F \subseteq E$ is a subspace of E if and only if

(a) $F \neq \emptyset$ (or equivalently, $\mathbf{0} \in F$), and

(b) for all $\lambda \in \mathbb{K}$ and all $u, v \in F$: $\lambda u + v \in F$.

Equivalently, F is nonempty and closed under linear combinations: for all $\lambda, \mu \in \mathbb{K}$ and $u, v \in F$, $\lambda u + \mu v \in F$.

Proof. If F is a subspace, then (a) and (b) are immediate from the definition. Conversely, assume (a) and (b). Taking $\lambda = 0$ in (b) shows $\mathbf{0} + v = v \in F$ for any $v \in F$, confirming closure under addition (take $\lambda = 1$). Taking $v = \mathbf{0}$ in (b) shows $\lambda u \in F$, confirming closure under scalar multiplication. Thus F satisfies all three conditions of the definition. □

Remark 13 (The nonemptiness condition)

Condition (a) cannot be dropped. The empty set $\emptyset$ is trivially closed under addition and scalar multiplication (vacuously) but is not a vector space.

Example 14 (Subspaces of $\mathbb{R}^2$)

The subspaces of $\mathbb{R}^2$ are precisely:

(i) $\{\mathbf{0}\}$ (the origin).

(ii) Lines through the origin: $\{ t\mathbf{v} \mid t \in \mathbb{R} \}$ for some $\mathbf{v} \neq \mathbf{0}$.

(iii) $\mathbb{R}^2$ itself.

Note that a line *not* passing through the origin (e.g. $\{ (x, y) \in \mathbb{R}^2 \mid x + y = 1 \}$) is *not* a subspace.

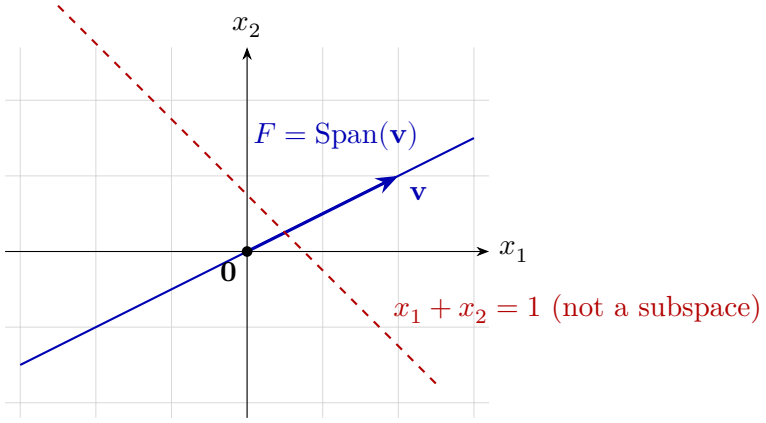


Figure 2.2: A subspace of $\mathbb{R}^2$ (a line through the origin) versus a non-subspace (a translated line).

Example 15 (Subspaces of $\mathbb{R}^3$)

The subspaces of $\mathbb{R}^3$ are:

(i) $\{\mathbf{0}\}$.

(ii) Lines through the origin.

(iii) Planes through the origin (e.g. $\{ (x, y, z) \in \mathbb{R}^3 \mid ax + by + cz = 0 \}$ with $(a, b, c) \neq \mathbf{0}$).

(iv) $\mathbb{R}^3$ itself.

This classification will follow from the theory of dimension developed later in this chapter.

Example 16 (Further examples of subspaces)

(a) The set of symmetric $n \times n$ matrices $\mathrm{Sym}_n(\mathbb{K}) = \{ A \in \mathcal{M}_n(\mathbb{K}) \mid A^{\mathsf{T}} = A \}$ is a subspace of $\mathcal{M}_n(\mathbb{K})$.

(b) The set of skew-symmetric matrices $\mathrm{Alt}_n(\mathbb{K}) = \{ A \in \mathcal{M}_n(\mathbb{K}) \mid A^{\mathsf{T}} = -A \}$ is a subspace of $\mathcal{M}_n(\mathbb{K})$.

(c) The set of polynomials of degree at most n, $\mathbb{K}_n[X]$, is a subspace of $\mathbb{K}[X]$.

(d) The set of even polynomials $\{ P \in \mathbb{K}[X] \mid P(-X) = P(X) \}$ is a subspace of $\mathbb{K}[X]$.

(e) The solution set of the differential equation $y'' + y = 0$ (a subset of $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$) is a subspace (the zero function is a solution, and linear combinations of solutions are solutions).

2.5 Intersection and sum of subspaces

Proposition 17 (Intersection of subspaces)

Let $(F_i)_{i\in I}$ be a (possibly infinite) family of subspaces of a $\mathbb{K}$-vector space E. Then $\bigcap_{i\in I} F_i$ is a subspace of E.

Proof. Let $F = \bigcap_{i\in I} F_i$.

- **Nonempty:** $\mathbf{0} \in F_i$ for every i, so $\mathbf{0} \in F$.
- **Closed under linear combinations:** Let $u, v \in F$ and $\lambda, \mu \in \mathbb{K}$. For each $i \in I$, $u, v \in F_i$ and F_i is a subspace, so $\lambda u + \mu v \in F_i$. Hence $\lambda u + \mu v \in F$. □

Remark 18 (Union is not a subspace in general)

In contrast, the *union* of two subspaces is generally *not* a subspace. For instance, in $\mathbb{R}^2$, let F_1 be the x-axis and F_2 the y-axis. Then $(1,0) \in F_1$ and $(0,1) \in F_2$, but $(1,0) + (0,1) = (1,1) \notin F_1 \cup F_2$.
In fact, $F_1 \cup F_2$ is a subspace if and only if $F_1 \subseteq F_2$ or $F_2 \subseteq F_1$.

The correct replacement for union is the *sum* of subspaces.

Definition 19 (Sum of subspaces)

Let $F_1, \dots, F_r$ be subspaces of E. Their *sum* is

$$F_1 + F_2 + \cdots + F_r := \{\, v_1 + v_2 + \cdots + v_r \mid v_i \in F_i \text{ for each } i \,\}.$$

For two subspaces, $F + G = \{\, u + v \mid u \in F,\ v \in G \,\}$.

Proposition 20 (Sum is the smallest containing subspace)

The sum $F_1 + \cdots + F_r$ is a subspace of E. It is the smallest subspace of E containing each F_i, i.e. $F_1 + \cdots + F_r = \bigcap \{\, H \mid H \text{ subspace of } E,\ F_i \subseteq H \text{ for all } i \,\}$.

Proof. We prove the case $r = 2$; the general case follows by induction.

Let $S = F + G$. First, $\mathbf{0} = \mathbf{0} + \mathbf{0} \in S$, so S is nonempty. Let $u_1 + v_1, u_2 + v_2 \in S$ (with $u_i \in F$, $v_i \in G$) and $\lambda \in \mathbb{K}$. Then

$$\lambda(u_1 + v_1) + (u_2 + v_2) = (\lambda u_1 + u_2) + (\lambda v_1 + v_2) \in S,$$

since $\lambda u_1 + u_2 \in F$ and $\lambda v_1 + v_2 \in G$. Hence S is a subspace.

For the minimality claim: $F \subseteq S$ (take $v = \mathbf{0}$) and $G \subseteq S$ (take $u = \mathbf{0}$), so S contains both. If H is any subspace containing F and G, then for any $u + v \in S$ with $u \in F$ and $v \in G$, we have $u, v \in H$, so $u + v \in H$; thus $S \subseteq H$. □

2.6 Direct sum and complementary subspaces

Definition 21 (Direct sum (internal))

Let F and G be subspaces of E. We say that E is the *direct sum* of F and G, written $E = F \oplus G$, if:

(i) $E = F + G$ (every vector in E can be written as $u + v$ with $u \in F$, $v \in G$), and

(ii) $F \cap G = \{\mathbf{0}\}$.

Equivalently, every $x \in E$ can be written *uniquely* as $x = u + v$ with $u \in F$ and $v \in G$.

Proposition 22 (Characterization of direct sum)

Let F and G be subspaces of E with $E = F + G$. The following are equivalent:

(i) $E = F \oplus G$.

(ii) $F \cap G = \{\mathbf{0}\}$.

(iii) Every $x \in E$ has a *unique* decomposition $x = u + v$ with $u \in F$ and $v \in G$.

Proof. **(i)⇔(ii)** is immediate from the definition.

(ii)⇒(iii): Suppose $x = u_1 + v_1 = u_2 + v_2$ with $u_i \in F$ and $v_i \in G$. Then $u_1 - u_2 = v_2 - v_1 \in F \cap G = \{\mathbf{0}\}$, so $u_1 = u_2$ and $v_1 = v_2$.

(iii)⇒(ii): The zero vector can be written as $\mathbf{0} = \mathbf{0} + \mathbf{0}$. If $w \in F \cap G$, then $\mathbf{0} = w + (-w)$ with $w \in F$ and $-w \in G$. By uniqueness, $w = \mathbf{0}$. □

Definition 23 (Complementary subspace)

If $E = F \oplus G$, we say that G is a *complement* of F in E (and F is a complement of G). In this case, F and G are called *complementary subspaces*.

Remark 24 (Non-uniqueness of complements)

A subspace may have many different complements. For instance, in $\mathbb{R}^2$, the x-axis has any non-horizontal line through the origin as a complement.

The direct sum extends naturally to more than two subspaces.

Definition 25 (Direct sum of r subspaces)

Let $F_1, \dots, F_r$ be subspaces of E. We say that $E = F_1 \oplus \cdots \oplus F_r$ if:

(i) $E = F_1 + \cdots + F_r$, and

(ii) for each $j \in \{1, \dots, r\}$, $F_j \cap (F_1 + \cdots + F_{j-1} + F_{j+1} + \cdots + F_r) = \{\mathbf{0}\}$.

Equivalently, every $x \in E$ has a unique decomposition $x = v_1 + \cdots + v_r$ with $v_i \in F_i$.

Example 26 (Direct sum decomposition in $\mathbb{R}^3$)

Let

$$F = \{\,(x,0,0) \mid x \in \mathbb{R}\,\} \qquad \text{(the } x\text{-axis)},$$
$$G = \{\,(0,y,z) \mid y,z \in \mathbb{R}\,\} \qquad \text{(the } yz\text{-plane)}.$$

Then $\mathbb{R}^3 = F \oplus G$, since every $(x,y,z) = (x,0,0) + (0,y,z)$ uniquely and $F \cap G = \{\mathbf{0}\}$.

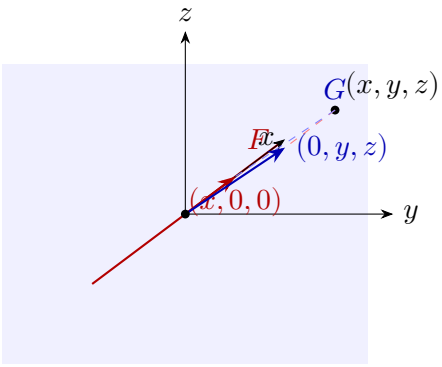


Figure 2.3: Direct sum decomposition $\mathbb{R}^3 = F \oplus G$ where F is the x-axis and G is the yz-plane.

2.7 Linear combinations and Span

Definition 27 (Linear combination)

Let E be a $\mathbb{K}$-vector space and $v_1, \dots, v_n \in E$. A *linear combination* of $v_1, \dots, v_n$ is any vector of the form

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n, \qquad \lambda_1, \dots, \lambda_n \in \mathbb{K}.$$

The scalars $\lambda_1, \dots, \lambda_n$ are called the *coefficients* of the linear combination.

Definition 28 (Span (generating set))

Let $\mathcal{F} = (v_1, \dots, v_n)$ be a family of vectors in E. The *Span* of $\mathcal{F}$ is

$$\mathrm{Span}(v_1, \dots, v_n) := \{\,\lambda_1 v_1 + \cdots + \lambda_n v_n \mid \lambda_1, \dots, \lambda_n \in \mathbb{K}\,\}.$$

It is the set of all linear combinations of $v_1, \dots, v_n$.
A family $\mathcal{F}$ is a *generating family* (or *Spanning set*) for E if $\mathrm{Span}(\mathcal{F}) = E$. In this case we say that $\mathcal{F}$ *Spans* (or *generates*) E.

Proposition 29 (Span is a subspace)

$\mathrm{Span}(v_1, \dots, v_n)$ is a subspace of E. Moreover, it is the smallest subspace containing $v_1, \dots, v_n$.

Proof. Let $W = \mathrm{Span}(v_1, \dots, v_n)$.

- $\mathbf{0} = 0v_1 + \cdots + 0v_n \in W$, so $W \neq \emptyset$.

- If $u = \sum_i \alpha_i v_i$ and $w = \sum_i \beta_i v_i$ are in W and $\lambda \in \mathbb{K}$, then $\lambda u + w = \sum_i (\lambda\alpha_i + \beta_i) v_i \in W$.

Hence W is a subspace. It contains each v_j (take $\lambda_j = 1$ and $\lambda_i = 0$ for $i \neq j$). If H is any subspace containing every v_j, then H contains all linear combinations of $v_1, \dots, v_n$, so $W \subseteq H$. □

Example 30 (Spanning $\mathbb{R}^3$)

The canonical vectors $\mathbf{e}_1 = (1,0,0)$, $\mathbf{e}_2 = (0,1,0)$, $\mathbf{e}_3 = (0,0,1)$ Span $\mathbb{R}^3$, since every $(a,b,c) \in \mathbb{R}^3$ equals $a\,\mathbf{e}_1 + b\,\mathbf{e}_2 + c\,\mathbf{e}_3$.

Example 31 (Spanning a plane in $\mathbb{R}^3$)

The vectors $\mathbf{u} = (1,1,0)$ and $\mathbf{v} = (0,1,1)$ Span the plane

$$\mathrm{Span}(\mathbf{u},\mathbf{v}) = \{\,(s, s+t, t) \mid s,t \in \mathbb{R}\,\} = \{\,(x,y,z) \in \mathbb{R}^3 \;\big|\; x - y + z = 0\,\}.$$

2.8 Linear independence

Definition 32 (Linear independence)

A family $(v_1, \dots, v_n)$ of vectors in E is *linearly independent* (or *free*) if

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = \mathbf{0} \implies \lambda_1 = \lambda_2 = \cdots = \lambda_n = 0.$$

A family that is not linearly independent is called *linearly dependent*.

Remark 33 (Interpretation)

Linear independence means that no vector in the family can be written as a linear combination of the others. Equivalently, the only way to represent $\mathbf{0}$ as a linear combination of $v_1, \dots, v_n$ is the *trivial* one (all coefficients zero).

Proposition 34 (Characterization of linear dependence)

A family $(v_1, \dots, v_n)$ with $n \geq 2$ is linearly dependent if and only if at least one vector v_j can be written as a linear combination of the others:

$$v_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} \mu_i\, v_i.$$

Proof. ($\Rightarrow$) If the family is dependent, there exist $\lambda_1, \dots, \lambda_n$, not all zero, with $\sum_i \lambda_i v_i = \mathbf{0}$. Pick j with $\lambda_j \neq 0$. Then $v_j = -\lambda_j^{-1} \sum_{i \neq j} \lambda_i v_i$.

($\Leftarrow$) If $v_j = \sum_{i \neq j} \mu_i v_i$, then $\sum_{i \neq j} \mu_i v_i + (-1) v_j = \mathbf{0}$ is a nontrivial relation. □

Proposition 35 (Properties of linear independence)

Let E be a $\mathbb{K}$-vector space.

(i) A single nonzero vector (v) is linearly independent.

(ii) Any subfamily of a linearly independent family is linearly independent.

(iii) If $(v_1, \dots, v_n)$ is linearly independent and $w \notin \mathrm{Span}(v_1, \dots, v_n)$, then $(v_1, \dots, v_n, w)$ is linearly independent.

(iv) Any family containing $\mathbf{0}$ is linearly dependent.

(v) Any family containing a repeated vector is linearly dependent.

Proof. (i) If $\lambda v = \mathbf{0}$ with $v \neq \mathbf{0}$, then $\lambda = 0$ by Proposition 3(vi).

(ii) Suppose $(v_{i_1}, \dots, v_{i_k})$ is a subfamily and $\sum_{j=1}^{k} \lambda_j v_{i_j} = \mathbf{0}$. Extend to a combination of the full family by setting the remaining coefficients to zero; independence of the full family forces all $\lambda_j = 0$.

(iii) Suppose $\lambda_1 v_1 + \cdots + \lambda_n v_n + \mu w = \mathbf{0}$. If $\mu \neq 0$, then $w = -\mu^{-1}(\lambda_1 v_1 + \cdots + \lambda_n v_n) \in \mathrm{Span}(v_1, \dots, v_n)$, contradicting the hypothesis. So $\mu = 0$, and then $\lambda_1 = \cdots = \lambda_n = 0$ by independence.

(iv) $1 \cdot \mathbf{0} = \mathbf{0}$ is a nontrivial relation.

(v) If $v_i = v_j$ for $i \neq j$, then $1 \cdot v_i + (-1) \cdot v_j = \mathbf{0}$ is nontrivial. □

Example 36 (Independence in $\mathbb{R}^3$)

(a) The canonical basis vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ are linearly independent: if $a\,\mathbf{e}_1 + b\,\mathbf{e}_2 + c\,\mathbf{e}_3 = \mathbf{0}$, then $(a, b, c) = (0, 0, 0)$.

(b) The vectors $(1, 1, 0)$, $(1, 0, 1)$, $(0, 1, 1)$ are linearly independent. Indeed, $\alpha(1, 1, 0) + \beta(1, 0, 1) + \gamma(0, 1, 1) = \mathbf{0}$ gives

$$\alpha + \beta = 0, \quad \alpha + \gamma = 0, \quad \beta + \gamma = 0,$$

which has the unique solution $\alpha = \beta = \gamma = 0$.

(c) The vectors $(1, 2, 3)$, $(4, 5, 6)$, $(7, 8, 9)$ are linearly *dependent*: $(1, 2, 3) - 2(4, 5, 6) + (7, 8, 9) = (0, 0, 0)$.

Example 37 (Independence in $\mathbb{K}_n[X]$)

The polynomials $1, X, X^2, \dots, X^n$ are linearly independent in $\mathbb{K}[X]$: if $\alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n = 0$ (the zero polynomial), then all $\alpha_i = 0$ by comparing coefficients.

2.9 Bases

Definition 38 (Basis)

A family $\mathcal{B} = (v_1, \dots, v_n)$ of vectors in E is a *basis* of E if it is both linearly independent and Spanning: $\mathcal{B}$ is linearly independent and $\mathrm{Span}(\mathcal{B}) = E$.

Theorem 39 (Characterization of a basis)

Let $\mathcal{B} = (v_1, \dots, v_n)$ be a family in E. The following are equivalent:

(i) $\mathcal{B}$ is a basis of E.

(ii) Every $v \in E$ can be written *uniquely* as $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$.

(iii) $\mathcal{B}$ is a maximal linearly independent family.

(iv) $\mathcal{B}$ is a minimal Spanning family.

Proof. **(i)⇒(ii):** Since $\mathcal{B}$ Spans E, at least one representation exists. Suppose $v = \sum_i \lambda_i v_i = \sum_i \mu_i v_i$. Then $\sum_i (\lambda_i - \mu_i) v_i = \mathbf{0}$, and independence gives $\lambda_i = \mu_i$ for all i.

(ii)⇒(i): Existence of a representation means $\mathcal{B}$ Spans E. If $\sum_i \lambda_i v_i = \mathbf{0}$, then $\sum_i \lambda_i v_i = \sum_i 0 \cdot v_i$ are two representations of $\mathbf{0}$; uniqueness gives $\lambda_i = 0$ for all i.

(i)⇒(iii): If $\mathcal{B}$ is a basis and we add any $w \in E$, then $w = \sum_i \lambda_i v_i$, so the enlarged family contains $w - \sum_i \lambda_i v_i = \mathbf{0}$ as a nontrivial relation; hence it is dependent. So $\mathcal{B}$ is maximal independent.

(iii)⇒(i): If $\mathcal{B}$ does not Span E, there exists $w \notin \mathrm{Span}(\mathcal{B})$, and $(v_1, \dots, v_n, w)$ is independent by Proposition 35(iii), contradicting maximality.

(i)⇒(iv): If we remove v_j, we claim the remaining family does not Span E. Indeed, v_j cannot be written as a linear combination of the other v_i (by independence), so v_j is not in the Span of the reduced family.

(iv)⇒(i): $\mathcal{B}$ Spans E by assumption. If $\mathcal{B}$ is dependent, some v_j is a combination of the others (by Proposition 34), so removing v_j still gives a Spanning family, contradicting minimality. □

Definition 40 (Coordinates)

If $\mathcal{B} = (v_1, \dots, v_n)$ is a basis of E and $v = \sum_i \lambda_i v_i$, the uniquely determined scalars $\lambda_1, \dots, \lambda_n$ are the *coordinates* (or *components*) of v relative to $\mathcal{B}$. The column vector

$$[v]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in \mathbb{K}^n$$

is called the *coordinate vector* of v in basis $\mathcal{B}$.

Example 41 (Canonical basis of $\mathbb{K}^n$)

The *canonical* (or *standard*) basis of $\mathbb{K}^n$ is $\mathcal{E} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ where $\mathbf{e}_i$ is the n-tuple with a 1 in position i and 0's elsewhere. The coordinates of $(x_1, \dots, x_n)$ in $\mathcal{E}$ are simply $x_1, \dots, x_n$.

Example 42 (Canonical basis of $\mathbb{K}_n[X]$)

The family $(1, X, X^2, \dots, X^n)$ is a basis of $\mathbb{K}_n[X]$: every polynomial of degree $\leq n$ is a unique linear combination of these monomials. In this basis, the coordinates of a polynomial are its coefficients.

Example 43 (Canonical basis of $\mathcal{M}_{n,p}(\mathbb{K})$)

The family $(E_{ij})_{1\leq i\leq n,\,1\leq j\leq p}$, where E_{ij} is the matrix with 1 in position (i,j) and 0's elsewhere, is a basis of $\mathcal{M}_{n,p}(\mathbb{K})$.

2.10 Dimension

The notion of dimension captures the "size" of a vector space. Its definition rests on a fundamental theorem about the relationship between independent families and Spanning families.

Theorem 44 (Steinitz exchange lemma)

Let E be a $\mathbb{K}$-vector space. If $(v_1,\dots,v_p)$ is linearly independent and $(w_1,\dots,w_q)$ Spans E, then $p\leq q$.

Proof. We proceed by induction on p.

Base case ($p=0$): The empty family is independent and $0\leq q$.

Inductive step: Assume the result holds for all independent families of size $p-1$. Suppose $(v_1,\dots,v_p)$ is independent and $(w_1,\dots,w_q)$ Spans E.

Since $(w_1,\dots,w_q)$ Spans E, we can write

$$v_p=\alpha_1 w_1+\cdots+\alpha_q w_q$$

for some $\alpha_i\in\mathbb{K}$. Not all α_i can be zero (since $v_p\neq\mathbf{0}$). By reindexing, assume $\alpha_q\neq 0$. Then

$$w_q=\alpha_q^{-1}\Big(v_p-\sum_{i=1}^{q-1}\alpha_i w_i\Big).$$

Therefore every vector in E that was a linear combination of $w_1,\dots,w_q$ can also be expressed using $w_1,\dots,w_{q-1},v_p$. That is, $(w_1,\dots,w_{q-1},v_p)$ still Spans E.

Now $(v_1,\dots,v_{p-1})$ is independent (as a subfamily of an independent family), and $(w_1,\dots,w_{q-1},v_p)$ Spans E. We claim $(v_1,\dots,v_{p-1})$ remains independent in E, so by the induction hypothesis, $p-1\leq q-1+1=q$... but we need to be more careful.

We refine the argument. Since $(w_1,\dots,w_{q-1},v_p)$ Spans E, each v_i $(1\leq i\leq p-1)$ can be written as a combination of $w_1,\dots,w_{q-1},v_p$. Since $(v_1,\dots,v_p)$ is independent, $v_1,\dots,v_{p-1}$ are not in $\mathrm{Span}(v_p)$ and hence depend nontrivially on $w_1,\dots,w_{q-1}$. We may thus view $(v_1,\dots,v_{p-1})$ as a linearly independent family in the space $\mathrm{Span}(w_1,\dots,w_{q-1},v_p)$.

Apply the exchange process again: write v_{p-1} as a combination of $w_1,\dots,w_{q-1},v_p$. The coefficient of some w_j must be nonzero (otherwise $v_{p-1}\in\mathrm{Span}(v_p)$, contradicting independence). Swap w_j for v_{p-1}.

Continuing this process p times, we replace p of the w_i's by $v_1,\dots,v_p$. At each step, at least one w_i must be available for replacement (its coefficient must be nonzero). This is possible only if $p\leq q$. □

Corollary 45 (Invariance of basis size)

If E has a finite basis, then every basis of E has the same number of elements.

Proof. Let $\mathcal{B}=(v_1,\dots,v_n)$ and $\mathcal{B}'=(w_1,\dots,w_m)$ be two bases. Since $\mathcal{B}$ is independent and $\mathcal{B}'$ Spans E, the Steinitz lemma gives $n\leq m$. Symmetrically, $m\leq n$. Hence $n=m$. □

Definition 46 (Dimension)

A $\mathbb{K}$-vector space E is *finite-dimensional* if it has a finite Spanning set. In this case, the *dimension* of E, denoted $\dim_{\mathbb{K}} E$ (or simply $\dim E$), is the common cardinality of all its bases.
By convention, $\dim\{\mathbf{0}\} = 0$.
If E has no finite Spanning set, it is *infinite-dimensional*.

Example 47 (Dimensions of standard spaces)

(a) $\dim_{\mathbb{K}} \mathbb{K}^n = n$ (the canonical basis has n elements).

(b) $\dim_{\mathbb{K}} \mathbb{K}_n[X] = n+1$ (the basis $1, X, \dots, X^n$ has $n+1$ elements).

(c) $\dim_{\mathbb{K}} \mathcal{M}_{n,p}(\mathbb{K}) = np$.

(d) $\mathbb{K}[X]$ is infinite-dimensional: the family $(1, X, X^2, \dots)$ is independent and Spans $\mathbb{K}[X]$, but it is not finite.

Theorem 48 (Existence of a basis (finite-dimensional case))

Every finite-dimensional vector space $E \neq \{\mathbf{0}\}$ has a basis. More precisely:

(i) Every Spanning family contains a basis (one can extract a basis from it).

(ii) Every linearly independent family can be extended to a basis.

Proof. (i) Let $\mathcal{F} = (w_1, \dots, w_q)$ Span E. If $\mathcal{F}$ is independent, it is a basis. If not, some w_j is a combination of the others; remove it. The resulting family still Spans E (any combination involving w_j can be rewritten using the others). Repeat until the family is independent. The process terminates since we cannot reduce below a single vector (assuming $E \neq \{\mathbf{0}\}$).

(ii) Let $(v_1, \dots, v_p)$ be independent. If it Spans E, it is a basis. If not, there exists $w \notin \text{Span}(v_1, \dots, v_p)$, and $(v_1, \dots, v_p, w)$ is independent by Proposition 35(iii). Repeat. By the Steinitz lemma, the size of an independent family is bounded by any Spanning family's size, so the process terminates. □

Theorem 49 (Existence of complements)

Let E be a finite-dimensional $\mathbb{K}$-vector space and F a subspace of E. Then F has at least one complement in E: there exists a subspace G such that $E = F \oplus G$.

Proof. Let $(v_1, \dots, v_p)$ be a basis of F. This is a linearly independent family in E; by Theorem 48(ii), extend it to a basis $(v_1, \dots, v_p, w_1, \dots, w_q)$ of E. Set $G = \text{Span}(w_1, \dots, w_q)$.

$E = F + G$**:** Any $x \in E$ can be written as $x = \sum_i \alpha_i v_i + \sum_j \beta_j w_j \in F + G$.

$F \cap G = \{\mathbf{0}\}$**:** If $x \in F \cap G$, write $x = \sum_i \alpha_i v_i = \sum_j \beta_j w_j$. Then $\sum_i \alpha_i v_i - \sum_j \beta_j w_j = \mathbf{0}$, and since $(v_1, \dots, v_p, w_1, \dots, w_q)$ is a basis (hence independent), all coefficients vanish: $x = \mathbf{0}$. □

2.11 Dimension formulas

Proposition 50 (Dimension of a subspace)

Let E be a finite-dimensional $\mathbb{K}$-vector space and F a subspace of E. Then:

(i) F is finite-dimensional and $\dim F \leq \dim E$.

(ii) $\dim F = \dim E$ if and only if $F = E$.

Proof. (i) Any independent family in F is also independent in E, so its size is at most $\dim E$ (by the Steinitz lemma). Take a maximal independent family in F; it is a basis of F (if it did not Span F, it could be enlarged, contradicting maximality). Hence F is finite-dimensional and $\dim F \leq \dim E$.

(ii) If $\dim F = \dim E = n$, let $(v_1, \dots, v_n)$ be a basis of F. This is an independent family of size n in E, hence a basis of E (a maximal independent family, since no independent family in E has more than $\dim E = n$ elements). Thus $F = \mathrm{Span}(v_1, \dots, v_n) = E$.

Conversely, $F = E$ trivially implies $\dim F = \dim E$. □

Proposition 51 (Dimension of a direct sum)

If $E = F \oplus G$, then $\dim E = \dim F + \dim G$.

Proof. Let $(v_1, \dots, v_p)$ be a basis of F and $(w_1, \dots, w_q)$ a basis of G. We show $(v_1, \dots, v_p, w_1, \dots, w_q)$ is a basis of E.

Spanning: Any $x \in E$ can be written $x = u + v$ with $u \in F$, $v \in G$. Expanding u and v in their respective bases gives x as a combination of $v_1, \dots, v_p, w_1, \dots, w_q$.

Independence: Suppose $\sum_i \alpha_i v_i + \sum_j \beta_j w_j = \mathbf{0}$. Then $\sum_i \alpha_i v_i = -\sum_j \beta_j w_j \in F \cap G = \{\mathbf{0}\}$. Hence $\sum_i \alpha_i v_i = \mathbf{0}$ and $\sum_j \beta_j w_j = \mathbf{0}$, which by independence of each basis gives all $\alpha_i = 0$ and all $\beta_j = 0$.

Therefore the combined family is a basis of E with $p + q$ elements. □

Corollary 52 (Dimension of a complement)

If F is a subspace of a finite-dimensional space E, then any complement G of F satisfies $\dim G = \dim E - \dim F$.

2.12 The Grassmann formula

Theorem 53 (Grassmann formula (dimension of a sum))

Let E be a finite-dimensional $\mathbb{K}$-vector space and let F, G be subspaces of E. Then

$$\dim(F + G) = \dim F + \dim G - \dim(F \cap G).$$

Proof. Let $p = \dim F$, $q = \dim G$, and $r = \dim(F \cap G)$.

Step 1. Let $(u_1, \dots, u_r)$ be a basis of $F \cap G$.

Step 2. Since $F \cap G \subseteq F$, we can extend $(u_1, \dots, u_r)$ to a basis of F:

$$(u_1, \dots, u_r, v_1, \dots, v_s) \quad \text{is a basis of } F,$$

where $s = p - r$.

Step 3. Similarly, extend $(u_1, \dots, u_r)$ to a basis of G:

$$(u_1, \dots, u_r,\ w_1, \dots, w_t) \quad \text{is a basis of } G,$$

where $t = q - r$.

Step 4. We claim that

$$\mathcal{B} = (u_1, \dots, u_r,\ v_1, \dots, v_s,\ w_1, \dots, w_t)$$

is a basis of $F + G$.

Spanning: Any $x \in F + G$ is $x = f + g$ with $f \in F$ and $g \in G$. Writing f in the basis of F and g in the basis of G:

$$x = \Big(\sum_{i=1}^{r} \alpha_i u_i + \sum_{j=1}^{s} \beta_j v_j\Big) + \Big(\sum_{i=1}^{r} \gamma_i u_i + \sum_{k=1}^{t} \delta_k w_k\Big) = \sum_{i=1}^{r} (\alpha_i + \gamma_i) u_i + \sum_{j=1}^{s} \beta_j v_j + \sum_{k=1}^{t} \delta_k w_k.$$

So $x \in \operatorname{Span}(\mathcal{B})$.

Independence: Suppose

$$\sum_{i=1}^{r} \alpha_i u_i + \sum_{j=1}^{s} \beta_j v_j + \sum_{k=1}^{t} \delta_k w_k = \mathbf{0}. \tag{2.1}$$

Set $h := \sum_{k=1}^{t} \delta_k w_k = -\sum_{i=1}^{r} \alpha_i u_i - \sum_{j=1}^{s} \beta_j v_j$.

The right-hand side lies in F (since $u_i, v_j \in F$). The left-hand side lies in G (since $w_k \in G$). Hence $h \in F \cap G$.

Since $(u_1, \dots, u_r)$ is a basis of $F \cap G$, we can write $h = \sum_{i=1}^{r} \mu_i u_i$ for some $\mu_i \in \mathbb{K}$. But also $h = \sum_{k=1}^{t} \delta_k w_k$, so

$$\sum_{k=1}^{t} \delta_k w_k - \sum_{i=1}^{r} \mu_i u_i = \mathbf{0}.$$

Since $(u_1, \dots, u_r, w_1, \dots, w_t)$ is a basis of G (hence independent), all $\delta_k = 0$ and all $\mu_i = 0$. In particular, $h = \mathbf{0}$.

Returning to (2.1) with all $\delta_k = 0$: $\sum_i \alpha_i u_i + \sum_j \beta_j v_j = \mathbf{0}$. Since $(u_1, \dots, u_r, v_1, \dots, v_s)$ is a basis of F (hence independent), all $\alpha_i = 0$ and all $\beta_j = 0$.

Conclusion. $\mathcal{B}$ is a basis of $F + G$ with $r + s + t = r + (p - r) + (q - r) = p + q - r$ elements, so

$$\dim(F + G) = p + q - r = \dim F + \dim G - \dim(F \cap G). \qquad \square$$

Corollary 54 (Criterion for direct sum via dimension)

Let F and G be subspaces of a finite-dimensional space E. Then $E = F \oplus G$ if and only if $E = F + G$ and $\dim E = \dim F + \dim G$. Equivalently, any two of the following three conditions imply the third:

(i) $E = F + G$,

(ii) $F \cap G = \{\mathbf{0}\}$,

(iii) $\dim E = \dim F + \dim G$.

Proof. By the Grassmann formula, $\dim(F + G) = \dim F + \dim G - \dim(F \cap G)$. Condition (ii) says $\dim(F \cap G) = 0$. Condition (i) says $\dim(F + G) = \dim E$. Condition (iii) is $\dim E = \dim F + \dim G$.

If (i) and (ii) hold: $\dim E = \dim(F+G) = \dim F + \dim G$, giving (iii).

If (i) and (iii) hold: $\dim F + \dim G = \dim E = \dim(F+G) = \dim F + \dim G - \dim(F \cap G)$, so $\dim(F \cap G) = 0$, giving (ii).

If (ii) and (iii) hold: $\dim(F+G) = \dim F + \dim G = \dim E$, and since $F + G \subseteq E$ is a subspace with the same dimension as E, Proposition 50(ii) gives $F + G = E$, i.e. (i). □

2.13 Rank of a family of vectors

Definition 55 (Rank of a family)

Let $(v_1, \dots, v_p)$ be a family of vectors in a $\mathbb{K}$-vector space E. The *rank* of this family is

$$\operatorname{rank}(v_1, \dots, v_p) := \dim \operatorname{Span}(v_1, \dots, v_p).$$

Proposition 56 (Properties of rank)

Let $\mathcal{F} = (v_1, \dots, v_p)$ be a family of vectors in E.

(i) $0 \leq \operatorname{rank}(\mathcal{F}) \leq p$.

(ii) $\operatorname{rank}(\mathcal{F}) = p$ if and only if $\mathcal{F}$ is linearly independent.

(iii) If E is finite-dimensional, $\mathcal{F}$ Spans E if and only if $\operatorname{rank}(\mathcal{F}) = \dim E$.

(iv) $\mathcal{F}$ is a basis of E if and only if $\operatorname{rank}(\mathcal{F}) = p = \dim E$.

Proof. (i) $\operatorname{Span}(\mathcal{F})$ is a subspace Spanned by p vectors, so $\dim \operatorname{Span}(\mathcal{F}) \leq p$. The lower bound is clear.

(ii) $\operatorname{rank}(\mathcal{F}) = p$ means $\operatorname{Span}(\mathcal{F})$ has a basis of size p. Since $\mathcal{F}$ Spans $\operatorname{Span}(\mathcal{F})$, we can extract a basis of size $\dim \operatorname{Span}(\mathcal{F}) = p$ from $\mathcal{F}$; but $\mathcal{F}$ already has p elements, so it must be the basis itself—hence $\mathcal{F}$ is independent. Conversely, if $\mathcal{F}$ is independent, it is a basis of $\operatorname{Span}(\mathcal{F})$, so $\operatorname{rank}(\mathcal{F}) = p$.

(iii) $\mathcal{F}$ Spans E iff $\operatorname{Span}(\mathcal{F}) = E$ iff $\dim \operatorname{Span}(\mathcal{F}) = \dim E$ (by Proposition 50(ii)).

(iv) Combines (ii) and (iii). □

Remark 57 (Rank of the columns of a matrix)

If $A \in \mathcal{M}_{n,p}(\mathbb{K})$ has columns $C_1, \dots, C_p \in \mathbb{K}^n$, then $\operatorname{rank}(C_1, \dots, C_p) = \dim \operatorname{Span}(C_1, \dots, C_p)$. This number is called the *column rank* of A. It equals the *row rank* and is simply called the *rank* of A, denoted $\operatorname{rank}(A)$. The proof of this equality will be given in Chapter 3.

2.14 Applications

2.14.1 Solution spaces of homogeneous linear systems

Proposition 58 (Dimension of the solution space)

Let $A \in \mathcal{M}_{n,p}(\mathbb{K})$ with $\operatorname{rank}(A) = r$. The solution space $\mathcal{S} = \{ X \in \mathbb{K}^p \mid AX = \mathbf{0} \}$ is a subspace of $\mathbb{K}^p$ of dimension $p - r$.

Proof. That $\mathcal{S}$ is a subspace was shown in Example 8. The dimension formula $\dim \mathcal{S} = p - r$ is the *rank–nullity theorem*, which will be proved rigorously in Chapter 3 once the necessary language of linear maps is available. For now, we note that Gaussian elimination produces exactly $p - r$ free variables, each of which gives rise to one basis vector of $\mathcal{S}$. □

Example 59 (A concrete system)

Consider the homogeneous system in $\mathbb{R}^4$:

$$\begin{cases} x_1 + 2x_2 - x_3 + x_4 = 0, \\ 2x_1 + 4x_2 + x_3 - 2x_4 = 0. \end{cases}$$

The coefficient matrix has rank 2 (since the two rows are not proportional after reduction). Hence $\dim \mathcal{S} = 4 - 2 = 2$.
Row reduction gives $x_1 = -2x_2 + x_3 - x_4$ and $x_3 = \frac{4}{3}x_4$ (after back-substitution). Setting the free variables x_2 and x_4 to $(1, 0)$ and $(0, 1)$ respectively yields a basis of $\mathcal{S}$.

2.14.2 Polynomial spaces

Example 60 (Even and odd polynomials)

Let $E_n = \mathbb{K}_n[X]$ (polynomials of degree $\leq n$). Define

$$F = \{ P \in E_n \mid P(-X) = P(X) \} \qquad \text{(even polynomials)},$$
$$G = \{ P \in E_n \mid P(-X) = -P(X) \} \qquad \text{(odd polynomials)}.$$

Then F and G are subspaces of E_n and $E_n = F \oplus G$.
Indeed, every polynomial P can be uniquely decomposed as

$$P(X) = \underbrace{\frac{P(X) + P(-X)}{2}}_{\in F} + \underbrace{\frac{P(X) - P(-X)}{2}}_{\in G}.$$

A basis of F is $(1, X^2, X^4, \ldots)$ (even powers up to n) and a basis of G is $(X, X^3, X^5, \ldots)$ (odd powers up to n). The dimensions satisfy

$$\dim F + \dim G = \left\lfloor \tfrac{n}{2} \right\rfloor + 1 + \left\lfloor \tfrac{n+1}{2} \right\rfloor = n + 1 = \dim E_n.$$

Example 61 (Symmetric and skew-symmetric matrices)

Let $E = \mathcal{M}_n(\mathbb{K})$ with $\mathrm{char}(\mathbb{K}) \neq 2$. Define

$$S = \{ A \in E \mid A^\mathsf{T} = A \},$$
$$A = \{ A \in E \mid A^\mathsf{T} = -A \}.$$

Then $E = S \oplus A$, since every matrix M decomposes uniquely as

$$M = \underbrace{\frac{M + M^\mathsf{T}}{2}}_{\in S} + \underbrace{\frac{M - M^\mathsf{T}}{2}}_{\in A}.$$

We have $\dim S = \frac{n(n+1)}{2}$ and $\dim A = \frac{n(n-1)}{2}$, and indeed $\frac{n(n+1)}{2} + \frac{n(n-1)}{2} = n^2 = \dim E$.

2.15 Exercises

Exercise 62 (Verifying vector space axioms)

Verify that the set $\mathbb{R}^+ = (0, \infty)$ with the operations

$$x \oplus y := xy, \qquad \lambda \odot x := x^\lambda,$$

is an $\mathbb{R}$-vector space. What is the zero vector? What is the additive inverse of x?

Exercise 63 (Subspace verification)

Determine which of the following subsets of $\mathbb{R}^3$ are subspaces. Justify your answers.

(a) $S_1 = \{ (x, y, z) \in \mathbb{R}^3 \mid x + 2y - z = 0 \}$.

(b) $S_2 = \{ (x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 \leq 1 \}$.

(c) $S_3 = \{ (x, y, z) \in \mathbb{R}^3 \mid x = y = z \}$.

(d) $S_4 = \{ (x, y, z) \in \mathbb{R}^3 \mid xy = 0 \}$.

(e) $S_5 = \{ (x, y, z) \in \mathbb{R}^3 \mid x + y + z = 1 \}$.

Exercise 64 (Subspaces of function spaces)

Let $E = \mathbb{R}^\mathbb{R}$ be the vector space of all functions $\mathbb{R} \to \mathbb{R}$. Prove that the following subsets are subspaces:

(a) The set of even functions $\{ f \in E \mid f(-x) = f(x) \text{ for all } x \}$.

(b) The set of functions vanishing at 0: $\{ f \in E \mid f(0) = 0 \}$.

(c) The set of periodic functions with period $T > 0$: $\{ f \in E \mid f(x + T) = f(x) \text{ for all } x \}$.

Exercise 65 (Linear independence in $\mathbb{R}^4$)

Determine whether the following vectors in $\mathbb{R}^4$ are linearly independent:

$$v_1 = (1,0,1,0), \quad v_2 = (0,1,0,1), \quad v_3 = (1,1,1,1), \quad v_4 = (1,0,0,1).$$

If they are dependent, find an explicit nontrivial linear relation.

Exercise 66 (Extending to a basis)

In $\mathbb{R}^4$, the vectors $v_1 = (1,1,0,0)$ and $v_2 = (0,1,1,0)$ are linearly independent. Extend $\{v_1, v_2\}$ to a basis of $\mathbb{R}^4$ by adding suitable vectors from the canonical basis.

Exercise 67 (Sum and intersection)

In $\mathbb{R}^4$, let

$$F = \mathrm{Span}\big((1,0,1,0),\,(0,1,0,1)\big),$$
$$G = \mathrm{Span}\big((1,1,0,0),\,(0,0,1,1)\big).$$

(a) Find $\dim F$, $\dim G$, and $\dim(F+G)$.

(b) Determine $F \cap G$ and verify the Grassmann formula.

(c) Is $F + G$ a direct sum?

Exercise 68 (Direct sum decomposition)

Let $E = \mathcal{M}_2(\mathbb{R})$. Define

$$F = \{\, A \in E \mid A^{\mathsf{T}} = A \,\}, \qquad G = \{\, A \in E \mid A^{\mathsf{T}} = -A \,\}.$$

(a) Show that $E = F \oplus G$.

(b) Find bases for F and G, and verify that $\dim F + \dim G = \dim E$.

Exercise 69 (Polynomial subspace)

In $\mathbb{R}_3[X]$ (polynomials of degree ≤ 3), let

$$F = \{\, P \in \mathbb{R}_3[X] \mid P(0) = 0 \text{ and } P(1) = 0 \,\}.$$

(a) Show that F is a subspace of $\mathbb{R}_3[X]$.

(b) Find a basis of F and determine $\dim F$.

(c) Find a complement of F in $\mathbb{R}_3[X]$.

Exercise 70 (The Grassmann formula in practice)

Let $E = \mathbb{R}^5$ and

$$F = \{ (x_1, x_2, x_3, x_4, x_5) \in \mathbb{R}^5 \mid x_1 - x_2 = 0,\ x_3 - x_4 + x_5 = 0 \},$$
$$G = \{ (x_1, x_2, x_3, x_4, x_5) \in \mathbb{R}^5 \mid x_1 = 0,\ x_2 - x_3 = 0,\ x_4 = 0 \}.$$

(a) Find bases for F and G.

(b) Compute $\dim F$, $\dim G$, $\dim(F \cap G)$, and $\dim(F + G)$.

(c) Verify the Grassmann formula.

Exercise 71 (Abstract dimension argument)

Let E be a vector space of dimension n and let F, G be subspaces with $\dim F + \dim G > n$. Prove that $F \cap G \neq \{\mathbf{0}\}$.

Exercise 72 (Characterizing bases via cardinality)

Let E be a $\mathbb{K}$-vector space with $\dim E = n$. Let $\mathcal{F} = (v_1, \dots, v_n)$ be a family of n vectors. Prove that the following are equivalent:

(i) $\mathcal{F}$ is a basis of E.

(ii) $\mathcal{F}$ is linearly independent.

(iii) $\mathcal{F}$ Spans E.

(Note: In general, one needs *both* independence and Spanning to guarantee a basis; the point of this exercise is that when the cardinality equals $\dim E$, either condition alone suffices.)

Exercise 73 (Direct sum of three subspaces)

In $\mathbb{R}^3$, let

$$F_1 = \mathrm{Span}((1,0,0)),$$
$$F_2 = \mathrm{Span}((0,1,0)),$$
$$F_3 = \mathrm{Span}((1,1,1)).$$

(a) Show that $\mathbb{R}^3 = F_1 \oplus F_2 \oplus F_3$.

(b) Exhibit three subspaces G_1, G_2, G_3 of $\mathbb{R}^3$ such that $G_i \cap G_j = \{\mathbf{0}\}$ for all $i \neq j$ and $G_1 + G_2 + G_3 = \mathbb{R}^3$, but $\mathbb{R}^3 \neq G_1 \oplus G_2 \oplus G_3$.

(*Hint:* pairwise trivial intersection does not imply direct sum for three or more subspaces.)

Exercise 74 (Infinite-dimensional spaces)

(a) Prove that $\mathbb{K}[X]$ is infinite-dimensional by showing that the family $(1, X, X^2, \dots)$ is linearly independent.

(b) Show that the function space $\mathbb{R}^{\mathbb{R}}$ is infinite-dimensional. (*Hint:* Consider the family $(\exp_\lambda)_{\lambda\in\mathbb{R}}$ where $\exp_\lambda(x) = e^{\lambda x}$, or use the inclusion $\mathbb{K}[X] \hookrightarrow \mathbb{R}^{\mathbb{R}}$ via the evaluation map.)

(c) Prove that every vector space has a basis (assuming the Axiom of Choice, or equivalently, Zorn's Lemma).

Exercise 75 (Grassmann formula for three subspaces)

Let F_1, F_2, F_3 be subspaces of a finite-dimensional space E. Prove the inequality

$$\dim(F_1+F_2+F_3) \geq \dim F_1+\dim F_2+\dim F_3-\dim(F_1\cap F_2)-\dim(F_1\cap F_3)-\dim(F_2\cap F_3).$$

Give an example where strict inequality holds.

Chapter summary

- A **vector space** over a field $\mathbb{K}$ is a set E with addition and scalar multiplication satisfying eight axioms **(V1)**–**(V8)**. The central examples are $\mathbb{K}^n$, $\mathcal{M}_{n,p}(\mathbb{K})$, polynomial spaces $\mathbb{K}_n[X]$ and $\mathbb{K}[X]$, and function spaces.
- A **subspace** is a nonempty subset closed under addition and scalar multiplication. The intersection of subspaces is a subspace; their union is generally not, and is replaced by their **sum**.
- The sum $E = F \oplus G$ is **direct** when $F \cap G = \{\mathbf{0}\}$, equivalently when every vector has a unique F-plus-G decomposition. Every subspace of a finite-dimensional space admits a complement.
- A **linear combination** of $v_1, \dots, v_n$ is a vector $\sum \lambda_i v_i$. The **Span** of a family is the subspace of all such combinations. A family is **linearly independent** if the only combination yielding $\mathbf{0}$ is the trivial one.
- A **basis** is a family that is both independent and Spanning, or equivalently, a family giving a *unique* representation for every vector. The **Steinitz exchange lemma** ensures that all bases have the same size; this common size is the **dimension**.
- Key dimension formulas:
  - $\dim(F \oplus G) = \dim F + \dim G$.
  - **Grassmann formula:** $\dim(F + G) = \dim F + \dim G - \dim(F \cap G)$.
  - $F \subseteq E$ and $\dim F = \dim E$ imply $F = E$.
- The **rank** of a family of vectors is the dimension of its Span. It equals the maximal number of independent vectors in the family.
- **Applications:** The solution space of a homogeneous system $AX = \mathbf{0}$ is a subspace of $\mathbb{K}^p$ of dimension $p - \operatorname{rank}(A)$. Polynomial spaces and matrix spaces admit natural direct sum decompositions (e.g. even/odd polynomials, symmetric/skew-symmetric matrices).

Chapter 3

Linear Maps and Matrices

The study of vector spaces becomes truly powerful only when we understand the *maps* between them that respect their algebraic structure. Consider the Euclidean plane $\mathbb{R}^2$. Many natural geometric transformations—rotations, reflections, projections onto a line, scalings—share a remarkable property: they preserve the operations of vector addition and scalar multiplication. A rotation through angle θ sends the sum of two vectors to the sum of their rotated images; scaling by a factor λ commutes with addition.

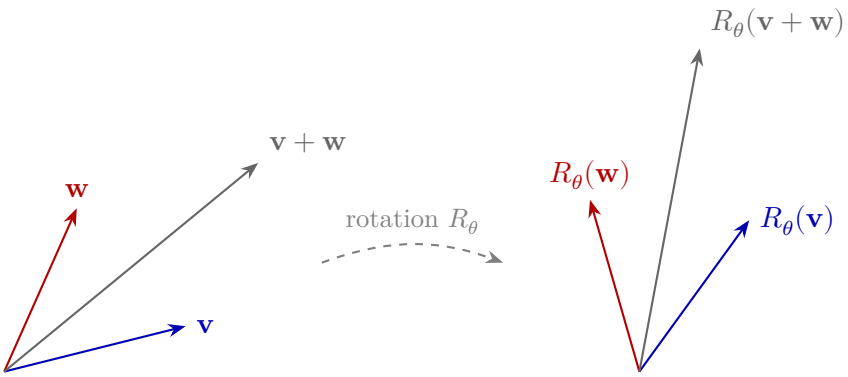


Figure 3.1: A rotation maps the parallelogram law to a rotated parallelogram: the image of a sum is the sum of the images.

These structure-preserving maps are called *linear maps*. They form the bridge between the abstract theory of vector spaces and the concrete computations of matrix algebra. In this chapter we develop their theory systematically: we define linear maps, study their kernel and image, prove the fundamental rank–nullity theorem, represent linear maps by matrices, and learn to change bases. Along the way we shall see that matrix multiplication is nothing but the composition of linear maps in disguise.

Throughout this chapter, $\mathbb{K}$ denotes a field (typically $\mathbb{R}$ or $\mathbb{C}$), and E, F, G denote $\mathbb{K}$-vector spaces unless stated otherwise. We freely use results from Chapter 2, especially the notions of subspace, basis, and dimension.

3.1 Definition and first properties

Definition 1 (Linear map)

Let E and F be vector spaces over $\mathbb{K}$. A map $f\colon E \to F$ is *linear* (or is a $\mathbb{K}$-*linear map*, or a *homomorphism of vector spaces*) if it satisfies the following two conditions:

(i) **Additivity:** $f(u+v) = f(u) + f(v)$ for all $u, v \in E$.

(ii) **Homogeneity:** $f(\lambda u) = \lambda\, f(u)$ for all $\lambda \in \mathbb{K}$, $u \in E$.

Equivalently, f is linear if and only if $f(\lambda u + \mu v) = \lambda\, f(u) + \mu\, f(v)$ for all $\lambda, \mu \in \mathbb{K}$ and all $u, v \in E$.

Remark 2 (Terminology)

Several special names are used:

- A linear map $f\colon E \to E$ (same domain and codomain) is called an *endomorphism* of E.
- A bijective linear map is called an *isomorphism*.
- A bijective endomorphism is called an *automorphism*.
- A linear map $f\colon E \to \mathbb{K}$ (codomain is the base field) is called a *linear form*.

Proposition 3 (Elementary properties)

Let $f\colon E \to F$ be a linear map. Then:

(i) $f(\mathbf{0}_E) = \mathbf{0}_F$.

(ii) $f(-v) = -f(v)$ for all $v \in E$.

(iii) $f\big(\sum_{i=1}^{n} \lambda_i v_i\big) = \sum_{i=1}^{n} \lambda_i\, f(v_i)$ for all $\lambda_i \in \mathbb{K}$, $v_i \in E$.

Proof. (i) Setting $\lambda = 0$ in homogeneity: $f(\mathbf{0}_E) = f(0 \cdot v) = 0 \cdot f(v) = \mathbf{0}_F$.

(ii) $f(-v) = f((-1)\cdot v) = (-1)\cdot f(v) = -f(v)$.

(iii) By induction on n, using additivity and homogeneity at each step. The base case $n = 1$ is homogeneity, and the inductive step follows from $f\big(\sum_{i=1}^{n+1} \lambda_i v_i\big) = f\big(\sum_{i=1}^{n} \lambda_i v_i + \lambda_{n+1} v_{n+1}\big) = f\big(\sum_{i=1}^{n} \lambda_i v_i\big) + \lambda_{n+1}\, f(v_{n+1})$. □

Proposition 4 (A linear map is determined by its values on a basis)

Let $\mathcal{B} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ be a basis of E, and let $w_1, \dots, w_n$ be arbitrary vectors in F. Then there exists a *unique* linear map $f\colon E \to F$ such that $f(\mathbf{e}_i) = w_i$ for all $i \in \{1, \dots, n\}$.

Proof. Existence. Every $v \in E$ has a unique decomposition $v = \sum_{i=1}^{n} \lambda_i \mathbf{e}_i$. Define $f(v) := \sum_{i=1}^{n} \lambda_i w_i$. One verifies directly that f is linear: for $v = \sum \lambda_i \mathbf{e}_i$ and $v' = \sum \mu_i \mathbf{e}_i$ and $\alpha, \beta \in \mathbb{K}$,

$$f(\alpha v + \beta v') = f\Big(\sum_i (\alpha\lambda_i + \beta\mu_i)\mathbf{e}_i\Big) = \sum_i (\alpha\lambda_i + \beta\mu_i) w_i = \alpha \sum_i \lambda_i w_i + \beta \sum_i \mu_i w_i = \alpha f(v) + \beta f(v').$$

Moreover $f(\mathbf{e}_i) = w_i$ since $\mathbf{e}_i = 0\cdot\mathbf{e}_1 + \cdots + 1\cdot\mathbf{e}_i + \cdots + 0\cdot\mathbf{e}_n$.

Uniqueness. Suppose $g\colon E \to F$ is linear with $g(\mathbf{e}_i) = w_i$. For any $v = \sum \lambda_i \mathbf{e}_i$, $g(v) = \sum \lambda_i\, g(\mathbf{e}_i) = \sum \lambda_i w_i = f(v)$. □

3.2 Examples of linear maps

Example 5 (Rotation in $\mathbb{R}^2$)

For a fixed angle θ, the map $R_\theta\colon \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$R_\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}$$

is a linear map (an automorphism, in fact, with inverse $R_{-\theta}$).

Example 6 (Orthogonal projection onto a line)

Let $\ell \subset \mathbb{R}^2$ be the line through the origin with unit direction vector $\mathbf{u} = (\cos\alpha, \sin\alpha)^{\mathsf{T}}$. The orthogonal projection onto ℓ is

$$\operatorname{proj}_\ell(\mathbf{v}) = \langle \mathbf{v}, \mathbf{u} \rangle\, \mathbf{u} = \begin{pmatrix} \cos^2\alpha & \cos\alpha\sin\alpha \\ \cos\alpha\sin\alpha & \sin^2\alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

This is linear. Note $\operatorname{proj}_\ell \circ \operatorname{proj}_\ell = \operatorname{proj}_\ell$ (idempotent).

Example 7 (Reflection)

The reflection of $\mathbb{R}^2$ across the line ℓ through the origin with direction angle α is given by

$$S_\alpha \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

This is a linear map satisfying $S_\alpha^2 = \mathrm{Id}$.

Example 8 (Scaling (homothety))

For $\lambda \in \mathbb{K}$, the map $h_\lambda\colon E \to E$ defined by $h_\lambda(v) = \lambda v$ is linear. It contracts ($|\lambda| < 1$), dilates ($|\lambda| > 1$), or reflects ($\lambda < 0$) vectors.

Example 9 (Differentiation)

Let $\mathcal{P}_n(\mathbb{R})$ be the space of real polynomials of degree at most n. The derivative map $D\colon \mathcal{P}_n(\mathbb{R}) \to \mathcal{P}_{n-1}(\mathbb{R})$ defined by $D(p) = p'$ is linear, since $(p+q)' = p' + q'$ and $(\lambda p)' = \lambda p'$.

Example 10 (Integration)

The map $I\colon \mathcal{C}([0,1], \mathbb{R}) \to \mathbb{R}$ defined by $I(f) = \int_0^1 f(t)\, dt$ is a linear form on the vector space of continuous real-valued functions on $[0,1]$.

Example 11 (Matrix–vector multiplication)

Let $A \in \mathcal{M}_{m,n}(\mathbb{K})$. The map $f_A \colon \mathbb{K}^n \to \mathbb{K}^m$ defined by $f_A(x) = Ax$ is linear. Conversely, every linear map $\mathbb{K}^n \to \mathbb{K}^m$ arises this way (see Section 3.9).

3.3 Geometric illustrations

The following figures illustrate how several linear maps transform the unit square in $\mathbb{R}^2$.

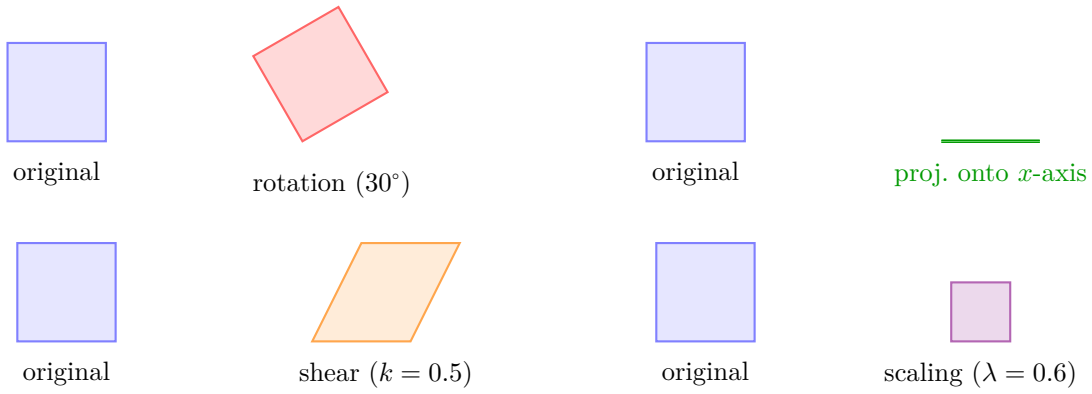


Figure 3.2: Effect of linear maps on the unit square: rotation, projection onto the x-axis, horizontal shear, and uniform scaling.

3.4 Kernel and image

Definition 12 (Kernel)

Let $f \colon E \to F$ be a linear map. The *kernel* (or *null space*) of f is

$$\operatorname{Ker} f := \{\, v \in E \mid f(v) = \mathbf{0}_F \,\}.$$

Definition 13 (Image)

The *image* (or *range*) of f is

$$\operatorname{Im} f := \{\, f(v) \mid v \in E \,\} = \{\, w \in F \mid \exists\, v \in E,\ f(v) = w \,\}.$$

Theorem 14 (Kernel and image are subspaces)

Let $f \colon E \to F$ be linear. Then:

(i) $\operatorname{Ker} f$ is a subspace of E.

(ii) $\operatorname{Im} f$ is a subspace of F.

Proof. (i) We verify the three subspace criteria. *Non-empty:* $f(\mathbf{0}_E) = \mathbf{0}_F$, so $\mathbf{0}_E \in \operatorname{Ker} f$. *Closed under addition:* if $u, v \in \operatorname{Ker} f$, then $f(u+v) = f(u) + f(v) = \mathbf{0}_F + \mathbf{0}_F = \mathbf{0}_F$, so $u + v \in \operatorname{Ker} f$. *Closed under scalar multiplication:* if $v \in \operatorname{Ker} f$ and $\lambda \in \mathbb{K}$, then $f(\lambda v) = \lambda f(v) = \lambda \cdot \mathbf{0}_F = \mathbf{0}_F$, so $\lambda v \in \operatorname{Ker} f$.

(ii) *Non-empty:* $\mathbf{0}_F = f(\mathbf{0}_E) \in \operatorname{Im} f$. *Closed under addition:* if $w_1, w_2 \in \operatorname{Im} f$, write $w_i = f(v_i)$; then $w_1 + w_2 = f(v_1) + f(v_2) = f(v_1 + v_2) \in \operatorname{Im} f$. *Scalar multiplication:* $\lambda w_1 = \lambda f(v_1) = f(\lambda v_1) \in \operatorname{Im} f$. □

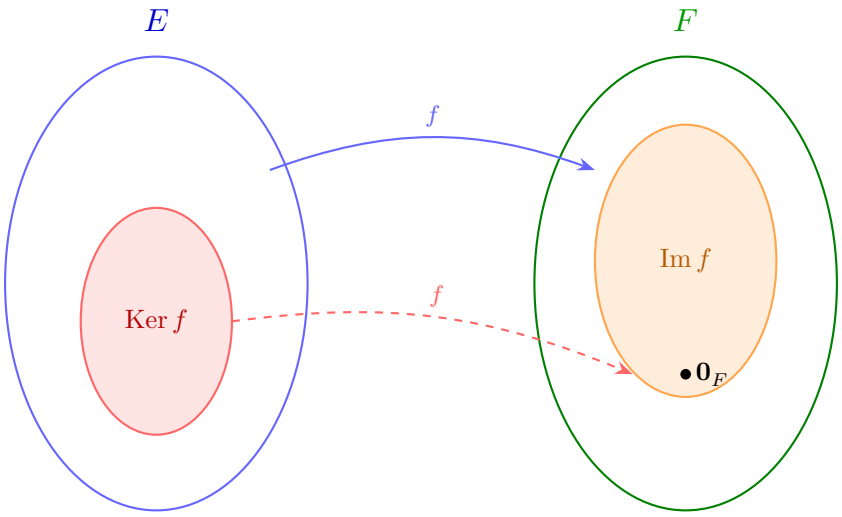


Figure 3.3: The kernel is a subspace of E mapping to $\mathbf{0}_F$; the image is a subspace of F.

Proposition 15 (Image of a Spanning set)

If $E = \operatorname{Span}(v_1, \dots, v_p)$, then $\operatorname{Im} f = \operatorname{Span}(f(v_1), \dots, f(v_p))$. In particular, if $\mathcal{B} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ is a basis of E, then $\operatorname{Im} f = \operatorname{Span}(f(\mathbf{e}_1), \dots, f(\mathbf{e}_n))$.

Proof. Every $w \in \operatorname{Im} f$ has the form $w = f(v)$ where $v = \sum_{i=1}^{p} \lambda_i v_i$. By linearity, $w = \sum \lambda_i f(v_i) \in \operatorname{Span}(f(v_1), \dots, f(v_p))$. Conversely, each $f(v_i) \in \operatorname{Im} f$, and $\operatorname{Im} f$ is a subspace, so it contains $\operatorname{Span}(f(v_1), \dots, f(v_p))$. □

Definition 16 (Rank and nullity)

Let $f\colon E \to F$ be a linear map between finite-dimensional spaces.

- The *rank* of f is $\operatorname{rank}(f) := \dim(\operatorname{Im} f)$.
- The *nullity* of f is $\dim(\operatorname{Ker} f)$.

3.5 The rank–nullity theorem

Theorem 17 (Rank–nullity theorem (dimension theorem))

Let E be a finite-dimensional vector space and let $f\colon E \to F$ be a linear map. Then $\operatorname{Im} f$ is finite-dimensional and

$$\boxed{\dim E \;=\; \dim(\operatorname{Ker} f) \;+\; \dim(\operatorname{Im} f) \;=\; \dim(\operatorname{Ker} f) \;+\; \operatorname{rank}(f).}$$

Proof. Set $n = \dim E$ and $r = \dim(\operatorname{Ker} f)$. Let $(u_1, \dots, u_r)$ be a basis of $\operatorname{Ker} f$. Since $\operatorname{Ker} f$ is a subspace of the finite-dimensional space E, we may extend this to a basis of E:

$$(u_1, \dots, u_r, v_1, \dots, v_s)$$

where $s = n-r$. We claim that $(f(v_1), \dots, f(v_s))$ is a basis of $\operatorname{Im} f$, which will prove $\dim(\operatorname{Im} f) = s = n - r$.

Step 1: $(f(v_1), \dots, f(v_s))$ Spans $\operatorname{Im} f$. Let $w \in \operatorname{Im} f$, say $w = f(x)$ with $x = \alpha_1 u_1 + \cdots + \alpha_r u_r + \beta_1 v_1 + \cdots + \beta_s v_s$. Then

$$w = f(x) = \alpha_1 \underbrace{f(u_1)}_{=\mathbf{0}} + \cdots + \alpha_r \underbrace{f(u_r)}_{=\mathbf{0}} + \beta_1 f(v_1) + \cdots + \beta_s f(v_s) = \beta_1 f(v_1) + \cdots + \beta_s f(v_s),$$

so $w \in \operatorname{Span}(f(v_1), \dots, f(v_s))$.

Step 2: $(f(v_1), \dots, f(v_s))$ is linearly independent. Suppose $\beta_1 f(v_1) + \cdots + \beta_s f(v_s) = \mathbf{0}_F$. By linearity, $f(\beta_1 v_1 + \cdots + \beta_s v_s) = \mathbf{0}_F$, so $\beta_1 v_1 + \cdots + \beta_s v_s \in \operatorname{Ker} f$. Since $(u_1, \dots, u_r)$ is a basis of $\operatorname{Ker} f$, there exist $\gamma_1, \dots, \gamma_r \in \mathbb{K}$ such that

$$\beta_1 v_1 + \cdots + \beta_s v_s = \gamma_1 u_1 + \cdots + \gamma_r u_r.$$

Rearranging: $\gamma_1 u_1 + \cdots + \gamma_r u_r - \beta_1 v_1 - \cdots - \beta_s v_s = \mathbf{0}_E$. Since $(u_1, \dots, u_r, v_1, \dots, v_s)$ is a basis of E, all coefficients are zero. In particular, $\beta_1 = \cdots = \beta_s = 0$.

We conclude that $(f(v_1), \dots, f(v_s))$ is a basis of $\operatorname{Im} f$, so $\dim(\operatorname{Im} f) = s = n-r$, i.e., $\dim E = \dim(\operatorname{Ker} f) + \dim(\operatorname{Im} f)$. □

Corollary 18 (Dimension bound on rank)

For any linear map $f : E \to F$ with E finite-dimensional,

$$\operatorname{rank}(f) \leq \min(\dim E, \dim F).$$

Proof. $\operatorname{rank}(f) = \dim(\operatorname{Im} f) \leq \dim F$ since $\operatorname{Im} f \subseteq F$, and $\operatorname{rank}(f) = \dim E - \dim(\operatorname{Ker} f) \leq \dim E$. □

3.6 Injectivity, surjectivity, bijectivity

Theorem 19 (Injectivity criterion)

A linear map $f : E \to F$ is injective if and only if $\operatorname{Ker} f = \{\mathbf{0}_E\}$.

Proof. ($\Rightarrow$) Suppose f is injective. If $v \in \operatorname{Ker} f$, then $f(v) = \mathbf{0}_F = f(\mathbf{0}_E)$. Injectivity gives $v = \mathbf{0}_E$.

($\Leftarrow$) Suppose $\operatorname{Ker} f = \{\mathbf{0}_E\}$. If $f(u) = f(v)$, then $f(u - v) = f(u) - f(v) = \mathbf{0}_F$, so $u - v \in \operatorname{Ker} f = \{\mathbf{0}_E\}$, hence $u = v$. □

Proposition 20 (Characterizations in finite dimension)

Let $f : E \to F$ be linear with $\dim E = \dim F = n < \infty$. Then the following are equivalent:

(i) f is injective.

(ii) f is surjective.

(iii) f is bijective (i.e., an isomorphism).

(iv) $\operatorname{rank}(f) = n$.

Proof. By the rank–nullity theorem, $\operatorname{rank}(f) = n - \dim(\operatorname{Ker} f)$.
(i) $\Leftrightarrow$ (iv): f is injective $\Leftrightarrow \operatorname{Ker} f = \{\mathbf{0}\} \Leftrightarrow \dim(\operatorname{Ker} f) = 0 \Leftrightarrow \operatorname{rank}(f) = n$.
(ii) $\Leftrightarrow$ (iv): f is surjective $\Leftrightarrow \operatorname{Im} f = F \Leftrightarrow \dim(\operatorname{Im} f) = \dim F = n \Leftrightarrow \operatorname{rank}(f) = n$.
(iii) $\Leftrightarrow$ (i) $\wedge$ (ii): immediate from the equivalences above. □

Remark 21 (Same dimension is essential)

The equivalence of injectivity and surjectivity *fails* when $\dim E \neq \dim F$. For instance, the inclusion $\mathbb{R}^2 \hookrightarrow \mathbb{R}^3$ (sending $(x, y) \mapsto (x, y, 0)$) is injective but not surjective.

Definition 22 (Isomorphism of vector spaces)

Two vector spaces E and F over $\mathbb{K}$ are *isomorphic*, written $E \cong F$, if there exists an isomorphism $f : E \to F$.

Theorem 23 (Classification by dimension)

Two finite-dimensional $\mathbb{K}$-vector spaces are isomorphic if and only if they have the same dimension. In particular, every n-dimensional $\mathbb{K}$-vector space is isomorphic to $\mathbb{K}^n$.

Proof. ($\Rightarrow$) If $f : E \xrightarrow{\sim} F$ is an isomorphism and $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ is a basis of E, then $(f(\mathbf{e}_1), \dots, f(\mathbf{e}_n))$ is a basis of F (an injective linear map sends linearly independent sets to linearly independent sets, and a surjective map ensures they Span F). Hence $\dim F = n = \dim E$.

($\Leftarrow$) Let $\dim E = \dim F = n$. Choose bases $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ of E and $(\mathbf{f}_1, \dots, \mathbf{f}_n)$ of F. By Proposition 4, there is a unique linear map $f : E \to F$ with $f(\mathbf{e}_i) = \mathbf{f}_i$. Since f maps a basis to a basis, it is bijective. □

3.7 Composition of linear maps

Proposition 24 (Composition is linear)

If $f : E \to F$ and $g : F \to G$ are linear maps, then the composition $g \circ f : E \to G$ is linear.

Proof. For all $\lambda, \mu \in \mathbb{K}$ and $u, v \in E$:

$$(g \circ f)(\lambda u + \mu v) = g\big(f(\lambda u + \mu v)\big) = g\big(\lambda f(u) + \mu f(v)\big) = \lambda\, g(f(u)) + \mu\, g(f(v)) = \lambda\,(g \circ f)(u) + \mu\,(g \circ f)(v).$$

□

Proposition 25 (Properties of composition)

Let $f : E \to F$, $g : F \to G$, $h : G \to H$ be linear.

(i) **Associativity:** $h \circ (g \circ f) = (h \circ g) \circ f$.

(ii) **Identity:** $f \circ \mathrm{Id}_E = f = \mathrm{Id}_F \circ f$.

(iii) If f is an isomorphism, its inverse $f^{-1} : F \to E$ is also linear, with $f^{-1} \circ f = \mathrm{Id}_E$ and $f \circ f^{-1} = \mathrm{Id}_F$.

Proof. (i) and (ii) follow from the corresponding properties of function composition. For (iii), let $w_1, w_2 \in F$ and $\lambda \in \mathbb{K}$. Write $w_i = f(v_i)$. Then $f^{-1}(\lambda w_1 + w_2) = f^{-1}(\lambda f(v_1) + f(v_2)) = f^{-1}(f(\lambda v_1 + v_2)) = \lambda v_1 + v_2 = \lambda f^{-1}(w_1) + f^{-1}(w_2)$. □

Proposition 26 (Kernel and image under composition)

Let $f\colon E \to F$ and $g\colon F \to G$ be linear. Then:

(i) $\operatorname{Ker} f \subseteq \operatorname{Ker}(g \circ f)$.

(ii) $\operatorname{Im}(g \circ f) \subseteq \operatorname{Im} g$.

(iii) If g is injective, then $\operatorname{Ker}(g \circ f) = \operatorname{Ker} f$.

(iv) If f is surjective, then $\operatorname{Im}(g \circ f) = \operatorname{Im} g$.

Proof. (i) If $v \in \operatorname{Ker} f$, then $(g \circ f)(v) = g(\mathbf{0}_F) = \mathbf{0}_G$.
(ii) Every element of $\operatorname{Im}(g \circ f)$ has the form $g(f(v)) \in \operatorname{Im} g$.
(iii) $v \in \operatorname{Ker}(g \circ f)$ means $g(f(v)) = \mathbf{0}_G$. If g is injective, $f(v) = \mathbf{0}_F$, so $v \in \operatorname{Ker} f$.
(iv) If f is surjective, every $w \in F$ is $f(v)$ for some v, so $g(w) = g(f(v)) \in \operatorname{Im}(g \circ f)$. Hence $\operatorname{Im} g \subseteq \operatorname{Im}(g \circ f)$. □

3.8 The vector space of linear maps

Theorem 27 ($\mathcal{L}(E, F)$ is a vector space)

Let E and F be vector spaces over $\mathbb{K}$. Define operations on the set $\mathcal{L}(E, F)$ of all linear maps from E to F:

- **Addition:** $(f + g)(v) := f(v) + g(v)$.
- **Scalar multiplication:** $(\lambda f)(v) := \lambda\, f(v)$.

Then $\mathcal{L}(E, F)$ is a $\mathbb{K}$-vector space, with zero element the zero map $\mathbf{0}\colon v \mapsto \mathbf{0}_F$.

Proof. One must verify the vector space axioms. We check that $f + g$ and λf are indeed linear (so that $\mathcal{L}(E, F)$ is closed under these operations), and the remaining axioms are inherited from those of F applied pointwise.

$f+g$ is linear: $(f+g)(\alpha u+\beta v) = f(\alpha u+\beta v)+g(\alpha u+\beta v) = \alpha f(u)+\beta f(v)+\alpha g(u)+\beta g(v) = \alpha(f+g)(u) + \beta(f+g)(v)$.

λf is linear: $(\lambda f)(\alpha u + \beta v) = \lambda f(\alpha u + \beta v) = \lambda(\alpha f(u) + \beta f(v)) = \alpha(\lambda f)(u) + \beta(\lambda f)(v)$.

Associativity of addition, commutativity, etc., all follow from the corresponding properties in F. □

Proposition 28 (Dimension of $\mathcal{L}(E, F)$)

If $\dim E = n$ and $\dim F = m$, then $\dim \mathcal{L}(E, F) = nm$.

Proof. This follows from the isomorphism $\mathcal{L}(E, F) \cong \mathcal{M}_{m,n}(\mathbb{K})$ established in Section 3.9: the space of $m \times n$ matrices has dimension mn. □

Remark 29 (The endomorphism algebra)

The space $\operatorname{End}(E) = \mathcal{L}(E, E)$ carries an additional operation: composition. This makes $\operatorname{End}(E)$ a $\mathbb{K}$-*algebra* (a vector space equipped with an associative bilinear multiplication and a unit element Id_E). Note that composition is not commutative in general.

3.9 Matrix of a linear map

Definition 30 (Matrix representation)

Let E and F be finite-dimensional with ordered bases $\mathcal{B} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ and $\mathcal{C} = (\mathbf{f}_1, \dots, \mathbf{f}_m)$ respectively. Let $f \colon E \to F$ be linear. For each $j \in \{1, \dots, n\}$, write

$$f(\mathbf{e}_j) = \sum_{i=1}^{m} a_{ij}\, \mathbf{f}_i.$$

The $m \times n$ matrix

$$\mathcal{M}_{\mathcal{C},\mathcal{B}}(f) := (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

is called the *matrix of f relative to the bases $\mathcal{B}$ and $\mathcal{C}$*. The j-th column is the coordinate vector of $f(\mathbf{e}_j)$ in basis $\mathcal{C}$.

Remark 31 (Convention)

When $E = F$ and $\mathcal{B} = \mathcal{C}$, we simply write $\mathcal{M}_{\mathcal{B}}(f)$. When working in $\mathbb{K}^n$ with the canonical basis $\mathcal{E}$, we identify f with the matrix $A = \mathcal{M}_{\mathcal{E}}(f)$ and write $f(x) = Ax$.

Example 32 (Matrix of a rotation)

The rotation $R_\theta \colon \mathbb{R}^2 \to \mathbb{R}^2$ of Example 5 has matrix in the canonical basis:

$$\mathcal{M}_{\mathcal{E}}(R_\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

The first column is $R_\theta(\mathbf{e}_1) = (\cos\theta, \sin\theta)^{\mathsf{T}}$ and the second column is $R_\theta(\mathbf{e}_2) = (-\sin\theta, \cos\theta)^{\mathsf{T}}$.

Example 33 (Matrix of differentiation)

Consider $D \colon \mathcal{P}_3(\mathbb{R}) \to \mathcal{P}_3(\mathbb{R})$, $D(p) = p'$, with basis $\mathcal{B} = (1, t, t^2, t^3)$. Then $D(1) = 0$, $D(t) = 1$, $D(t^2) = 2t$, $D(t^3) = 3t^2$, so

$$\mathcal{M}_{\mathcal{B}}(D) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Theorem 34 (The matrix representation is an isomorphism)

The map

$$\Phi \colon \mathcal{L}(E, F) \to \mathcal{M}_{m,n}(\mathbb{K}), \qquad f \mapsto \mathcal{M}_{\mathcal{C},\mathcal{B}}(f)$$

is an isomorphism of vector spaces. Moreover:

(i) $\mathcal{M}_{\mathcal{C},\mathcal{B}}(f+g) = \mathcal{M}_{\mathcal{C},\mathcal{B}}(f) + \mathcal{M}_{\mathcal{C},\mathcal{B}}(g)$.

(ii) $\mathcal{M}_{\mathcal{C},\mathcal{B}}(\lambda f) = \lambda\, \mathcal{M}_{\mathcal{C},\mathcal{B}}(f)$.

(iii) If $g\colon F \to G$ is linear with G having basis $\mathcal{D}$, then

$$\mathcal{M}_{\mathcal{D},\mathcal{B}}(g \circ f) = \mathcal{M}_{\mathcal{D},\mathcal{C}}(g) \cdot \mathcal{M}_{\mathcal{C},\mathcal{B}}(f).$$

Proof. Linearity of Φ (parts (i) and (ii)) follows directly from the definitions. Bijectivity follows from Proposition 4: for every matrix $A \in \mathcal{M}_{m,n}(\mathbb{K})$, there is a unique $f \in \mathcal{L}(E,F)$ with $\Phi(f) = A$ (define f by $f(\mathbf{e}_j) = \sum_i a_{ij}\mathbf{f}_i$).

(iii) Let $A = \mathcal{M}_{\mathcal{C},\mathcal{B}}(f)$ and $B = \mathcal{M}_{\mathcal{D},\mathcal{C}}(g)$. The j-th column of $\mathcal{M}_{\mathcal{D},\mathcal{B}}(g\circ f)$ is the coordinate vector of $(g\circ f)(\mathbf{e}_j) = g(f(\mathbf{e}_j))$ in basis $\mathcal{D}$. Now $f(\mathbf{e}_j) = \sum_{k=1}^{m} a_{kj}\mathbf{f}_k$, so

$$g(f(\mathbf{e}_j)) = \sum_{k=1}^{m} a_{kj}\, g(\mathbf{f}_k) = \sum_{k=1}^{m} a_{kj} \sum_{i=1}^{\ell} b_{ik}\, \mathbf{d}_i = \sum_{i=1}^{\ell} \Big(\sum_{k=1}^{m} b_{ik}\, a_{kj}\Big)\mathbf{d}_i.$$

The coefficient of $\mathbf{d}_i$ is $\sum_k b_{ik}a_{kj} = (BA)_{ij}$, proving $\mathcal{M}_{\mathcal{D},\mathcal{B}}(g\circ f) = BA$. □

Remark 35 (Matrix multiplication = composition)

Theorem 34(iii) reveals the true meaning of matrix multiplication: it is the algebraic encoding of the composition of linear maps. The product BA of matrices is defined precisely so that the matrix of $g\circ f$ equals the product of the matrices of g and f.

3.10 Change of basis

Definition 36 (Transition matrix (change-of-basis matrix))

Let $\mathcal{B} = (\mathbf{e}_1,\dots,\mathbf{e}_n)$ and $\mathcal{B}' = (\mathbf{e}'_1,\dots,\mathbf{e}'_n)$ be two bases of E. The *transition matrix* from $\mathcal{B}$ to $\mathcal{B}'$ is

$$P_{\mathcal{B}\to\mathcal{B}'} := \mathcal{M}_{\mathcal{B}}(\mathrm{Id}_E, \mathcal{B}', \mathcal{B}) = \big[\,[\mathbf{e}'_1]_{\mathcal{B}}\ \ [\mathbf{e}'_2]_{\mathcal{B}}\ \ \cdots\ \ [\mathbf{e}'_n]_{\mathcal{B}}\,\big],$$

where $[\mathbf{e}'_j]_{\mathcal{B}}$ is the column of coordinates of $\mathbf{e}'_j$ in basis $\mathcal{B}$.

Proposition 37 (Properties of transition matrices)

(i) $P_{\mathcal{B}\to\mathcal{B}'}$ is invertible, with $(P_{\mathcal{B}\to\mathcal{B}'})^{-1} = P_{\mathcal{B}'\to\mathcal{B}}$.

(ii) If $[v]_{\mathcal{B}}$ and $[v]_{\mathcal{B}'}$ denote the coordinate vectors of $v \in E$ in the two bases, then

$$[v]_{\mathcal{B}} = P_{\mathcal{B}\to\mathcal{B}'}\,[v]_{\mathcal{B}'}.$$

(iii) For three bases $\mathcal{B},\mathcal{B}',\mathcal{B}''$: $P_{\mathcal{B}\to\mathcal{B}''} = P_{\mathcal{B}\to\mathcal{B}'}\cdot P_{\mathcal{B}'\to\mathcal{B}''}$.

Proof. (i) The transition matrix is the matrix of Id_E relative to $\mathcal{B}'$ (source) and $\mathcal{B}$ (target). Since Id_E is an isomorphism, its matrix is invertible. The inverse is the matrix of Id_E relative to $\mathcal{B}$ and $\mathcal{B}'$, which is $P_{\mathcal{B}'\to\mathcal{B}}$.

(ii) Let $v = \sum_j x'_j\mathbf{e}'_j = \sum_i x_i\,\mathbf{e}_i$. Then $[v]_{\mathcal{B}} = (x_1,\dots,x_n)^{\mathsf{T}}$ and $[v]_{\mathcal{B}'} = (x'_1,\dots,x'_n)^{\mathsf{T}}$. Since $\mathbf{e}'_j = \sum_i p_{ij}\mathbf{e}_i$ where $P=(p_{ij})$, $v = \sum_j x'_j\sum_i p_{ij}\mathbf{e}_i = \sum_i(\sum_j p_{ij}x'_j)\mathbf{e}_i$, giving $x_i = \sum_j p_{ij}x'_j$, i.e., $[v]_{\mathcal{B}} = P[v]_{\mathcal{B}'}$.

(iii) Follows from (i) and the multiplicativity of matrix representations under composition: $\mathrm{Id}_E = \mathrm{Id}_E \circ \mathrm{Id}_E$. □

Theorem 38 (Change-of-basis formula for linear maps)

Let $f \in \mathrm{End}(E)$. Let $\mathcal{B}$ and $\mathcal{B}'$ be bases of E, and let $P = P_{\mathcal{B}\to\mathcal{B}'}$. If $A = \mathcal{M}_{\mathcal{B}}(f)$ and $A' = \mathcal{M}_{\mathcal{B}'}(f)$, then

$$\boxed{A' = P^{-1} A P.}$$

More generally, if $f\colon E \to F$ with bases $\mathcal{B}, \mathcal{B}'$ of E and $\mathcal{C}, \mathcal{C}'$ of F, and $P = P_{\mathcal{B}\to\mathcal{B}'}$, $Q = P_{\mathcal{C}\to\mathcal{C}'}$, then

$$\mathcal{M}_{\mathcal{C}',\mathcal{B}'}(f) = Q^{-1}\,\mathcal{M}_{\mathcal{C},\mathcal{B}}(f)\,P.$$

Proof. We have $f = \mathrm{Id}_F \circ f \circ \mathrm{Id}_E$. Using Theorem 34(iii):

$$\begin{aligned}\mathcal{M}_{\mathcal{C}',\mathcal{B}'}(f) &= \mathcal{M}_{\mathcal{C}',\mathcal{C}'}(\mathrm{Id}_F)\cdot\mathcal{M}_{\mathcal{C}',\mathcal{B}'}(f)\\ &= \mathcal{M}_{\mathcal{C}',\mathcal{C}}(\mathrm{Id}_F)\cdot\mathcal{M}_{\mathcal{C},\mathcal{B}}(f)\cdot\mathcal{M}_{\mathcal{B},\mathcal{B}'}(\mathrm{Id}_E)\\ &= Q^{-1}\cdot A\cdot P.\end{aligned}$$

Here we used $\mathcal{M}_{\mathcal{C}',\mathcal{C}}(\mathrm{Id}_F) = (P_{\mathcal{C}\to\mathcal{C}'})^{-1} = Q^{-1}$ and $\mathcal{M}_{\mathcal{B},\mathcal{B}'}(\mathrm{Id}_E) = P_{\mathcal{B}\to\mathcal{B}'} = P$.

For the special case $E = F$, $\mathcal{B} = \mathcal{C}$, $\mathcal{B}' = \mathcal{C}'$, $P = Q$: $A' = P^{-1}AP$. □

Definition 39 (Similar matrices)

Two matrices $A, A' \in \mathcal{M}_n(\mathbb{K})$ are *similar* if there exists an invertible matrix $P \in \mathrm{GL}_n(\mathbb{K})$ such that $A' = P^{-1}AP$. Similar matrices represent the same endomorphism in different bases.

Example 40 (Change of basis for a projection)

Consider the projection $\pi\colon \mathbb{R}^2 \to \mathbb{R}^2$ onto the x-axis, with canonical matrix $A = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$. In the basis $\mathcal{B}' = ((1,1)^{\mathsf{T}}, (1,-1)^{\mathsf{T}})$, the transition matrix is $P = \left(\begin{smallmatrix}1&1\\1&-1\end{smallmatrix}\right)$, with $P^{-1} = \frac{1}{2}\left(\begin{smallmatrix}1&1\\1&-1\end{smallmatrix}\right)$. Then

$$A' = P^{-1}AP = \frac{1}{2}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1&1\\1&-1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1&1\\0&0\end{pmatrix} = \begin{pmatrix}\frac{1}{2}&\frac{1}{2}\\\frac{1}{2}&\frac{1}{2}\end{pmatrix}.$$

3.11 Operations on matrices

We now consolidate the algebraic operations on matrices, all of which are motivated by the corresponding operations on linear maps.

Definition 41 (Matrix addition and scalar multiplication)

Let $A = (a_{ij})$ and $B = (b_{ij})$ be $m \times n$ matrices over $\mathbb{K}$.

(i) $A + B := (a_{ij} + b_{ij})$.

(ii) $\lambda A := (\lambda\, a_{ij})$ for $\lambda \in \mathbb{K}$.

With these operations, $\mathcal{M}_{m,n}(\mathbb{K})$ is a vector space of dimension mn.

Definition 42 (Matrix multiplication)

Let $A = (a_{ij}) \in \mathcal{M}_{m,n}(\mathbb{K})$ and $B = (b_{jk}) \in \mathcal{M}_{n,p}(\mathbb{K})$. Their product is the matrix $AB = (c_{ik}) \in \mathcal{M}_{m,p}(\mathbb{K})$ where

$$c_{ik} = \sum_{j=1}^{n} a_{ij}\, b_{jk}.$$

This is the "row-by-column" rule: the (i,k)-entry of AB is the dot product of the i-th row of A with the k-th column of B.

Proposition 43 (Properties of matrix multiplication)

(i) **Associativity:** $A(BC) = (AB)C$ (when dimensions match).

(ii) **Distributivity:** $A(B+C) = AB + AC$ and $(A+B)C = AC + BC$.

(iii) **Scalar compatibility:** $\lambda(AB) = (\lambda A)B = A(\lambda B)$.

(iv) **Identity:** $I_m A = A = A I_n$ for $A \in \mathcal{M}_{m,n}(\mathbb{K})$.

(v) **Non-commutativity:** In general, $AB \neq BA$.

Definition 44 (Transpose)

The *transpose* of $A = (a_{ij}) \in \mathcal{M}_{m,n}(\mathbb{K})$ is $A^{\mathsf{T}} = (a_{ji}) \in \mathcal{M}_{n,m}(\mathbb{K})$.

Proposition 45 (Properties of the transpose)

(i) $(A+B)^{\mathsf{T}} = A^{\mathsf{T}} + B^{\mathsf{T}}$.

(ii) $(\lambda A)^{\mathsf{T}} = \lambda\, A^{\mathsf{T}}$.

(iii) $(A^{\mathsf{T}})^{\mathsf{T}} = A$.

(iv) $(AB)^{\mathsf{T}} = B^{\mathsf{T}}\, A^{\mathsf{T}}$ (reversal of order).

Proof. We prove (iv); the others are immediate. Let $A \in \mathcal{M}_{m,n}(\mathbb{K})$, $B \in \mathcal{M}_{n,p}(\mathbb{K})$. The (k,i)-entry of $(AB)^{\mathsf{T}}$ is $(AB)_{ik} = \sum_j a_{ij} b_{jk}$. The (k,i)-entry of $B^{\mathsf{T}} A^{\mathsf{T}}$ is $\sum_j (B^{\mathsf{T}})_{kj} (A^{\mathsf{T}})_{ji} = \sum_j b_{jk}\, a_{ij} = \sum_j a_{ij} b_{jk}$. □

3.12 Inverse matrices

Definition 46 (Invertible matrix)

A square matrix $A \in \mathcal{M}_n(\mathbb{K})$ is *invertible* (or *non-singular*) if there exists a matrix $B \in \mathcal{M}_n(\mathbb{K})$ such that $AB = BA = I_n$. The matrix B is unique and is denoted A^{-1}.

Proposition 47 (Properties of inverses)

Let $A, B \in \mathrm{GL}_n(\mathbb{K})$ (i.e., A and B are invertible).

(i) $(A^{-1})^{-1} = A$.

(ii) $(AB)^{-1} = B^{-1}A^{-1}$ (reversal of order).

(iii) $(A^{\mathsf{T}})^{-1} = (A^{-1})^{\mathsf{T}}$.

(iv) $(\lambda A)^{-1} = \lambda^{-1}A^{-1}$ for $\lambda \neq 0$.

Proof. (ii) We verify: $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$, and similarly $(B^{-1}A^{-1})(AB) = I_n$. The remaining parts are proved similarly. □

Theorem 48 (Invertibility criteria)

For $A \in \mathcal{M}_n(\mathbb{K})$, the following are equivalent:

(i) A is invertible.

(ii) The linear map $x \mapsto Ax$ is an isomorphism of $\mathbb{K}^n$.

(iii) $\operatorname{Ker}(A) = \{\mathbf{0}\}$ (i.e., $Ax = 0$ implies $x = 0$).

(iv) The columns of A form a basis of $\mathbb{K}^n$.

(v) $\operatorname{rank}(A) = n$.

Proof. This follows from Proposition 20 applied to the linear map $f_A \colon \mathbb{K}^n \to \mathbb{K}^n$, $f_A(x) = Ax$. The matrix A is invertible if and only if f_A is bijective (i.e., an isomorphism). The equivalences (ii)–(v) were established in Proposition 20 and the preceding discussion. □

Example 49 (Inverse of a 2×2 matrix)

For $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $ad - bc \neq 0$:

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

3.13 Dual spaces

Definition 50 (Dual space)

Let E be a vector space over $\mathbb{K}$. The *dual space* of E is

$$E^* := \mathcal{L}(E, \mathbb{K}) = \{\, \varphi \colon E \to \mathbb{K} \mid \varphi \text{ is linear} \,\}.$$

Elements of E^* are called *linear forms* (or *covectors* or *linear functionals*).

Example 51 (Linear forms on $\mathbb{R}^n$)

Every linear form on $\mathbb{R}^n$ has the form $\varphi(\mathbf{x}) = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ for some fixed scalars $a_1, \ldots, a_n \in \mathbb{R}$.

Definition 52 (Dual basis)

Let $\mathcal{B} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ be a basis of the finite-dimensional space E. For each $i \in \{1, \dots, n\}$, define the linear form $\mathbf{e}_i^* \in E^*$ by

$$\mathbf{e}_i^*(\mathbf{e}_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

The family $\mathcal{B}^* = (\mathbf{e}_1^*, \dots, \mathbf{e}_n^*)$ is called the *dual basis* of $\mathcal{B}$.

Theorem 53 (The dual basis is a basis of E^*)

If $\dim E = n$, then $\mathcal{B}^*$ is a basis of E^*, and $\dim E^* = n$. Every linear form $\varphi \in E^*$ can be written uniquely as

$$\varphi = \sum_{i=1}^{n} \varphi(\mathbf{e}_i)\, \mathbf{e}_i^*.$$

Proof. Spanning. Let $\varphi \in E^*$ and set $\psi = \sum_{i=1}^{n} \varphi(\mathbf{e}_i)\, \mathbf{e}_i^*$. For each basis vector $\mathbf{e}_j$: $\psi(\mathbf{e}_j) = \sum_i \varphi(\mathbf{e}_i)\, \mathbf{e}_i^*(\mathbf{e}_j) = \sum_i \varphi(\mathbf{e}_i)\, \delta_{ij} = \varphi(\mathbf{e}_j)$. Since φ and ψ agree on a basis, they are equal (Proposition 4).

Linear independence. Suppose $\sum_i \lambda_i\, \mathbf{e}_i^* = 0$ (the zero form). Evaluating at $\mathbf{e}_j$: $\sum_i \lambda_i\, \delta_{ij} = \lambda_j = 0$ for each j. □

Remark 54 (Finite dimension is essential)

In infinite dimension, E^* is generally much larger than E. For instance, if $E = \mathbb{K}[t]$ (polynomials of all degrees), then E^* is not isomorphic to E. The theory of dual spaces becomes significantly richer (and subtler) in that setting.

3.14 Applications

3.14.1 Computer graphics transformations

Every 2D transformation used in computer graphics—translation, rotation, scaling, shearing—can be expressed as a linear map (or, in the case of translations, an *affine* map made linear by *homogeneous coordinates*).

In homogeneous coordinates, a point (x, y) is represented as the triple $(x, y, 1)^{\mathsf{T}}$, and transformations become 3×3 matrices:

$$\underbrace{\begin{pmatrix} \cos\theta & -\sin\theta & t_x \\ \sin\theta & \cos\theta & t_y \\ 0 & 0 & 1 \end{pmatrix}}_{\text{rotate by } \theta, \text{ translate by } (t_x, t_y)} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta + t_x \\ x\sin\theta + y\cos\theta + t_y \\ 1 \end{pmatrix}.$$

Composing transformations corresponds to multiplying their matrices. This is the foundation of the rendering pipeline in OpenGL, DirectX, and every modern graphics system: the entire scene geometry is transformed by chains of matrix multiplications.

3.14.2 Preview: Markov chains

A *Markov chain* models a system that transitions between finitely many states with fixed probabilities. The transition probabilities are encoded in a *stochastic matrix* $P = (p_{ij}) \in \mathcal{M}_n(\mathbb{R})$ where $p_{ij} \geq 0$ and $\sum_j p_{ij} = 1$ for each row i.

If $\mathbf{x}^{(k)} \in \mathbb{R}^n$ is the probability distribution at time step k (a row vector), then

$$\mathbf{x}^{(k+1)} = \mathbf{x}^{(k)} \cdot P.$$

The long-term behavior of the chain is governed by the eigenvalues and eigenvectors of P—a topic we will study in detail in Chapter 6. For now, observe that computing the state after k steps amounts to computing $\mathbf{x}^{(0)} \cdot P^k$, a purely linear-algebraic problem.

3.15 Exercises

Exercise 55 (Verifying linearity)

Which of the following maps are linear? Justify each answer.

(a) $f\colon \mathbb{R}^2 \to \mathbb{R}$, $f(x, y) = 3x - 2y$.

(b) $g\colon \mathbb{R}^2 \to \mathbb{R}$, $g(x, y) = x^2 + y$.

(c) $h\colon \mathbb{R}^3 \to \mathbb{R}^2$, $h(x, y, z) = (x + z,\ 2y - x)$.

(d) $k\colon \mathbb{R}^2 \to \mathbb{R}^2$, $k(x, y) = (x + 1,\ y)$.

Exercise 56 (Kernel and image computation)

Let $f\colon \mathbb{R}^3 \to \mathbb{R}^2$ be defined by $f(x, y, z) = (x + y - z,\ 2x + y + z)$.

(a) Find $\operatorname{Ker} f$ and give a basis.

(b) Find $\operatorname{Im} f$ and determine $\operatorname{rank}(f)$.

(c) Verify the rank–nullity theorem for this map.

Exercise 57 (Matrix of a linear map)

Let $f\colon \mathbb{R}^3 \to \mathbb{R}^2$ be defined by $f(\mathbf{e}_1) = (1, 2)^{\mathsf{T}}$, $f(\mathbf{e}_2) = (0, -1)^{\mathsf{T}}$, $f(\mathbf{e}_3) = (3, 0)^{\mathsf{T}}$ (with respect to the canonical bases). Write down $\mathcal{M}(f)$ and compute $f(1, 1, 1)^{\mathsf{T}}$.

Exercise 58 (Composition and matrix multiplication)

Let $f\colon \mathbb{R}^2 \to \mathbb{R}^3$ and $g\colon \mathbb{R}^3 \to \mathbb{R}^2$ have matrices

$$A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 0 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & 1 \end{pmatrix}.$$

(a) Compute BA and AB.

(b) Which product represents $g \circ f$? Which represents $f \circ g$?

(c) Determine $\operatorname{Ker}(g \circ f)$ and $\operatorname{rank}(g \circ f)$.

Exercise 59 (Change of basis)

Let $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ be defined by $f(x,y) = (3x+y,\ x+3y)$.

(a) Write $\mathcal{M}_{\mathcal{E}}(f)$ in the canonical basis $\mathcal{E}$.

(b) Let $\mathcal{B}' = ((1,1)^{\mathsf{T}}, (1,-1)^{\mathsf{T}})$. Find the transition matrix P from $\mathcal{E}$ to $\mathcal{B}'$.

(c) Compute $\mathcal{M}_{\mathcal{B}'}(f) = P^{-1}\mathcal{M}_{\mathcal{E}}(f)\,P$.

(d) Interpret the result geometrically.

Exercise 60 (Rank–nullity applications)

(a) Let $f\colon \mathbb{R}^5 \to \mathbb{R}^3$ be linear with $\dim(\operatorname{Ker} f) = 2$. What is $\operatorname{rank}(f)$?

(b) Let $g\colon \mathbb{R}^4 \to \mathbb{R}^4$ be linear with $\operatorname{rank}(g) = 3$. What is $\dim(\operatorname{Ker} g)$? Is g surjective?

(c) Prove that there is no surjective linear map from $\mathbb{R}^3$ to $\mathbb{R}^4$.

(d) Prove that there is no injective linear map from $\mathbb{R}^4$ to $\mathbb{R}^3$.

Exercise 61 (Projections)

A linear map $p\colon E \to E$ is called a *projection* if $p \circ p = p$ (idempotent).

(a) Show that $\operatorname{Im} p = \operatorname{Ker}(\mathrm{Id}_E - p)$.

(b) Show that $\operatorname{Ker} p = \operatorname{Im}(\mathrm{Id}_E - p)$.

(c) Deduce that $E = \operatorname{Ker} p \oplus \operatorname{Im} p$.

(d) If $\dim E = n$ and $\operatorname{rank}(p) = r$, show there exists a basis in which $\mathcal{M}(p) = \operatorname{diag}(1,\dots,1,0,\dots,0)$ (r ones).

Exercise 62 (Dual basis computation)

Let $\mathcal{B} = (\mathbf{e}_1, \mathbf{e}_2)$ be the basis of $\mathbb{R}^2$ with $\mathbf{e}_1 = (1,1)^{\mathsf{T}}$, $\mathbf{e}_2 = (1,-1)^{\mathsf{T}}$. Find explicit formulas for $\mathbf{e}_1^*$ and $\mathbf{e}_2^*$ (as functions of the canonical coordinates x_1, x_2).

Exercise 63 (Injectivity and surjectivity)

Let $f\colon E \to F$ and $g\colon F \to G$ be linear maps between finite-dimensional spaces.

(a) Prove: $\operatorname{rank}(g \circ f) \le \min(\operatorname{rank} f, \operatorname{rank} g)$.

(b) Prove the *Sylvester rank inequality*: $\operatorname{rank} f + \operatorname{rank} g - \dim F \le \operatorname{rank}(g \circ f)$. *Hint:* Apply the rank–nullity theorem to the restriction $g|_{\operatorname{Im} f}$.

(c) Deduce: if $g \circ f = 0$, then $\operatorname{rank} f + \operatorname{rank} g \le \dim F$.

Exercise 64 (Nilpotent endomorphisms)

An endomorphism $f \in \mathrm{End}(E)$ is *nilpotent* of index k if $f^k = 0$ but $f^{k-1} \neq 0$.

(a) Show that if f is nilpotent, then f is not invertible.

(b) Show that the chain $\{\mathbf{0}\} \subseteq \operatorname{Ker} f \subseteq \operatorname{Ker} f^2 \subseteq \cdots$ is strictly increasing until it stabilizes at E.

(c) Prove that the nilpotency index satisfies $k \leq \dim E$.

(d) Prove that $\mathrm{Id} + f$ is invertible, and find a formula for $(\mathrm{Id} + f)^{-1}$ in terms of powers of f. *Hint:* geometric series.

Exercise 65 (Linear maps on polynomial spaces)

Let $E = \mathcal{P}_3(\mathbb{R})$ (polynomials of degree ≤ 3) with basis $\mathcal{B} = (1, t, t^2, t^3)$. Define $T : E \to E$ by $T(p)(t) = p(t+1)$.

(a) Verify that T is linear.

(b) Compute the matrix $\mathcal{M}_{\mathcal{B}}(T)$.

(c) Determine $\operatorname{Ker} T$ and $\operatorname{Im} T$. Is T an isomorphism?

(d) Compute T^{-1} and interpret it.

Exercise 66 (The trace as a linear form)

Show that the trace map $\mathrm{tr} : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$, defined by $\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}$, is a linear form. Determine $\mathrm{Ker}(\mathrm{tr})$ and its dimension.

Chapter summary

- A **linear map** $f : E \to F$ preserves addition and scalar multiplication. It is completely determined by its values on a basis (Proposition 4).
- The **kernel** $\operatorname{Ker} f$ and **image** $\operatorname{Im} f$ are subspaces (Theorem 14). The kernel measures "information lost" by f; the image measures "information reached."
- The **rank–nullity theorem** (Theorem 17): $\dim E = \dim(\operatorname{Ker} f) + \operatorname{rank}(f)$.
- A linear map between spaces of equal finite dimension is injective if and only if it is surjective if and only if it is bijective (Proposition 20).
- The set $\mathcal{L}(E, F)$ of all linear maps is itself a vector space of dimension $\dim E \cdot \dim F$ (Theorem 27 and Proposition 28).
- Choosing bases allows us to represent every linear map as a **matrix** (Definition 30). **Composition** of linear maps corresponds to **matrix multiplication** (Theorem 34).
- Under a **change of basis** with transition matrix P, the matrix of an endomorphism transforms as $A' = P^{-1}AP$ (Theorem 38).
- A square matrix is **invertible** if and only if its kernel is trivial, equivalently if and only if its rank equals its size (Theorem 48).

- The **dual space** $E^* = \mathcal{L}(E, \mathbb{K})$ has the same dimension as E in finite dimension, and admits a canonical **dual basis** (Theorem 53).

Chapter 4

Systems of Linear Equations and Gaussian Elimination

Systems of linear equations are among the oldest and most ubiquitous objects in mathematics. They appear whenever several quantities are linked by proportional relationships: currents in an electrical network must satisfy Kirchhoff's laws, prices in a multi-market economic equilibrium are determined by supply-and-demand balances, forces on a bridge truss must cancel for the structure to remain in static equilibrium. Even the modern theory of machine learning ultimately reduces the training of linear models to the solution of (often very large) linear systems.

The algorithmic heart of the subject is *Gaussian elimination*, a systematic procedure that transforms any system into an equivalent one whose solutions can be read off by back-substitution. Despite its simplicity, the algorithm is remarkably powerful: it simultaneously tells us whether a system has solutions, how many free parameters the solution set carries, and provides an explicit parametric description.

In this chapter we formalise systems of linear equations, introduce the matrix language $Ax = b$, develop row reduction to (reduced) echelon form, define the rank of a matrix, and prove the Rouché–Capelli theorem that characterises consistency. We then establish the fundamental structure theorem: the general solution of a consistent system is a translate of the solution space of the associated homogeneous system. Throughout, we provide geometric interpretations and worked examples.

Throughout this chapter, $\mathbb{K}$ denotes a field (typically $\mathbb{R}$ or $\mathbb{C}$), and we freely use results from Chapter 2 and Chapter 3.

4.1 Systems of linear equations

Definition 1 (System of linear equations)

A *system of m linear equations in n unknowns* over a field $\mathbb{K}$ is a collection of equations

$$\begin{cases} a_{11}\,x_1 + a_{12}\,x_2 + \cdots + a_{1n}\,x_n = b_1, \\ a_{21}\,x_1 + a_{22}\,x_2 + \cdots + a_{2n}\,x_n = b_2, \\ \qquad\qquad\qquad\qquad\qquad\quad \vdots \\ a_{m1}\,x_1 + a_{m2}\,x_2 + \cdots + a_{mn}\,x_n = b_m, \end{cases}$$

where $a_{ij} \in \mathbb{K}$ are the *coefficients* and $b_i \in \mathbb{K}$ are the *right-hand sides* (or *constant terms*). A vector $(s_1, \dots, s_n) \in \mathbb{K}^n$ is a *solution* if substituting $x_j = s_j$ satisfies every equation

simultaneously. The *solution set* is

$$\mathcal{S} := \{\, x \in \mathbb{K}^n \mid Ax = b \,\}.$$

4.1.1 Matrix form

The system above can be written compactly as a single matrix equation

$$Ax = b, \tag{4.1}$$

where

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in \mathcal{M}_{m,n}(\mathbb{K}), \qquad x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n, \qquad b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{K}^m.$$

The matrix A is called the *coefficient matrix*. The *augmented matrix* is the $m \times (n+1)$ matrix

$$(A \mid b) := \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right). \tag{4.2}$$

Remark 2 (Column picture)

The equation $Ax = b$ can also be read as asking whether b lies in the column space of A: writing $A = (\mathbf{a}_1 \mid \mathbf{a}_2 \mid \cdots \mid \mathbf{a}_n)$, the system is consistent if and only if

$$b = x_1\,\mathbf{a}_1 + x_2\,\mathbf{a}_2 + \cdots + x_n\,\mathbf{a}_n$$

for some scalars $x_j \in \mathbb{K}$; that is, $b \in \operatorname{Im}(A)$ where we view A as a linear map $\mathbb{K}^n \to \mathbb{K}^m$.

4.2 Homogeneous and non-homogeneous systems

Definition 3 (Homogeneous system)

The system $Ax = b$ is called *homogeneous* if $b = \mathbf{0}$, and *non-homogeneous* (or *inhomogeneous*) otherwise. Given a (possibly non-homogeneous) system $Ax = b$, the system $Ax = \mathbf{0}$ is called its *associated homogeneous system*.

Proposition 4 (The solution set of a homogeneous system is a subspace)

Let $A \in \mathcal{M}_{m,n}(\mathbb{K})$. The solution set of $Ax = \mathbf{0}$ is a vector subspace of $\mathbb{K}^n$. It coincides with $\operatorname{Ker}(A)$, the kernel of the linear map $x \mapsto Ax$.

Proof. The zero vector satisfies $A\mathbf{0} = \mathbf{0}$, so $\mathcal{S}_0 \neq \emptyset$. If $u, v \in \mathcal{S}_0$ and $\lambda \in \mathbb{K}$, then $A(\lambda u + v) = \lambda Au + Av = \lambda\mathbf{0} + \mathbf{0} = \mathbf{0}$, so $\lambda u + v \in \mathcal{S}_0$. By the subspace criterion (Chapter 2), $\mathcal{S}_0$ is a subspace of $\mathbb{K}^n$. By definition, $\mathcal{S}_0 = \{\, x \in \mathbb{K}^n \mid Ax = \mathbf{0} \,\} = \operatorname{Ker}(A)$. □

Proposition 5 (Affine structure of the solution set)

Let $Ax = b$ be a consistent system (i.e. $\mathcal{S} \neq \emptyset$), and let $x_0 \in \mathcal{S}$ be any particular solution. Then

$$\mathcal{S} = x_0 + \operatorname{Ker}(A) := \{\, x_0 + h \mid h \in \operatorname{Ker}(A) \,\}. \tag{4.3}$$

In particular, $\mathcal{S}$ is an *affine subspace* of $\mathbb{K}^n$ of dimension $\dim \operatorname{Ker}(A)$.

Proof. ($\supseteq$) If $h \in \operatorname{Ker}(A)$, then $A(x_0 + h) = Ax_0 + Ah = b + \mathbf{0} = b$, so $x_0 + h \in \mathcal{S}$.

($\subseteq$) If $x \in \mathcal{S}$, set $h := x - x_0$. Then $Ah = Ax - Ax_0 = b - b = \mathbf{0}$, so $h \in \operatorname{Ker}(A)$ and $x = x_0 + h$. □

4.3 Elementary row operations

Definition 6 (Elementary row operations)

The following three operations on the rows of a matrix are called *elementary row operations* (EROs):

(E1) **Row interchange:** Swap rows i and j $\quad (R_i \leftrightarrow R_j)$.

(E2) **Row scaling:** Multiply row i by a non-zero scalar $\lambda \in \mathbb{K}^*$ $\quad (R_i \leftarrow \lambda R_i)$.

(E3) **Row replacement:** Add λ times row j to row i $\quad (R_i \leftarrow R_i + \lambda R_j)$, where $i \neq j$.

Proposition 7 (EROs preserve the solution set)

If the augmented matrix $(A' \mid b')$ is obtained from $(A \mid b)$ by an elementary row operation, then the systems $Ax = b$ and $A'x = b'$ have the same solution set.

Proof. Each ERO is reversible: (E1) is its own inverse; (E2) is reversed by scaling by λ^{-1}; (E3) is reversed by subtracting λ times row j. Hence any solution of one system is a solution of the other. More precisely, each ERO amounts to left-multiplication by an invertible *elementary matrix* $E \in \mathrm{GL}_m(\mathbb{K})$. Since $Ax = b$ if and only if $E(Ax) = Eb$, i.e. $(EA)x = Eb$, the solution set is unchanged. □

Definition 8 (Row equivalence)

Two matrices are *row equivalent* if one can be obtained from the other by a finite sequence of elementary row operations. We write $A \sim A'$.

4.4 Echelon forms

Definition 9 (Row echelon form)

A matrix is in *row echelon form* (REF) if:

(i) All zero rows are at the bottom.

(ii) The first non-zero entry in each non-zero row (called the *pivot*) is strictly to the right of the pivot in the row above.

Definition 10 (Reduced row echelon form)

A matrix is in *reduced row echelon form* (RREF) if it is in REF and, additionally:

(i) Every pivot is equal to 1.

(ii) Each pivot is the only non-zero entry in its column.

Example 11 (Echelon forms)

The following matrix is in row echelon form (pivots are boxed):

$$\begin{pmatrix} \boxed{2} & 3 & -1 & 7 \\ 0 & \boxed{5} & 4 & 2 \\ 0 & 0 & 0 & \boxed{1} \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Its reduced row echelon form is

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

where the $*$ entries are determined by the original entries.

Theorem 12 (Existence and uniqueness of RREF)

Every matrix $A \in \mathcal{M}_{m,n}(\mathbb{K})$ is row equivalent to a unique matrix in reduced row echelon form.

Proof. *Existence* follows from the Gaussian elimination algorithm described in Section 4.5, which produces a REF, followed by Gauss–Jordan elimination (Section 4.6), which produces the RREF.

Uniqueness. Suppose R and R' are two RREFs row equivalent to A. Then R and R' are row equivalent to each other, so they define the same system of homogeneous equations $Rx = \mathbf{0}$ and $R'x = \mathbf{0}$ (by Proposition 7). In particular, their solution sets coincide: $\operatorname{Ker}(R) = \operatorname{Ker}(R')$.

We show $R = R'$ column by column. Let j be any column index. If j is a pivot column of R, say with pivot in row i, then the i-th equation of $Rx = \mathbf{0}$ reads $x_j = -\sum_k r_{ik}\, x_k$ where the sum is over the non-pivot (free) variables. Since $\operatorname{Ker}(R) = \operatorname{Ker}(R')$, column j must also be a pivot column of R' in the same row, and the coefficients must agree. Similarly for non-pivot columns. Hence $R = R'$. □

4.5 Gaussian elimination

Gaussian elimination transforms a matrix into row echelon form using elementary row operations. The algorithm proceeds as follows.

Algorithm (Gaussian elimination).

Step 1. Start with column $j = 1$ and row $i = 1$.

Step 2. *Pivot selection.* In column j, find a non-zero entry in rows $i, i+1, \dots, m$. If none exists, increment j and repeat. If $j > n$, stop.

Step 3. *Swap.* If the non-zero entry is in row $k \neq i$, swap $R_i \leftrightarrow R_k$.

Step 4. *Elimination.* For each row $\ell = i+1, \dots, m$, perform $R_\ell \leftarrow R_\ell - \frac{a_{\ell j}}{a_{ij}} R_i$ to create zeros below the pivot.

Step 5. Increment i and j; go to Step 2.

Example 13 (Gaussian elimination: a 3×4 system)

Solve the system

$$\begin{cases} x_1 + 2x_2 - x_3 + 3x_4 = 5, \\ 2x_1 + 5x_2 + x_3 + 2x_4 = 8, \\ x_1 + 3x_2 + 2x_3 - x_4 = 1. \end{cases}$$

The augmented matrix and its row reduction:

$$\left(\begin{array}{cccc|c} 1 & 2 & -1 & 3 & 5 \\ 2 & 5 & 1 & 2 & 8 \\ 1 & 3 & 2 & -1 & 1 \end{array}\right) \xrightarrow[R_3 \leftarrow R_3 - R_1]{R_2 \leftarrow R_2 - 2R_1} \left(\begin{array}{cccc|c} 1 & 2 & -1 & 3 & 5 \\ 0 & 1 & 3 & -4 & -2 \\ 0 & 1 & 3 & -4 & -4 \end{array}\right)$$

$$\xrightarrow{R_3 \leftarrow R_3 - R_2} \left(\begin{array}{cccc|c} 1 & 2 & -1 & 3 & 5 \\ 0 & 1 & 3 & -4 & -2 \\ 0 & 0 & 0 & 0 & -2 \end{array}\right).$$

The last row reads $0 = -2$, a contradiction. Hence the system is **inconsistent**: $\mathcal{S} = \emptyset$.

Example 14 (A consistent system with free variables)

Solve the system

$$\begin{cases} x_1 + 2x_2 + x_3 = 4, \\ 2x_1 + 5x_2 + 4x_3 = 11, \\ x_1 + 3x_2 + 3x_3 = 7. \end{cases}$$

Row reduction of the augmented matrix:

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 4 \\ 2 & 5 & 4 & 11 \\ 1 & 3 & 3 & 7 \end{array}\right) \xrightarrow[R_3 \leftarrow R_3 - R_1]{R_2 \leftarrow R_2 - 2R_1} \left(\begin{array}{ccc|c} 1 & 2 & 1 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{array}\right) \xrightarrow{R_3 \leftarrow R_3 - R_2} \left(\begin{array}{ccc|c} 1 & 2 & 1 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

The pivot columns are 1 and 2; the variable x_3 is free . Back-substitution gives:

$$x_2 = 3 - 2x_3, \qquad x_1 = 4 - 2x_2 - x_3 = -2 + 3x_3.$$

Setting $x_3 = t \in \mathbb{K}$, the solution set is

$$\mathcal{S} = \left\{ \begin{pmatrix} -2 + 3t \\ 3 - 2t \\ t \end{pmatrix} : t \in \mathbb{K} \right\} = \begin{pmatrix} -2 \\ 3 \\ 0 \end{pmatrix} + t \begin{pmatrix} 3 \\ -2 \\ 1 \end{pmatrix}, \quad t \in \mathbb{K}.$$

This is a line in $\mathbb{K}^3$: a particular solution plus the kernel $\operatorname{Ker}(A) = \operatorname{Span}\left(\begin{pmatrix} 3 \\ -2 \\ 1 \end{pmatrix} \right)$.

4.6 Gauss–Jordan elimination

After reaching row echelon form, *Gauss–Jordan elimination* continues with back-elimination to reach the reduced row echelon form.

Algorithm (Gauss–Jordan: from REF to RREF).

Step 1. Starting from the *bottom-most* pivot, scale its row so the pivot becomes 1.

Step 2. Use this pivot to eliminate all entries *above* it in the same column.

Step 3. Move to the next pivot above and repeat.

Example 15 (Gauss–Jordan continuation)

Continuing from Example 14, we had the REF

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

The pivots are already 1. Eliminate above the second pivot:

$$\xrightarrow{R_1 \leftarrow R_1 - 2R_2} \left(\begin{array}{ccc|c} 1 & 0 & -3 & -2 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

This is the RREF. The solution can be read off directly: $x_1 = -2 + 3x_3$, $x_2 = 3 - 2x_3$, confirming the result of Example 14.

4.7 Rank of a matrix

Definition 16 (Rank via echelon form)

The *rank* of a matrix $A \in \mathcal{M}_{m,n}(\mathbb{K})$, denoted $\operatorname{rank}(A)$, is the number of pivots in any row echelon form of A.

Proposition 17 (Rank is well-defined)

The rank does not depend on which row echelon form is chosen: it equals the number of pivots in the unique RREF of A.

Proof. By Theorem 12, the RREF is unique. Since the number of pivots in any REF equals the number of pivots in the RREF (the Gauss–Jordan steps do not create or destroy pivots), the rank is well-defined. □

Proposition 18 (Rank equals column rank equals row rank)

For any matrix $A \in \mathcal{M}_{m,n}(\mathbb{K})$, the following are equal:

(i) The number of pivots in an echelon form of A.

(ii) $\dim(\operatorname{Im} A)$, i.e. the dimension of the column space of A.

(iii) The dimension of the row space of A.

In particular, $\operatorname{rank}(A) = \operatorname{rank}(A^{\mathsf{T}})$.

Proof. (i)= (ii): The pivot columns of A form a basis for the column space $\operatorname{Im}(A)$ (the corresponding columns of the *original* A, selected via the pivot positions of the RREF, are linearly independent and Span $\operatorname{Im}(A)$). Thus $\dim(\operatorname{Im} A)$ equals the number of pivots.

(i)= (iii): Row operations do not change the row space (each new row is a linear combination of the old rows, and the operation is reversible). The non-zero rows of a REF are linearly independent (by the staircase structure), so they form a basis for the row space. Their count equals the number of pivots. □

Remark 19 (Rank and the rank–nullity theorem)

The rank–nullity theorem (Chapter 3) applied to the linear map $x \mapsto Ax$ gives

$$\operatorname{rank}(A) + \dim \operatorname{Ker}(A) = n, \tag{4.4}$$

where n is the number of columns (i.e. unknowns). Thus the number of free variables in the general solution equals $n - \operatorname{rank}(A)$.

4.8 The Rouché–Capelli theorem

The central consistency criterion is the following classical result.

Theorem 20 (Rouché–Capelli theorem)

The system $Ax = b$ is consistent (i.e. has at least one solution) if and only if

$$\operatorname{rank}(A) = \operatorname{rank}(A \mid b). \tag{4.5}$$

When this condition holds, the dimension of the solution set is $n - \operatorname{rank}(A)$, where n is the number of unknowns. In particular:

- If $\operatorname{rank}(A) = n$, the solution is unique.
- If $\operatorname{rank}(A) < n$, there are infinitely many solutions (assuming $\mathbb{K}$ is infinite), parametrised by $n - \operatorname{rank}(A)$ free variables.

Proof. Write $r = \operatorname{rank}(A)$ and $r' = \operatorname{rank}(A \mid b)$. Since every column of A is also a column of $(A \mid b)$, we always have $r \le r' \le r + 1$.

(⇒) Suppose $\mathcal{S} \neq \emptyset$, say $x_0 \in \mathcal{S}$. Then $b = Ax_0$ is a linear combination of the columns of A, so b lies in the column space of A. Adding the column b to A does not increase the dimension of the column space: $\operatorname{rank}(A \mid b) = \dim \operatorname{Span}(\text{columns of } A, b) = \dim \operatorname{Span}(\text{columns of } A) = \operatorname{rank}(A)$. Hence $r' = r$.

(⇐) Suppose $\operatorname{rank}(A) = \operatorname{rank}(A \mid b)$. Then the column spaces satisfy $\operatorname{Im}(A \mid b) = \operatorname{Im}(A)$, which means b is a linear combination of the columns of A. That is, there exists $x_0 \in \mathbb{K}^n$ with $Ax_0 = b$, so the system is consistent.

The dimension statement follows from Proposition 5 and Eq. (4.4): $\dim \mathcal{S} = \dim \operatorname{Ker}(A) = n - \operatorname{rank}(A)$. □

Corollary 21 (Homogeneous systems always have non-trivial solutions when $n > m$)

If $A \in \mathcal{M}_{m,n}(\mathbb{K})$ with $n > m$ (more unknowns than equations), then $Ax = \mathbf{0}$ has a non-trivial solution.

Proof. We have $\operatorname{rank}(A) \leq m < n$, so $\dim \operatorname{Ker}(A) = n - \operatorname{rank}(A) \geq 1$. □

4.9 Structure of the solution set

We now state and prove the complete structure theorem, synthesising the results of the preceding sections.

Theorem 22 (Structure of the general solution)

Let $A \in \mathcal{M}_{m,n}(\mathbb{K})$ and $b \in \mathbb{K}^m$, and suppose $Ax = b$ is consistent. Let $x_p \in \mathbb{K}^n$ be any particular solution. Then:

(i) $\operatorname{Ker}(A) = \{\, x \in \mathbb{K}^n \mid Ax = \mathbf{0} \,\}$ is a vector subspace of $\mathbb{K}^n$ of dimension $n - \operatorname{rank}(A)$.

(ii) The general solution of $Ax = b$ is

$$\mathcal{S} = \{\, x_p + h \;\big|\; h \in \operatorname{Ker}(A) \,\} = x_p + \operatorname{Ker}(A). \tag{4.6}$$

(iii) If $\{h_1, \dots, h_k\}$ is a basis of $\operatorname{Ker}(A)$ (where $k = n - \operatorname{rank}(A)$), then every solution can be written uniquely as

$$x = x_p + t_1 h_1 + t_2 h_2 + \cdots + t_k h_k, \qquad t_1, \dots, t_k \in \mathbb{K}. \tag{4.7}$$

Proof. (i) follows from Proposition 4 and Eq. (4.4).

(ii) is exactly Proposition 5.

(iii) Since $\{h_1, \dots, h_k\}$ is a basis of $\operatorname{Ker}(A)$, every $h \in \operatorname{Ker}(A)$ can be written uniquely as $h = t_1 h_1 + \cdots + t_k h_k$. Combined with (ii), every $x \in \mathcal{S}$ has the unique representation $x = x_p + t_1 h_1 + \cdots + t_k h_k$. The uniqueness of the t_i follows from the linear independence of the h_i: if $x_p + \sum t_i h_i = x_p + \sum t'_i h_i$, then $\sum (t_i - t'_i) h_i = \mathbf{0}$, forcing $t_i = t'_i$ for all i. □

4.10 Parametric representation of solutions

When solving a system $Ax = b$ by Gaussian elimination, the RREF identifies which variables are *pivot variables* (corresponding to pivot columns) and which are *free variables* (corresponding to non-pivot columns). A parametric representation is obtained by:

1. Expressing each pivot variable in terms of the free variables.
2. Assigning arbitrary parameters $t_1, t_2, \dots$ to the free variables.
3. Writing the general solution as a vector.

Example 23 (Parametric form with two free variables)

Consider the system with RREF

$$\left(\begin{array}{ccccc|c} 1 & 3 & 0 & -2 & 0 & 4 \\ 0 & 0 & 1 & 5 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Pivot variables: x_1, x_3, x_5. Free variables: $x_2 = s$, $x_4 = t$. Reading off:

$$x_1 = 4 - 3s + 2t, \quad x_3 = -1 - 5t, \quad x_5 = 2.$$

The parametric form is

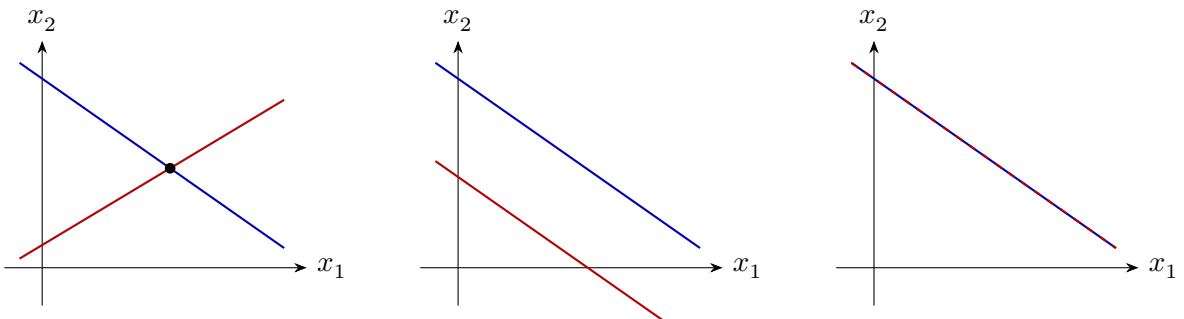
$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \underbrace{\begin{pmatrix} 4 \\ 0 \\ -1 \\ 0 \\ 2 \end{pmatrix}}_{x_p} + s \underbrace{\begin{pmatrix} -3 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}}_{h_1} + t \underbrace{\begin{pmatrix} 2 \\ 0 \\ -5 \\ 1 \\ 0 \end{pmatrix}}_{h_2}, \qquad s, t \in \mathbb{K}.$$

Here $\operatorname{rank}(A) = 3$, $n = 5$, and $\dim \operatorname{Ker}(A) = 5 - 3 = 2$.

4.11 Geometric interpretation

4.11.1 Two equations in two unknowns

A single linear equation $a_1x_1 + a_2x_2 = b$ in two unknowns describes a *line* in $\mathbb{R}^2$. A system of two such equations corresponds to two lines, and the solution set is their intersection.



Unique solution
$\operatorname{rank}(A) = 2$

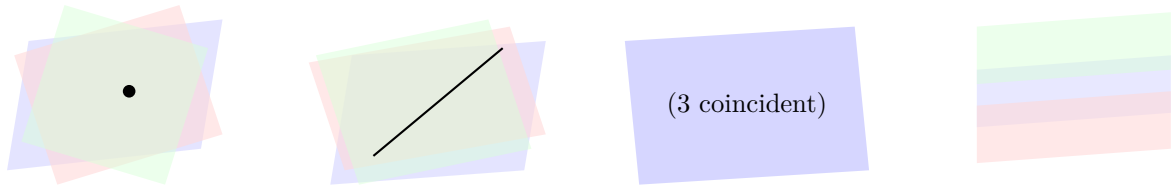
No solution
(parallel lines)

Infinitely many
(coincident lines)

Figure 4.1: Three possibilities for a 2×2 linear system over $\mathbb{R}$.

4.11.2 Three equations in three unknowns

Each equation $a_1x_1 + a_2x_2 + a_3x_3 = b$ describes a *plane* in $\mathbb{R}^3$. A system of three such equations asks for the common intersection of three planes. The possibilities are richer than in $\mathbb{R}^2$.



Unique point | Line | Plane | No solution (parallel planes)

Figure 4.2: Selected configurations for three planes in $\mathbb{R}^3$: unique intersection point, intersection along a line, three coincident planes, and three parallel planes.

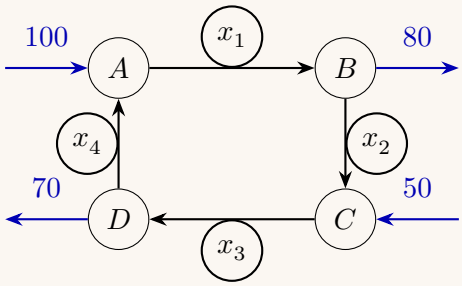
4.12 Applications

4.12.1 Network flows

Consider a network of one-way streets or pipelines with known flow rates entering and leaving the network. At each junction (node), conservation of flow requires that the total flow in equals the total flow out. This yields one linear equation per node.

Example 24 (Traffic flow)

Consider the network with four intersections where external flows are given and the internal flows x_1, x_2, x_3, x_4 are unknown:



Flow conservation at each node:

$$\begin{aligned} A:&\quad 100 + x_4 = x_1, \\ B:&\quad x_1 = 80 + x_2, \\ C:&\quad x_2 + 50 = x_3, \\ D:&\quad x_3 = 70 + x_4. \end{aligned} \qquad \Longleftrightarrow \qquad \begin{aligned} &x_1 - x_4 = 100, \\ &x_1 - x_2 = 80, \\ &x_2 - x_3 = -50, \\ &x_3 - x_4 = 70. \end{aligned}$$

Row reduction shows $\operatorname{rank}(A) = 3$ and $n = 4$, giving one free variable. Setting $x_4 = t$:

$$x_1 = 100 + t, \quad x_2 = 20 + t, \quad x_3 = 70 + t, \quad x_4 = t.$$

Physical constraints ($x_i \geq 0$) require $t \geq 0$.

4.12.2 Electrical circuits

In an electrical circuit, Kirchhoff's current law (KCL) states that the algebraic sum of currents at any node is zero, and Kirchhoff's voltage law (KVL) states that the algebraic sum of voltage drops around any closed loop is zero. Combined with Ohm's law ($V = IR$), these yield a linear system for the unknown currents.

Example 25 (A simple resistive circuit)

Consider a circuit with two loops sharing a branch. Let I_1, I_2, I_3 be the branch currents and $R_1 = 2\,\Omega$, $R_2 = 4\,\Omega$, $R_3 = 6\,\Omega$ the resistances, with a voltage source $V = 12\,\mathrm{V}$. Applying KCL and KVL:

$$\begin{cases} I_1 - I_2 - I_3 = 0 & \text{(KCL at node)},\\ 2I_1 + 6I_3 = 12 & \text{(KVL, loop 1)},\\ 4I_2 - 6I_3 = 0 & \text{(KVL, loop 2)}. \end{cases}$$

Solving by Gaussian elimination gives $I_1 = \frac{36}{11}\,\mathrm{A}$, $I_2 = \frac{18}{11}\,\mathrm{A}$, $I_3 = \frac{18}{11}\cdot\frac{2}{3} = \frac{12}{11}\,\mathrm{A}$.

4.12.3 Preview: least squares

When a system $Ax = b$ is *overdetermined* (more equations than unknowns, typically inconsistent), one seeks the vector $\hat{x}$ that minimises $\|Ax - b\|^2$. A fundamental result (to be proved in the chapter on inner product spaces) states that $\hat{x}$ satisfies the *normal equations*

$$A^{\mathsf{T}} A\,\hat{x} = A^{\mathsf{T}} b. \tag{4.8}$$

This is a (consistent) square linear system, solvable by Gaussian elimination. Least squares is the mathematical foundation of linear regression, signal processing, and data fitting.

4.13 Exercises

Exercise 26 (Row reduction practice)

Reduce the following matrix to RREF and find $\operatorname{rank}(A)$:

$$A = \begin{pmatrix} 1 & 2 & -1 & 0 \\ 2 & 4 & 1 & 3 \\ 3 & 6 & 2 & 5 \end{pmatrix}.$$

Exercise 27 (Solving a 3×3 system)

Solve the system

$$\begin{cases} x + y + z = 6,\\ 2x + 3y + z = 14,\\ x + 2y - z = 2. \end{cases}$$

Exercise 28 (Homogeneous system)

Find the general solution of $Ax = \mathbf{0}$ where

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 1 & 2 & 3 \end{pmatrix}.$$

What is $\dim \operatorname{Ker}(A)$?

Exercise 29 (Consistency conditions)

For which values of $a \in \mathbb{R}$ is the system

$$\begin{cases} x + y = 1, \\ 2x + 2y = a, \end{cases}$$

consistent? When consistent, describe the solution set geometrically.

Exercise 30 (Parametric solutions)

Solve the system and express the solution in parametric vector form:

$$\begin{cases} x_1 + 3x_2 - 2x_3 + x_4 = 4, \\ 2x_1 + 6x_2 - 3x_3 + 5x_4 = 11, \\ x_1 + 3x_2 + x_4 = 5. \end{cases}$$

Identify the particular solution and a basis for the kernel.

Exercise 31 (Rank and the Rouché–Capelli theorem)

Let

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 3 \\ 3 & 6 & 4 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}.$$

Compute $\operatorname{rank}(A)$ and $\operatorname{rank}(A \mid b)$. Is $Ax = b$ consistent? If so, find the solution set.

Exercise 32 (Family of systems)

For which values of $\lambda \in \mathbb{R}$ does the system

$$\begin{cases} x + y + \lambda z = 1, \\ x + \lambda y + z = 1, \\ \lambda x + y + z = 1, \end{cases}$$

have (a) a unique solution, (b) infinitely many solutions, (c) no solution?

Exercise 33 (Network flow)

In a road network with five nodes, the flow conservation equations yield the system

$$\begin{cases} x_1 + x_2 = 200, \\ x_2 + x_3 = 150, \\ x_3 + x_4 = 180, \\ x_4 + x_5 = 120. \end{cases}$$

Find the general solution. If all flows must be non-negative, determine the feasible range for x_1.

Exercise 34 (Computing a kernel basis)

Find a basis for $\operatorname{Ker}(A)$ where

$$A = \begin{pmatrix} 1 & 0 & -2 & 1 & 3 \\ 0 & 1 & 3 & -1 & 0 \\ 2 & 1 & -1 & 1 & 6 \\ 1 & 1 & 1 & 0 & 3 \end{pmatrix}.$$

Verify that $\operatorname{rank}(A) + \dim \operatorname{Ker}(A) = 5$.

Exercise 35 (Rank inequalities)

Let $A \in \mathcal{M}_{m,n}(\mathbb{K})$ and $B \in \mathcal{M}_{n,p}(\mathbb{K})$. Prove:

(a) $\operatorname{rank}(AB) \leq \min(\operatorname{rank}(A), \operatorname{rank}(B))$.

(b) *Sylvester's rank inequality:* $\operatorname{rank}(AB) \geq \operatorname{rank}(A) + \operatorname{rank}(B) - n$.

Hint for (b): use the rank–nullity theorem and show $\operatorname{Ker}(B) \subseteq \operatorname{Ker}(AB)$.

Exercise 36 (Normal equations)

Consider the inconsistent system (three equations, two unknowns):

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix}.$$

(a) Form the normal equations $A^{\mathsf{T}} A\,\hat{x} = A^{\mathsf{T}} b$.

(b) Solve for $\hat{x}$ by Gaussian elimination.

(c) Interpret $\hat{x}$ as the coefficients of the best-fit line $y = x_1 + x_2 t$ through the data points $(1,1)$, $(2,2)$, $(3,4)$.

Exercise 37 (Intersection of subspaces via systems)

Let $U = \operatorname{Span}\left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right)$ and $W = \operatorname{Span}\left(\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right)$ be subspaces of $\mathbb{R}^4$.

(a) Set up a linear system whose solutions describe $U \cap W$.

(b) Solve the system and find a basis for $U \cap W$.

(c) Verify the Grassmann formula: $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$.

Exercise 38 (Proving row equivalence preserves solution sets)

Give a detailed proof that each elementary row operation on the augmented matrix $(A \mid b)$ preserves the solution set of $Ax = b$. Explicitly construct the inverse operation in each case.

Exercise 39 (RREF uniqueness)

Provide a complete proof that two row-equivalent matrices in reduced row echelon form must be identical. *Hint:* proceed by induction on the number of columns, using the fact that the two matrices have identical null spaces.

4.14 Chapter summary

- A **system of linear equations** $Ax = b$ involves a coefficient matrix $A \in \mathcal{M}_{m,n}(\mathbb{K})$, an unknown vector $x \in \mathbb{K}^n$, and a right-hand side $b \in \mathbb{K}^m$.
- **Elementary row operations** (row swap, row scaling, row replacement) transform a system into a row-equivalent one with the same solution set.
- **Gaussian elimination** reduces A to **row echelon form** (REF); **Gauss–Jordan elimination** continues to the unique **reduced row echelon form** (RREF).
- The **rank** $\operatorname{rank}(A)$ is the number of pivots, equal to the dimension of both the column space and the row space.
- **Rouché–Capelli theorem**: $Ax = b$ is consistent $\iff \operatorname{rank}(A) = \operatorname{rank}(A \mid b)$.
- The **general solution** of a consistent system is $\mathcal{S} = x_p + \operatorname{Ker}(A)$, an affine subspace of dimension $n - \operatorname{rank}(A)$.
- **Rank–nullity:** $\operatorname{rank}(A) + \dim \operatorname{Ker}(A) = n$ (number of columns).
- Geometrically, a linear equation in $\mathbb{R}^2$ defines a line, in $\mathbb{R}^3$ a plane; the solution set of a system is the intersection of these geometric objects.
- Applications include network flows, electrical circuits (Kirchhoff's laws), and least squares (normal equations).

Chapter 5

Determinants

How can one tell, by a single number, whether a square matrix is invertible? How can one compute the area of a parallelogram Spanned by two vectors, or the volume of a parallelepiped in $\mathbb{R}^3$? These seemingly different questions are all answered by the same object: the *determinant*.

Consider two vectors $\mathbf{u} = (a, b)$ and $\mathbf{v} = (c, d)$ in $\mathbb{R}^2$. The signed area of the parallelogram they Span is $ad - bc$—precisely the determinant of the matrix whose rows (or columns) are $\mathbf{u}$ and $\mathbf{v}$. This quantity is zero exactly when the two vectors are collinear, i.e. when the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ fails to be invertible. The sign records the *orientation*: positive if $\mathbf{v}$ lies to the left of $\mathbf{u}$, negative otherwise.

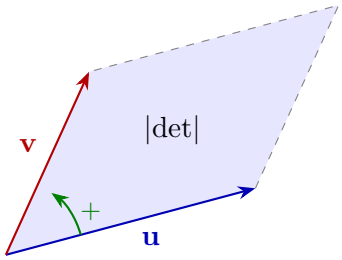


Figure 5.1: The absolute value of $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ gives the area of the parallelogram; the sign encodes orientation.

In this chapter we develop the theory of determinants rigorously. We begin with the combinatorial machinery of permutations and their signatures, define the determinant via the Leibniz formula, establish its fundamental properties, prove cofactor expansion, derive Cramer's rule, and explore geometric interpretations and applications.

Throughout this chapter, $\mathbb{K}$ denotes a field (typically $\mathbb{R}$ or $\mathbb{C}$), and all matrices are square unless stated otherwise. We write $\mathcal{M}_n(\mathbb{K})$ for the space of $n \times n$ matrices with entries in $\mathbb{K}$, and we freely use notation and results from Chapters 2 and 3.

5.1 Permutations and the symmetric group

Definition 1 (Permutation)

A *permutation* of the set $\{1, 2, \dots, n\}$ is a bijection $\sigma \colon \{1, \dots, n\} \to \{1, \dots, n\}$. The set of all such permutations, equipped with composition, is the *symmetric group* $\mathfrak{S}_n$. Its cardinality is $|\mathfrak{S}_n| = n!$.

We use two-line notation and cycle notation interchangeably. For instance, the permutation

$\sigma \in \mathfrak{S}_4$ with $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 3$, $\sigma(4) = 1$ is written

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\ 2\ 4).$$

Definition 2 (Transposition)

A *transposition* is a permutation that exchanges exactly two elements and fixes all others. We write τ_{ij} for the transposition that swaps i and j (with $i \neq j$).

Proposition 3 (Generation by transpositions)

Every permutation $\sigma \in \mathfrak{S}_n$ can be written as a product (composition) of transpositions.

Proof. It suffices to show every cycle decomposes into transpositions, since every permutation is a product of disjoint cycles. Indeed, $(a_1\ a_2\ \cdots\ a_k) = \tau_{a_1 a_k} \circ \tau_{a_1 a_{k-1}} \circ \cdots \circ \tau_{a_1 a_2}$. □

Definition 4 (Inversions and signature)

An *inversion* of $\sigma \in \mathfrak{S}_n$ is a pair (i, j) with $1 \leq i < j \leq n$ and $\sigma(i) > \sigma(j)$. The *signature* (or *sign*) of σ is

$$\operatorname{sgn}(\sigma) := (-1)^{N(\sigma)},$$

where $N(\sigma)$ denotes the number of inversions of σ. Equivalently,

$$\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

A permutation is called *even* if $\operatorname{sgn}(\sigma) = +1$ and *odd* if $\operatorname{sgn}(\sigma) = -1$.

Proposition 5 (Properties of the signature)

For all $\sigma, \tau \in \mathfrak{S}_n$:

(i) $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$.

(ii) $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$.

(iii) Every transposition has signature -1.

(iv) If $\sigma = \tau_1 \circ \cdots \circ \tau_r$ is a product of transpositions, then $\operatorname{sgn}(\sigma) = (-1)^r$. In particular, the parity of r depends only on σ, not on the decomposition.

Proof. Consider the product formula $\operatorname{sgn}(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$.

(iii) Let $\tau = \tau_{pq}$ with $p < q$. In the product $\prod_{i<j}(\tau(j) - \tau(i))$, compared to $\prod_{i<j}(j - i)$, the factor $(q - p)$ changes sign (to $(p - q)$), and for each k strictly between p and q, the two factors involving k and p, and k and q, exchange roles, contributing no net sign change. A careful count shows the total sign is -1.

(i) From the product formula, $\operatorname{sgn}(\sigma\circ\tau) = \prod_{i<j} \frac{(\sigma\circ\tau)(j)-(\sigma\circ\tau)(i)}{j-i}$. Write $j-i = \frac{j-i}{\tau(j)-\tau(i)} \cdot (\tau(j)-\tau(i))$ (since τ is a bijection, the denominator is nonzero when $i < j$), and rearrange to factor the product as $\operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$.

(ii) Follows from (i) applied to $\sigma \circ \sigma^{-1} = \mathrm{Id}$ and $\operatorname{sgn}(\mathrm{Id}) = +1$.

(iv) Follows from (i) and (iii) by induction. □

Example 6 (Signatures in $\mathfrak{S}_3$)

The group $\mathfrak{S}_3$ has $3! = 6$ elements:

σ	Id	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$\operatorname{sgn}(\sigma)$	$+1$	-1	-1	-1	$+1$	$+1$

The three-cycles are even (each is a product of two transpositions: $(1\,2\,3) = (1\,3)(1\,2)$), while the transpositions are odd.

Example 7 (Computing a signature)

Let $\sigma = (1\,3\,5\,2) \in \mathfrak{S}_5$, so $\sigma(1) = 3$, $\sigma(3) = 5$, $\sigma(5) = 2$, $\sigma(2) = 1$, $\sigma(4) = 4$. The inversions are $(1,2), (2,5), (3,5)$, giving $N(\sigma) = 3$. Alternatively, $(1\,3\,5\,2) = (1\,2)(1\,5)(1\,3)$ is a product of 3 transpositions, so $\operatorname{sgn}(\sigma) = (-1)^3 = -1$.

5.2 Definition of the determinant

Definition 8 (Determinant (Leibniz formula))

Let $A = (a_{ij})_{1 \le i,j \le n} \in \mathcal{M}_n(\mathbb{K})$. The *determinant* of A is

$$\det(A) := \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Remark 9 (Small cases)

For $n = 1$: $\det(a) = a$.

For $n = 2$: $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$.

For $n = 3$: $\det \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} = a_1b_2c_3 + a_2b_3c_1 + a_3b_1c_2 - a_3b_2c_1 - a_2b_1c_3 - a_1b_3c_2$, which is the *Sarrus rule*.

5.3 Alternating multilinear characterization

We now give an axiomatic characterization of the determinant. Denote the rows of A by $R_1, \dots, R_n \in \mathbb{K}^n$, so that we may write $\det(A)$ as a function of these row vectors: $\det(A) = D(R_1, \dots, R_n)$.

Definition 10 (Multilinear and alternating)

A function $D \colon (\mathbb{K}^n)^n \to \mathbb{K}$ is:

(i) *multilinear* (in the rows) if for each i, D is linear in the i-th argument with all other arguments fixed:

$$D(R_1, \dots, \alpha R_i + \beta R_i', \dots, R_n) = \alpha\, D(R_1, \dots, R_i, \dots, R_n) + \beta\, D(R_1, \dots, R_i', \dots, R_n).$$

(ii) *alternating* if $D(R_1, \dots, R_n) = 0$ whenever two rows are equal: $R_i = R_j$ for some

$i \neq j$.

Lemma 11 (Alternating implies antisymmetric)

If D is multilinear and alternating, then swapping two rows changes the sign:

$$D(R_1, \dots, R_i, \dots, R_j, \dots, R_n) = -D(R_1, \dots, R_j, \dots, R_i, \dots, R_n).$$

Proof. Expand $D(\dots, R_i + R_j, \dots, R_i + R_j, \dots) = 0$ by multilinearity. Two of the four terms vanish (identical rows), leaving $D(\dots, R_i, \dots, R_j, \dots) + D(\dots, R_j, \dots, R_i, \dots) = 0$. □

Theorem 12 (Uniqueness of the determinant)

The determinant is the unique function $D \colon (\mathbb{K}^n)^n \to \mathbb{K}$ that is:

(i) multilinear in the rows,

(ii) alternating,

(iii) normalized: $D(I_n) = 1$.

Proof. **Existence.** We verify that the Leibniz formula defines a function satisfying (i)–(iii).

Multilinearity: each term $\operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$ is linear in each row R_k (the factor $a_{k,\sigma(k)}$ appears linearly), and the sum of linear functions is linear.

Alternating: suppose $R_p = R_q$ for $p \neq q$. Pair each $\sigma \in \mathfrak{S}_n$ with $\sigma' = \sigma \circ \tau_{pq}$. Then $\operatorname{sgn}(\sigma') = -\operatorname{sgn}(\sigma)$ while $\prod_i a_{i,\sigma'(i)} = \prod_i a_{i,\sigma(i)}$ (since swapping rows p, q with identical entries has no effect on the product). Hence the terms cancel pairwise, giving $D = 0$.

Normalization: for $A = I_n$, $a_{i,\sigma(i)} = \delta_{i,\sigma(i)}$, so the only surviving permutation is $\sigma = \mathrm{Id}$, giving $D(I_n) = \operatorname{sgn}(\mathrm{Id}) \cdot 1 = 1$.

Uniqueness. Let D satisfy (i)–(iii). Write $R_i = \sum_{j=1}^{n} a_{ij}\, \mathbf{e}_j$. By multilinearity,

$$D(R_1, \dots, R_n) = \sum_{j_1, \dots, j_n = 1}^{n} a_{1,j_1} \cdots a_{n,j_n}\, D(\mathbf{e}_{j_1}, \dots, \mathbf{e}_{j_n}).$$

By the alternating property, $D(\mathbf{e}_{j_1}, \dots, \mathbf{e}_{j_n}) = 0$ unless $j_1, \dots, j_n$ are all distinct, i.e. $(j_1, \dots, j_n)$ is a permutation σ. In that case, repeated application of Lemma 11 gives $D(\mathbf{e}_{\sigma(1)}, \dots, \mathbf{e}_{\sigma(n)}) = \operatorname{sgn}(\sigma)\, D(\mathbf{e}_1, \dots, \mathbf{e}_n) = \operatorname{sgn}(\sigma)$. Therefore $D(R_1, \dots, R_n) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$, which is the Leibniz formula. □

5.4 Properties of the determinant

Proposition 13 (Effect of row operations)

Let $A \in \mathcal{M}_n(\mathbb{K})$ with rows $R_1, \dots, R_n$.

(i) **Scaling:** Multiplying row R_i by $\lambda \in \mathbb{K}$ multiplies $\det(A)$ by λ.

(ii) **Swap:** Swapping two rows multiplies $\det(A)$ by -1.

(iii) **Row addition:** Adding a scalar multiple of one row to another does not change $\det(A)$: replacing R_i by $R_i + \lambda R_j$ (with $j \neq i$) leaves det unchanged.

In particular, $\det(\lambda A) = \lambda^n \det(A)$ for all $\lambda \in \mathbb{K}$.

Proof. (i) and (ii) follow immediately from multilinearity and Lemma 11.

(iii) By multilinearity in row i, $D(R_1,\dots,R_i+\lambda R_j,\dots,R_n) = D(R_1,\dots,R_i,\dots,R_n)+\lambda\, D(R_1,\dots,R_j,\dots,R_n)$, where in the second term row j appears in both positions i and j, so the alternating property gives 0. □

Theorem 14 (Determinant of a transpose)

For all $A \in \mathcal{M}_n(\mathbb{K})$, $\det(A^\mathsf{T}) = \det(A)$.

Proof. Denote $B = A^\mathsf{T}$, so $b_{ij} = a_{ji}$. Then

$$\det(B) = \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} b_{i,\sigma(i)} = \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}.$$

Substituting $\tau = \sigma^{-1}$ (a bijection on $\mathfrak{S}_n$ with $\operatorname{sgn}(\tau) = \operatorname{sgn}(\sigma)$), and writing $j = \sigma(i)$ so $i = \tau(j)$:

$$\det(B) = \sum_{\tau\in\mathfrak{S}_n} \operatorname{sgn}(\tau) \prod_{j=1}^{n} a_{j,\tau(j)} = \det(A).$$ □

Remark 15 (Columns behave like rows)

Since $\det(A^\mathsf{T}) = \det(A)$, every property of det stated for rows also holds for columns: the determinant is also multilinear and alternating in the columns.

Theorem 16 (Determinant of a product)

For all $A, B \in \mathcal{M}_n(\mathbb{K})$,

$$\det(AB) = \det(A)\det(B).$$

Proof. Fix $A \in \mathcal{M}_n(\mathbb{K})$ and define $D\colon \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$ by $D(B) = \det(AB)$, viewed as a function of the rows of B.

If B has rows $R_1,\dots,R_n$, then AB has rows $AR_1^\mathsf{T},\dots,AR_n^\mathsf{T}$ (where we view each R_i as a row vector and A acts by left-multiplication after transposing). More precisely, the i-th row of AB is $\sum_{k=1}^{n} b_{ik}\, C_k$, where C_k is the k-th row of A viewed appropriately. Rewriting: the i-th row of AB is a linear function of the i-th row of B.

Hence $B \mapsto \det(AB)$ is multilinear and alternating in the rows of B (since det itself is). By the uniqueness Theorem 12, $D(B) = D(I_n)\cdot\det(B) = \det(A)\cdot\det(B)$. □

Corollary 17 (Determinant of an inverse)

If $A \in \mathrm{GL}_n(\mathbb{K})$, then $\det(A^{-1}) = \frac{1}{\det(A)}$.

Proof. $\det(A)\det(A^{-1}) = \det(AA^{-1}) = \det(I_n) = 1$. □

Proposition 18 (Triangular matrices)

If A is upper or lower triangular, then $\det(A) = \prod_{i=1}^{n} a_{ii}$. In particular, $\det(I_n) = 1$ and $\det(\operatorname{diag}(\lambda_1,\dots,\lambda_n)) = \lambda_1\cdots\lambda_n$.

Proof. In the Leibniz formula, the product $\prod_{i=1}^{n} a_{i,\sigma(i)}$ vanishes unless $\sigma(i) \geq i$ for all i (upper triangular case). The only permutation satisfying this is $\sigma = \mathrm{Id}$, so $\det(A) = \prod_{i=1}^{n} a_{ii}$. □

Proposition 19 (Block triangular matrices)

Let A be a block upper (or lower) triangular matrix:

$$A = \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix},$$

where $A_{11} \in \mathcal{M}_p(\mathbb{K})$ and $A_{22} \in \mathcal{M}_q(\mathbb{K})$ with $p+q=n$. Then $\det(A) = \det(A_{11}) \cdot \det(A_{22})$.

Proof. Fix A_{11} and A_{12}, and consider $D(A_{22}) := \det(A)$ as a function of the rows of A_{22} (these are the last q rows of A). Since the block has zeros below A_{11}, the last q rows of A are $(0, \dots, 0, r_{q,1}, \dots, r_{q,q})$ where $(r_{q,1}, \dots, r_{q,q})$ is a row of A_{22}. By multilinearity and the alternating property of det, D is multilinear and alternating in the rows of A_{22}. Hence $D(A_{22}) = D(I_q) \cdot \det(A_{22})$. But when $A_{22} = I_q$, the matrix A is block upper triangular with $A_{22} = I_q$, and we can row-reduce A_{12} to zero using the last q rows without changing the determinant, obtaining $\det\left(\begin{smallmatrix} A_{11} & 0 \\ 0 & I_q \end{smallmatrix}\right) = \det(A_{11})$. Therefore $D(I_q) = \det(A_{11})$. □

5.5 Cofactor expansion (Laplace expansion)

Definition 20 (Minor and cofactor)

Let $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{K})$. The (i,j)-*minor* of A, denoted M_{ij}, is the determinant of the $(n-1) \times (n-1)$ submatrix obtained by deleting row i and column j. The (i,j)-*cofactor* is

$$C_{ij} := (-1)^{i+j} M_{ij}.$$

Theorem 21 (Laplace expansion)

For any $A \in \mathcal{M}_n(\mathbb{K})$:

(i) **Expansion along row i:** $\det(A) = \sum_{j=1}^{n} a_{ij} C_{ij} = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} M_{ij}$.

(ii) **Expansion along column j:** $\det(A) = \sum_{i=1}^{n} a_{ij} C_{ij} = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} M_{ij}$.

Moreover, expanding along a "foreign" row or column gives zero:

$$\sum_{j=1}^{n} a_{ij} C_{kj} = 0 \quad \text{for } i \neq k, \qquad \sum_{i=1}^{n} a_{ij} C_{ik} = 0 \quad \text{for } j \neq k.$$

Proof. **(i) Expansion along row i.** In the Leibniz formula $\det(A) = \sum_{\sigma} \operatorname{sgn}(\sigma) \prod_{\ell=1}^{n} a_{\ell,\sigma(\ell)}$, group the terms according to the value $\sigma(i) = j$:

$$\det(A) = \sum_{j=1}^{n} a_{ij} \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \sigma(i)=j}} \operatorname{sgn}(\sigma) \prod_{\ell \neq i} a_{\ell,\sigma(\ell)}.$$

We claim that $\sum_{\sigma:\sigma(i)=j} \operatorname{sgn}(\sigma) \prod_{\ell \neq i} a_{\ell,\sigma(\ell)} = (-1)^{i+j} M_{ij}$.

To see this, consider the permutations $\sigma \in \mathfrak{S}_n$ with $\sigma(i) = j$. Any such σ is determined by its restriction to $\{1, \dots, n\} \setminus \{i\}$, which is a bijection onto $\{1, \dots, n\} \setminus \{j\}$. We can identify this

restriction with a permutation $\sigma' \in \mathfrak{S}_{n-1}$ after relabelling: the rows $1, \dots, i-1, i+1, \dots, n$ become $1, \dots, n-1$ and similarly for columns. The relabelling involves moving index i to position n (via $i-1$ adjacent transpositions in the row indices) and index j to position n (via $j-1$ adjacent transpositions in the column indices), contributing a sign of $(-1)^{(n-i)+(n-j)} = (-1)^{i+j}$ (since $(-1)^{2n} = 1$). Thus $\operatorname{sgn}(\sigma) = (-1)^{i+j}\operatorname{sgn}(\sigma')$, and the inner sum becomes $(-1)^{i+j}\det(A_{ij}) = (-1)^{i+j}M_{ij} = C_{ij}$.

(ii) follows from (i) applied to A^{T}, using $\det(A^{\mathsf{T}}) = \det(A)$.

Foreign expansion. Consider $\sum_{j=1}^{n} a_{ij}C_{kj}$ with $i \neq k$. This equals the determinant of the matrix A' obtained from A by replacing row k with row R_i (since the cofactors C_{kj} depend only on the rows other than row k, and the formula gives the expansion of $\det(A')$ along row k). But A' has two identical rows (R_i appears in both positions i and k), so $\det(A') = 0$ by the alternating property. □

Example 22 (3×3 determinant by cofactor expansion)

Compute $\det \begin{pmatrix} 2 & 1 & 3 \\ 0 & -1 & 4 \\ 5 & 2 & 1 \end{pmatrix}$ by expanding along the first column:

$$\det(A) = 2 \cdot (-1)^{1+1} \det \begin{pmatrix} -1 & 4 \\ 2 & 1 \end{pmatrix} + 0 \cdot (-1)^{2+1} \det \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} + 5 \cdot (-1)^{3+1} \det \begin{pmatrix} 1 & 3 \\ -1 & 4 \end{pmatrix}$$
$$= 2(-1-8) + 0 + 5(4+3) = 2(-9) + 5 \cdot 7 = -18 + 35 = 17.$$

5.6 The adjugate matrix and Cramer's rule

Definition 23 (Adjugate (classical adjoint))

The *adjugate* (or *classical adjoint*, or *comatrix*) of $A \in \mathcal{M}_n(\mathbb{K})$ is the $n \times n$ matrix

$$\operatorname{adj}(A) := (C_{ji})_{1 \le i,j \le n} = (\text{cofactor matrix})^{\mathsf{T}},$$

where $C_{ij} = (-1)^{i+j}M_{ij}$ is the (i,j)-cofactor.

Theorem 24 (Adjugate identity)

For all $A \in \mathcal{M}_n(\mathbb{K})$,

$$A \cdot \operatorname{adj}(A) = \operatorname{adj}(A) \cdot A = \det(A) \cdot I_n.$$

Proof. The (i,k)-entry of $A \cdot \operatorname{adj}(A)$ is $\sum_{j=1}^{n} a_{ij}\,[\operatorname{adj}(A)]_{jk} = \sum_{j=1}^{n} a_{ij}\,C_{kj}$. By Theorem 21, this equals $\det(A)$ if $i = k$ and 0 if $i \neq k$ (foreign expansion). Thus $A \cdot \operatorname{adj}(A) = \det(A)\,I_n$. The identity $\operatorname{adj}(A) \cdot A = \det(A)\,I_n$ is proved by considering columns instead of rows (or by applying the row result to A^{T} and transposing). □

Corollary 25 (Inverse via adjugate)

If $\det(A) \neq 0$, then A is invertible and

$$A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A).$$

Theorem 26 (Cramer's rule)

Let $A \in \mathcal{M}_n(\mathbb{K})$ with $\det(A) \neq 0$, and let $b \in \mathbb{K}^n$. The unique solution $x = (x_1, \dots, x_n)^{\mathsf{T}}$ of $Ax = b$ is given by

$$x_j = \frac{\det(A_j)}{\det(A)}, \qquad j = 1, \dots, n,$$

where A_j is the matrix obtained from A by replacing column j with b.

Proof. Since $\det(A) \neq 0$, the system has a unique solution $x = A^{-1}b = \frac{1}{\det(A)} \operatorname{adj}(A)\, b$. The j-th component is

$$x_j = \frac{1}{\det(A)} \sum_{i=1}^{n} C_{ij}\, b_i = \frac{1}{\det(A)} \sum_{i=1}^{n} (-1)^{i+j} M_{ij}\, b_i.$$

But $\sum_{i=1}^{n} (-1)^{i+j} b_i\, M_{ij}$ is precisely the cofactor expansion of $\det(A_j)$ along column j (since column j of A_j is b, and the minors M_{ij} are unchanged). Hence $x_j = \det(A_j)/\det(A)$. □

Example 27 (Cramer's rule in dimension 2)

Solve $\begin{cases} 3x + 2y = 7 \\ x - y = 1 \end{cases}$.

Here $A = \left(\begin{smallmatrix} 3 & 2 \\ 1 & -1 \end{smallmatrix}\right)$, $\det(A) = -3 - 2 = -5$, $\det(A_1) = \det\left(\begin{smallmatrix} 7 & 2 \\ 1 & -1 \end{smallmatrix}\right) = -9$, $\det(A_2) = \det\left(\begin{smallmatrix} 3 & 7 \\ 1 & 1 \end{smallmatrix}\right) = -4$. So $x = \frac{-9}{-5} = \frac{9}{5}$, $y = \frac{-4}{-5} = \frac{4}{5}$.

5.7 Determinant and invertibility

Theorem 28 (Invertibility criterion)

A matrix $A \in \mathcal{M}_n(\mathbb{K})$ is invertible if and only if $\det(A) \neq 0$.

Proof. ($\Rightarrow$) If A is invertible, then $\det(A)\det(A^{-1}) = \det(I_n) = 1$, so $\det(A) \neq 0$.

($\Leftarrow$) If $\det(A) \neq 0$, then by Theorem 24, $A \cdot \frac{1}{\det(A)} \operatorname{adj}(A) = I_n$, so A is invertible (with explicit inverse given by Corollary 25).

Alternatively, if A is not invertible, its columns are linearly dependent: some column is a linear combination of the others. By multilinearity and the alternating property in columns, $\det(A) = 0$. □

Corollary 29 (The general linear group)

$\mathrm{GL}_n(\mathbb{K}) = \{\, A \in \mathcal{M}_n(\mathbb{K}) \mid \det(A) \neq 0 \,\}$. The determinant defines a group homomorphism $\det \colon \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ (where $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ is the multiplicative group of $\mathbb{K}$).

Proof. The first statement is Theorem 28. The multiplicativity $\det(AB) = \det(A)\det(B)$ (Theorem 16) shows that det is a group homomorphism. Its kernel is the *special linear group* $\mathrm{SL}_n(\mathbb{K}) = \{\, A \in \mathrm{GL}_n(\mathbb{K}) \mid \det(A) = 1 \,\}$. □

5.8 Determinant of a linear map

Definition 30 (Determinant of an endomorphism)

Let E be a finite-dimensional $\mathbb{K}$-vector space and $f \in \mathrm{End}(E)$. Choose any basis $\mathcal{B}$ of E and define

$$\det(f) := \det(\mathcal{M}_{\mathcal{B}}(f)).$$

Proposition 31 (Well-definedness)

The determinant $\det(f)$ does not depend on the choice of basis.

Proof. Let $\mathcal{B}$ and $\mathcal{B}'$ be two bases of E, and let P be the change-of-basis matrix from $\mathcal{B}$ to $\mathcal{B}'$. Then $\mathcal{M}_{\mathcal{B}'}(f) = P^{-1}\,\mathcal{M}_{\mathcal{B}}(f)\,P$, so

$$\det(\mathcal{M}_{\mathcal{B}'}(f)) = \det(P^{-1})\det(\mathcal{M}_{\mathcal{B}}(f))\det(P) = \frac{1}{\det(P)}\det(\mathcal{M}_{\mathcal{B}}(f))\det(P) = \det(\mathcal{M}_{\mathcal{B}}(f)). \quad \square$$

Proposition 32 (Properties of det for endomorphisms)

Let E be a finite-dimensional $\mathbb{K}$-vector space and $f, g \in \mathrm{End}(E)$.

(i) $\det(g \circ f) = \det(g)\det(f)$.

(ii) f is an automorphism if and only if $\det(f) \neq 0$.

(iii) $\det(\mathrm{Id}_E) = 1$.

(iv) $\det(\lambda f) = \lambda^n \det(f)$ where $n = \dim E$.

Proof. All properties follow immediately from the corresponding properties of matrix determinants and the identity $\mathcal{M}_{\mathcal{B}}(g \circ f) = \mathcal{M}_{\mathcal{B}}(g) \cdot \mathcal{M}_{\mathcal{B}}(f)$. $\square$

5.9 Geometric interpretation

The determinant has a rich geometric meaning in $\mathbb{R}^n$.

Theorem 33 (Determinant as signed volume)

Let $v_1, \dots, v_n \in \mathbb{R}^n$ be the column vectors of a matrix $A \in \mathcal{M}_n(\mathbb{R})$. Then:

(i) $|\det(A)|$ equals the n-dimensional volume of the parallelepiped $P = \{\, t_1 v_1 + \cdots + t_n v_n \mid 0 \le t_i \le 1 \,\}$.

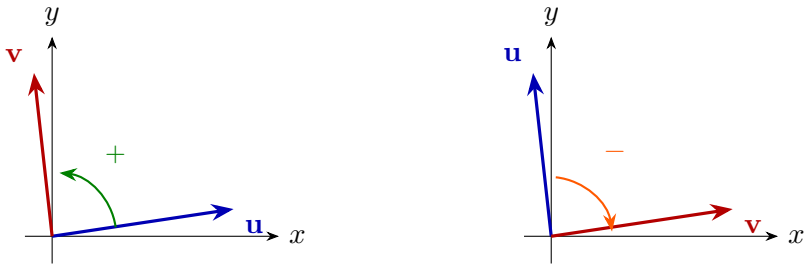
(ii) $\det(A) > 0$ if and only if the ordered basis $(v_1, \dots, v_n)$ has the same orientation as the standard basis.

Proof sketch. (i) Both $|\det|$ and the volume function are multiplicative under composition ($|\det(AB)| = |\det A||\det B|$), agree on elementary matrices (which correspond to elementary row operations with known geometric effects), and every invertible matrix is a product of elementary matrices. For the singular case, both sides equal zero.

(ii) The determinant is a continuous function of the columns. The set of invertible matrices $\mathrm{GL}_n(\mathbb{R})$ has exactly two connected components, distinguished by the sign of det. The identity matrix I_n has $\det = 1 > 0$ and corresponds to the standard orientation. $\square$

2D: parallelogram **3D:** parallelepiped

Figure 5.2: The determinant computes signed areas and volumes.



$\det > 0$ (positive orientation) $\det < 0$ (negative orientation)

Figure 5.3: The sign of the determinant encodes orientation.

5.10 Applications

5.10.1 Cross product in $\mathbb{R}^3$

Definition 34 (Cross product)

For $\mathbf{u} = (u_1, u_2, u_3)$ and $\mathbf{v} = (v_1, v_2, v_3)$ in $\mathbb{R}^3$, the *cross product* is defined (formally) by

$$\mathbf{u} \times \mathbf{v} := \det \begin{pmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{pmatrix} = \begin{pmatrix} u_2 v_3 - u_3 v_2 \\ u_3 v_1 - u_1 v_3 \\ u_1 v_2 - u_2 v_1 \end{pmatrix}.$$

Proposition 35 (Properties of the cross product)

For $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^3$ and $\alpha \in \mathbb{R}$:

(i) **Antisymmetry:** $\mathbf{v} \times \mathbf{u} = -(\mathbf{u} \times \mathbf{v})$.

(ii) **Bilinearity:** $(\alpha \mathbf{u} + \mathbf{w}) \times \mathbf{v} = \alpha(\mathbf{u} \times \mathbf{v}) + \mathbf{w} \times \mathbf{v}$.

(iii) **Orthogonality:** $(\mathbf{u} \times \mathbf{v}) \cdot \mathbf{u} = (\mathbf{u} \times \mathbf{v}) \cdot \mathbf{v} = 0$.

(iv) **Norm:** $\|\mathbf{u} \times \mathbf{v}\|$ equals the area of the parallelogram Spanned by $\mathbf{u}$ and $\mathbf{v}$.

(v) **Scalar triple product:** $(\mathbf{u} \times \mathbf{v}) \cdot \mathbf{w} = \det(\mathbf{u}, \mathbf{v}, \mathbf{w})$ (columns).

Proof. (i)–(ii) follow from properties of the determinant. (iii) If we substitute $\mathbf{u}$ for $\mathbf{w}$ in the triple product $\det(\mathbf{u}, \mathbf{v}, \mathbf{w})$, the matrix has two identical columns, so $\det = 0$. (iv) follows from the identity $\|\mathbf{u} \times \mathbf{v}\|^2 = \|\mathbf{u}\|^2 \|\mathbf{v}\|^2 - (\mathbf{u} \cdot \mathbf{v})^2$ (Lagrange identity). (v) is verified by direct computation: both sides equal $u_1(v_2 w_3 - v_3 w_2) - u_2(v_1 w_3 - v_3 w_1) + u_3(v_1 w_2 - v_2 w_1)$. □

5.10.2 Area and volume formulas

Proposition 36 (Area of a triangle)

The area of a triangle with vertices $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3 = (x_3, y_3)$ in $\mathbb{R}^2$ is

$$\text{Area} = \frac{1}{2}\left|\det \begin{pmatrix} x_2 - x_1 & x_3 - x_1 \\ y_2 - y_1 & y_3 - y_1 \end{pmatrix}\right| = \frac{1}{2}\left|\det \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix}\right|.$$

Proof. The triangle is half the parallelogram Spanned by $\overrightarrow{P_1P_2}$ and $\overrightarrow{P_1P_3}$. The second formula follows by cofactor expansion along the third column of the 3×3 matrix. □

5.10.3 Vandermonde determinant

Theorem 37 (Vandermonde determinant)

For $x_1, \dots, x_n \in \mathbb{K}$,

$$V(x_1, \dots, x_n) := \det \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i).$$

In particular, $V(x_1, \dots, x_n) \neq 0$ if and only if the x_i are pairwise distinct.

Proof. We proceed by induction on n. For $n = 1$, $V(x_1) = 1$ and the empty product is 1. For $n = 2$, $V(x_1, x_2) = x_2 - x_1$.

For the inductive step, subtract x_1 times column $j-1$ from column j, for $j = n, n-1, \dots, 2$ (right to left). This does not change the determinant. Row 1 becomes $(1, 0, 0, \dots, 0)$, and for $i \geq 2$, the entry in row i, column j becomes $x_i^{j-1} - x_1 x_i^{j-2} = x_i^{j-2}(x_i - x_1)$. Expanding along row 1 and factoring out $(x_i - x_1)$ from row i (for $i = 2, \dots, n$):

$$V(x_1, \dots, x_n) = \prod_{i=2}^{n} (x_i - x_1) \cdot V(x_2, \dots, x_n).$$

By the induction hypothesis, $V(x_2, \dots, x_n) = \prod_{2 \le i < j \le n} (x_j - x_i)$, so

$$V(x_1, \dots, x_n) = \prod_{i=2}^{n} (x_i - x_1) \cdot \prod_{2 \le i < j \le n} (x_j - x_i) = \prod_{1 \le i < j \le n} (x_j - x_i).$$ □

Example 38 (Vandermonde for $n = 3$)

$$\det \begin{pmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{pmatrix} = (b - a)(c - a)(c - b).$$

Remark 39 (Application of Vandermonde)

The Vandermonde determinant appears in polynomial interpolation: the system expressing a polynomial of degree $\leq n - 1$ through n points (x_i, y_i) has a unique solution if and only if the x_i are distinct, since the coefficient matrix is the Vandermonde matrix.

5.11 Exercises

Exercise 40 (Determinants of small matrices)

Compute the following determinants:

(a) $\det \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$.

(b) $\det \begin{pmatrix} 2 & -1 & 3 \\ 0 & 4 & 1 \\ 1 & 2 & -1 \end{pmatrix}$.

(c) $\det \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Exercise 41 (Row operations and determinant)

Let $A \in \mathcal{M}_3(\mathbb{R})$ with $\det(A) = 6$. Compute $\det(B)$ where B is obtained from A by:

(a) swapping rows 1 and 3,

(b) multiplying row 2 by -4,

(c) adding 5 times row 1 to row 2,

(d) performing all three operations in sequence.

Exercise 42 (Determinant and scalar multiplication)

Let $A \in \mathcal{M}_n(\mathbb{K})$ with $\det(A) = d$. Express the following in terms of d and n:

(a) $\det(3A)$.

(b) $\det(-A)$.

(c) $\det(A^\mathsf{T})$.

(d) $\det(A^2)$.

Exercise 43 (Determinant of a rank-1 update)

Let $A \in \mathrm{GL}_n(\mathbb{K})$ and let $u, v \in \mathbb{K}^n$ (column vectors). Prove the *matrix determinant lemma*:

$$\det(A + uv^\mathsf{T}) = (1 + v^\mathsf{T} A^{-1} u)\det(A).$$

Hint: Factor $A + uv^\mathsf{T} = A(I + A^{-1}uv^\mathsf{T})$ and compute the determinant of $I + wv^\mathsf{T}$ for a column vector $w = A^{-1}u$.

Exercise 44 (Cofactor expansion practice)

Compute the determinant of

$$A = \begin{pmatrix} 2 & 0 & 1 & 3 \\ 1 & -1 & 0 & 2 \\ 3 & 2 & 0 & 1 \\ 0 & 4 & -1 & 0 \end{pmatrix}$$

by expanding along a row or column of your choice (choose wisely to minimise work).

Exercise 45 (Adjugate of a 2×2 matrix)

For $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, compute $\operatorname{adj}(A)$ and verify that $A \cdot \operatorname{adj}(A) = \det(A)\, I_2$.

Exercise 46 (Cramer's rule application)

Use Cramer's rule to solve the system

$$\begin{cases} x + 2y - z = 3, \\ 2x - y + 3z = 1, \\ 3x + y + 2z = 7. \end{cases}$$

Exercise 47 (Vandermonde determinant)

(a) Compute the Vandermonde determinant $V(1, 2, 3, 4)$.

(b) For which values of $a \in \mathbb{R}$ is the Vandermonde matrix with nodes $1, a, a^2$ singular?

Exercise 48 (Determinant and eigenvalues)

Let $A \in \mathcal{M}_n(\mathbb{K})$.

(a) Show that λ is an eigenvalue of A if and only if $\det(A - \lambda I_n) = 0$.

(b) If A has eigenvalues $\lambda_1, \dots, \lambda_n$ (counted with algebraic multiplicity), prove that $\det(A) = \lambda_1 \cdots \lambda_n$.

Exercise 49 (Determinant of a block diagonal matrix)

Let $A = \operatorname{diag}(A_1, A_2, \dots, A_k)$ be a block diagonal matrix where $A_i \in \mathcal{M}_{n_i}(\mathbb{K})$. Prove that $\det(A) = \det(A_1) \det(A_2) \cdots \det(A_k)$.

Exercise 50 (Antisymmetric matrices)

Let $A \in \mathcal{M}_n(\mathbb{R})$ be *antisymmetric*, i.e. $A^{\mathsf{T}} = -A$.

(a) Show that if n is odd, then $\det(A) = 0$.

(b) Give an example of a 2×2 antisymmetric matrix with $\det(A) \neq 0$.

(c) Show that for even n, $\det(A) \geq 0$. *Hint:* Consider $\det(A) = \det(A^{\mathsf{T}}) = \det(-A)$.

Exercise 51 (Derivative of the determinant)

Let $A(t) = (a_{ij}(t))$ be an $n \times n$ matrix whose entries are differentiable functions of $t \in \mathbb{R}$. Prove *Jacobi's formula*:

$$\frac{d}{dt}\det(A(t)) = \sum_{i=1}^{n} \det(A_1(t), \dots, A_i'(t), \dots, A_n(t)),$$

where $A_i(t)$ denotes the i-th row of $A(t)$ and $A_i'(t)$ its derivative. *Hint:* Use multilinearity of det in the rows and the product rule.

Exercise 52 (Cauchy determinant)

Let $x_1, \dots, x_n$ and $y_1, \dots, y_n$ be elements of a field $\mathbb{K}$ with $x_i + y_j \neq 0$ for all i, j. The *Cauchy matrix* is $C = (c_{ij})$ with $c_{ij} = \frac{1}{x_i + y_j}$. Prove the *Cauchy determinant formula*:

$$\det(C) = \frac{\prod_{1 \le i < j \le n}(x_j - x_i)(y_j - y_i)}{\prod_{i,j=1}^{n}(x_i + y_j)}.$$

Hint: Proceed by induction, reducing to a Vandermonde-type computation.

Exercise 53 (Determinant of the commutator)

Let $A, B \in \mathcal{M}_n(\mathbb{K})$.

(a) Show that if $n = 2$ and $\operatorname{tr}(A) = \operatorname{tr}(B) = 0$, then $\det(AB - BA) \le 0$ when $\mathbb{K} = \mathbb{R}$.

(b) Construct $A, B \in \mathcal{M}_3(\mathbb{R})$ such that $\det(AB - BA) \neq 0$.

(c) Show that for any n, $\operatorname{tr}(AB - BA) = 0$.

Exercise 54 (Polynomial identity for determinants)

Let $A, B \in \mathcal{M}_n(\mathbb{K})$. Show that

$$\det(A + B) + \det(A - B) = 2 \sum_{k \text{ even}} D_k(A, B),$$

where $D_k(A, B)$ is the sum of all determinants obtained by choosing k rows from B and the remaining $n - k$ rows from A (in their original positions). Verify this for $n = 2$ explicitly.

Chapter summary

- A **permutation** of $\{1, \dots, n\}$ is a bijection; the set of all permutations forms the **symmetric group** $\mathfrak{S}_n$ of order $n!$. Every permutation has a well-defined **signature** $\operatorname{sgn}(\sigma) = \pm 1$ (Definition 4).
- The **determinant** of $A \in \mathcal{M}_n(\mathbb{K})$ is defined by the **Leibniz formula** (Definition 8): $\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$.
- The determinant is the *unique* function that is **multilinear**, **alternating** in the rows, and satisfies $\det(I_n) = 1$ (Theorem 12).

- Key **properties**: $\det(A^\mathsf{T}) = \det(A)$ (Theorem 14), $\det(AB) = \det(A)\det(B)$ (Theorem 16), triangular matrices have det $= \prod a_{ii}$ (Proposition 18).
- **Cofactor (Laplace) expansion** computes det by expanding along any row or column (Theorem 21).
- The **adjugate matrix** satisfies $A \cdot \operatorname{adj}(A) = \det(A)\, I_n$ (Theorem 24), yielding the formula $A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)$.
- **Cramer's rule** gives an explicit formula for the solution of $Ax = b$ when $\det(A) \neq 0$ (Theorem 26).
- A is **invertible** if and only if $\det(A) \neq 0$ (Theorem 28).
- The determinant of a **linear map** is well-defined (independent of the choice of basis, Proposition 31).
- **Geometrically**, $|\det(A)|$ is the volume of the parallelepiped Spanned by the columns, and $\operatorname{sgn}(\det)$ encodes orientation (Theorem 33).
- **Applications**: the cross product in $\mathbb{R}^3$, area and volume formulas, and the **Vandermonde determinant** $\prod_{i<j}(x_j - x_i)$ (Theorem 37).

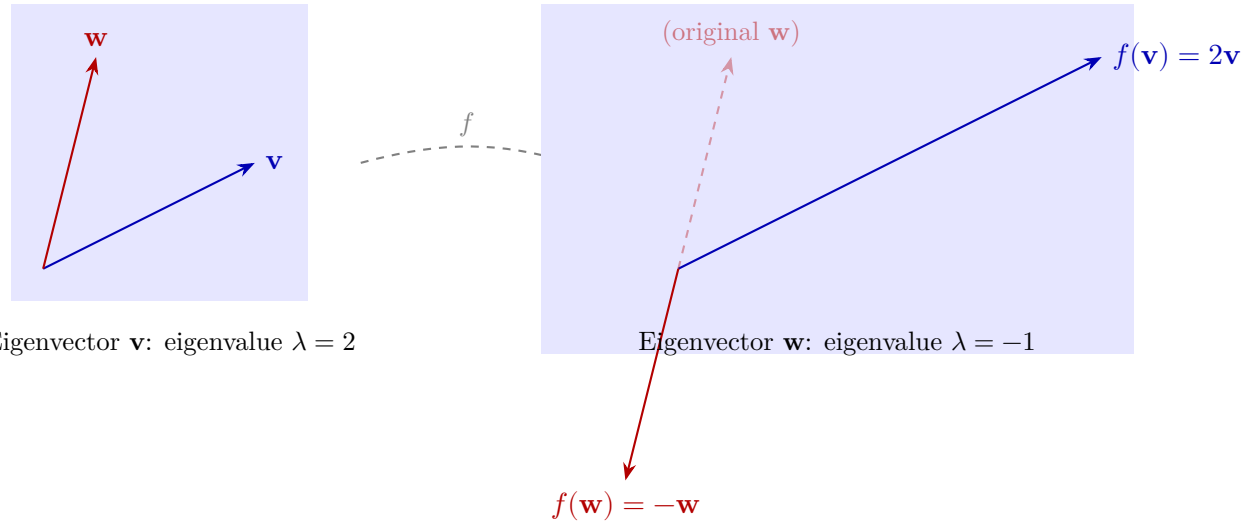
Chapter 6

Eigenvalues, Eigenvectors, and Diagonalization

Among all the questions one can ask about a linear map, perhaps the most fundamental is this: *does there exist a basis in which the map takes a particularly simple form?* The simplest form one can hope for is a diagonal matrix, and the search for such a basis leads directly to the theory of eigenvalues and eigenvectors.

This theory is not merely an exercise in abstraction. Eigenvalues appear throughout mathematics and its applications:

- **Differential equations.** The solutions of a linear system $\mathbf{x}'(t) = A\mathbf{x}(t)$ are determined by the eigenvalues of A; exponential growth, decay, and oscillation all correspond to different eigenvalue configurations.
- **Markov chains.** The long-run behaviour of a stochastic process is governed by the eigenvalue 1 and its eigenvector (the steady-state distribution).
- **Vibrations and resonance.** The natural frequencies of a vibrating string, membrane, or mechanical system are the square roots of the eigenvalues of the associated stiffness matrix.
- **Principal component analysis (PCA).** In statistics and data science, the principal components are the eigenvectors of the covariance matrix, and the eigenvalues measure the variance along each component.



Eigenvector $\mathbf{v}$: eigenvalue $\lambda = 2$

Eigenvector $\mathbf{w}$: eigenvalue $\lambda = -1$

Figure 6.1: An endomorphism acts on eigenvectors by scaling: $\mathbf{v}$ is stretched by factor 2, and $\mathbf{w}$ is flipped (eigenvalue -1).

Throughout this chapter, $\mathbb{K}$ denotes a field (typically $\mathbb{R}$ or $\mathbb{C}$), E denotes a finite-dimensional $\mathbb{K}$-vector space with $\dim E = n$, and $f \in \mathrm{End}(E)$ is an endomorphism of E. We shall use results from Chapter 3 freely, especially the notions of kernel, image, determinant, and matrix representation.

6.1 Eigenvalues and eigenvectors

Definition 1 (Eigenvalue and eigenvector of an endomorphism)

Let $f \in \mathrm{End}(E)$. A scalar $\lambda \in \mathbb{K}$ is called an *eigenvalue* of f if there exists a nonzero vector $v \in E$ such that

$$f(v) = \lambda v.$$

Any such nonzero vector v is called an *eigenvector* of f associated with (or belonging to) the eigenvalue λ.

Remark 2 (The zero vector is never an eigenvector)

By convention, the zero vector is *not* an eigenvector, even though $f(\mathbf{0}) = \lambda\mathbf{0}$ holds for every λ. This convention ensures that the set of eigenvectors associated with a given eigenvalue, together with $\mathbf{0}$, forms a subspace.

Definition 3 (Eigenvalue and eigenvector of a matrix)

Let $A \in \mathcal{M}_n(\mathbb{K})$. A scalar $\lambda \in \mathbb{K}$ is an eigenvalue of A if there exists a nonzero column vector $X \in \mathbb{K}^n$ such that $AX = \lambda X$. Such an X is an eigenvector of A for λ.

Proposition 4 (Reformulation via the kernel)

Let $f \in \mathrm{End}(E)$ and $\lambda \in \mathbb{K}$. Then λ is an eigenvalue of f if and only if

$$\mathrm{Ker}(f - \lambda\,\mathrm{Id}) \neq \{\mathbf{0}\}.$$

Equivalently, for $A \in \mathcal{M}_n(\mathbb{K})$, λ is an eigenvalue of A if and only if $\det(A - \lambda I_n) = 0$.

Proof. We have $f(v) = \lambda v$ if and only if $(f - \lambda\,\mathrm{Id})(v) = \mathbf{0}$, i.e. $v \in \mathrm{Ker}(f - \lambda\,\mathrm{Id})$. A nonzero such v exists precisely when $\mathrm{Ker}(f - \lambda\,\mathrm{Id}) \neq \{\mathbf{0}\}$, which is equivalent to $f - \lambda\,\mathrm{Id}$ being non-injective, hence non-invertible (in finite dimension). For a matrix A this means $\det(A - \lambda I_n) = 0$. □

Example 5 (Eigenvalues of a 2×2 matrix)

Let $A = \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix}$. We solve $\det(A - \lambda I_2) = 0$:

$$\det \begin{pmatrix} 3-\lambda & 1 \\ 0 & 2-\lambda \end{pmatrix} = (3-\lambda)(2-\lambda) = 0,$$

so $\lambda_1 = 3$ and $\lambda_2 = 2$.

For $\lambda_1 = 3$: $(A - 3I_2)X = \mathbf{0}$ gives $\begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \mathbf{0}$, hence $y = 0$ and x is free. An

eigenvector is $\binom{1}{0}$.

For $\lambda_2 = 2$: $(A - 2I_2)X = \mathbf{0}$ gives $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \mathbf{0}$, hence $x = -y$. An eigenvector is $\binom{-1}{1}$.

Proposition 6 (Eigenvectors for distinct eigenvalues are linearly independent)

Let $f \in \mathrm{End}(E)$ and let $\lambda_1, \dots, \lambda_r$ be pairwise distinct eigenvalues of f, with associated eigenvectors $v_1, \dots, v_r$. Then $(v_1, \dots, v_r)$ is linearly independent.

Proof. By induction on r. The case $r = 1$ is clear since $v_1 \neq \mathbf{0}$.

Suppose the result holds for $r-1$ eigenvalues and consider a relation $\sum_{i=1}^{r} \alpha_i v_i = \mathbf{0}$. Apply f:

$$\sum_{i=1}^{r} \alpha_i \lambda_i v_i = \mathbf{0}.$$

Subtract λ_r times the original relation:

$$\sum_{i=1}^{r-1} \alpha_i (\lambda_i - \lambda_r) v_i = \mathbf{0}.$$

By the induction hypothesis, $\alpha_i(\lambda_i - \lambda_r) = 0$ for all $i = 1, \dots, r-1$. Since the eigenvalues are distinct, $\lambda_i - \lambda_r \neq 0$, so $\alpha_i = 0$ for $i = 1, \dots, r-1$. Substituting back gives $\alpha_r v_r = \mathbf{0}$, whence $\alpha_r = 0$. □

Corollary 7 (Bound on the number of eigenvalues)

An endomorphism of an n-dimensional space has at most n distinct eigenvalues.

Proof. If there were $n+1$ distinct eigenvalues, the corresponding eigenvectors would form a linearly independent family of $n+1$ vectors in an n-dimensional space, contradicting the definition of dimension. □

6.2 Eigenspaces

Definition 8 (Eigenspace)

Let $f \in \mathrm{End}(E)$ and $\lambda \in \mathbb{K}$ be an eigenvalue of f. The *eigenspace* of f associated with λ is

$$E_\lambda(f) := \mathrm{Ker}(f - \lambda \,\mathrm{Id}) = \{\, v \in E \mid f(v) = \lambda v \,\}.$$

For a matrix $A \in \mathcal{M}_n(\mathbb{K})$, we write $E_\lambda(A) = \mathrm{Ker}(A - \lambda I_n)$.

Proposition 9 (Eigenspaces are subspaces)

For every eigenvalue λ of f, the eigenspace $E_\lambda(f)$ is a vector subspace of E of dimension at least 1.

Proof. Since $f - \lambda \,\mathrm{Id}$ is a linear map, its kernel $\mathrm{Ker}(f - \lambda \,\mathrm{Id})$ is a subspace of E (the kernel of any linear map is a subspace). It contains at least one nonzero vector (the eigenvector guaranteed by the definition of eigenvalue), so $\dim E_\lambda(f) \geq 1$. □

Proposition 10 (Sum of eigenspaces is direct)

Let $\lambda_1, \dots, \lambda_r$ be pairwise distinct eigenvalues of f. Then the sum $E_{\lambda_1}(f) + \cdots + E_{\lambda_r}(f)$ is a direct sum:

$$E_{\lambda_1}(f) + \cdots + E_{\lambda_r}(f) = E_{\lambda_1}(f) \oplus \cdots \oplus E_{\lambda_r}(f).$$

Proof. Suppose $v_1 + \cdots + v_r = \mathbf{0}$ with $v_i \in E_{\lambda_i}(f)$. We must show each $v_i = \mathbf{0}$. If some $v_i \neq \mathbf{0}$, let $S = \{\, i \mid v_i \neq \mathbf{0} \,\}$. Then the nonzero vectors $(v_i)_{i \in S}$ are eigenvectors for pairwise distinct eigenvalues, hence linearly independent by Proposition 6. But $\sum_{i \in S} v_i = \mathbf{0}$ (the terms with $v_i = \mathbf{0}$ contribute nothing), contradicting linear independence. Therefore $S = \emptyset$ and all $v_i = \mathbf{0}$. □

6.3 Characteristic polynomial

Definition 11 (Characteristic polynomial of a matrix)

Let $A \in \mathcal{M}_n(\mathbb{K})$. The *characteristic polynomial* of A is

$$\chi_A(\lambda) := \det(A - \lambda I_n) \in \mathbb{K}[\lambda].$$

It is a polynomial of degree n in λ.

Remark 12 (Sign convention)

Some authors define $\chi_A(\lambda) = \det(\lambda I_n - A)$ instead, which differs from our convention by a factor of $(-1)^n$. With our convention, the leading term is $(-1)^n \lambda^n$; with the other convention it is λ^n. Both conventions are standard. The eigenvalues (roots of χ_A) are the same either way.

Proposition 13 (Properties of the characteristic polynomial)

Let $A \in \mathcal{M}_n(\mathbb{K})$ with characteristic polynomial $\chi_A(\lambda) = (-1)^n \lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_0$. Then:

(i) $\deg \chi_A = n$ and the leading coefficient is $(-1)^n$.

(ii) $c_{n-1} = (-1)^{n-1} \operatorname{tr}(A)$.

(iii) $c_0 = \chi_A(0) = \det(A)$.

(iv) The eigenvalues of A are exactly the roots of χ_A in $\mathbb{K}$.

(v) Similar matrices have the same characteristic polynomial: if $B = P^{-1}AP$ then $\chi_B = \chi_A$.

Proof. (i) The determinant of $A - \lambda I_n$ is a sum over permutations $\sigma \in S_n$ of products $\prod_{i=1}^{n} (A - \lambda I_n)_{i,\sigma(i)}$. The only permutation contributing a term of degree n is the identity $\sigma = \mathrm{Id}$, which gives $\prod_{i=1}^{n} (a_{ii} - \lambda)$. The leading term is $(-\lambda)^n = (-1)^n \lambda^n$.

(ii) In the expansion of $\prod_{i=1}^{n} (a_{ii} - \lambda)$, the coefficient of λ^{n-1} is $(-1)^{n-1} \sum_{i=1}^{n} a_{ii} = (-1)^{n-1} \operatorname{tr}(A)$. No other permutation contributes a term of degree $n-1$ (such a permutation would need at least two non-diagonal factors, each of degree 0 in λ, leaving degree at most $n-2$).

(iii) $\chi_A(0) = \det(A - 0 \cdot I_n) = \det(A)$.

(iv) λ is an eigenvalue if and only if $\det(A - \lambda I_n) = 0$, i.e. $\chi_A(\lambda) = 0$.

(v) $\chi_B(\lambda) = \det(P^{-1}AP - \lambda I_n) = \det(P^{-1}(A - \lambda I_n)P) = \det(P^{-1})\det(A - \lambda I_n)\det(P) = \chi_A(\lambda)$. □

Definition 14 (Characteristic polynomial of an endomorphism)

Let $f \in \mathrm{End}(E)$ and let $A = \mathcal{M}_{\mathcal{B}}(f)$ be the matrix of f in some basis $\mathcal{B}$ of E. The *characteristic polynomial* of f is

$$\chi_f(\lambda) := \chi_A(\lambda) = \det(A - \lambda I_n).$$

By property (v) above, this is independent of the choice of basis $\mathcal{B}$.

Example 15 (Characteristic polynomial of a 2×2 matrix)

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then

$$\chi_A(\lambda) = \det \begin{pmatrix} a-\lambda & b \\ c & d-\lambda \end{pmatrix} = (a-\lambda)(d-\lambda) - bc = \lambda^2 - (a+d)\lambda + (ad-bc) = \lambda^2 - \mathrm{tr}(A)\lambda + \det(A).$$

Example 16 (Characteristic polynomial of a 3×3 matrix)

Let $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 2 \end{pmatrix}$. Then

$$\begin{aligned} \chi_A(\lambda) &= \det \begin{pmatrix} 2-\lambda & 1 & 0 \\ 0 & 3-\lambda & 1 \\ 0 & 0 & 2-\lambda \end{pmatrix} \\ &= (2-\lambda)(3-\lambda)(2-\lambda) \\ &= (2-\lambda)^2(3-\lambda) = -(\lambda-2)^2(\lambda-3). \end{aligned}$$

The eigenvalues are $\lambda_1 = 2$ (a double root) and $\lambda_2 = 3$ (a simple root).

6.4 The Cayley–Hamilton theorem

Theorem 17 (Cayley–Hamilton)

Let $A \in \mathcal{M}_n(\mathbb{K})$ with characteristic polynomial χ_A. Then

$$\chi_A(A) = 0_{n \times n}.$$

That is, every square matrix satisfies its own characteristic polynomial. Equivalently, if $f \in \mathrm{End}(E)$, then $\chi_f(f) = 0$ (the zero endomorphism).

Proof. Write $B(\lambda) := \mathrm{adj}(A - \lambda I_n)$ for the classical adjoint (adjugate) of $A - \lambda I_n$. By the adjugate formula for determinants,

$$(A - \lambda I_n)\, B(\lambda) = \det(A - \lambda I_n)\, I_n = \chi_A(\lambda)\, I_n.$$

Each entry of $B(\lambda)$ is a cofactor of $A - \lambda I_n$, hence a polynomial in λ of degree at most $n-1$. We can therefore write

$$B(\lambda) = B_0 + B_1\lambda + B_2\lambda^2 + \cdots + B_{n-1}\lambda^{n-1},$$

where $B_0, B_1, \ldots, B_{n-1} \in \mathcal{M}_n(\mathbb{K})$ are constant matrices. Similarly, write the characteristic polynomial as

$$\chi_A(\lambda) = c_0 + c_1\lambda + c_2\lambda^2 + \cdots + c_n\lambda^n,$$

where $c_n = (-1)^n$.

Now expand the identity $(A - \lambda I_n)\, B(\lambda) = \chi_A(\lambda)\, I_n$:

$$\begin{aligned} AB_0 &= c_0 I_n, \\ AB_1 - B_0 &= c_1 I_n, \\ AB_2 - B_1 &= c_2 I_n, \\ &\vdots \\ AB_{n-1} - B_{n-2} &= c_{n-1} I_n, \\ -B_{n-1} &= c_n I_n. \end{aligned}$$

Multiply the k-th equation (from $k=0$ to $k=n$) on the left by A^k and sum:

$$\begin{aligned} &A^0(AB_0) + A^1(AB_1 - B_0) + A^2(AB_2 - B_1) + \cdots + A^n(-B_{n-1}) \\ &= c_0 I_n + c_1 A + c_2 A^2 + \cdots + c_n A^n \\ &= \chi_A(A). \end{aligned}$$

On the left-hand side, all terms cancel telescopically:

$$AB_0 + A^2B_1 - AB_0 + A^3B_2 - A^2B_1 + \cdots - A^nB_{n-1} = 0_{n\times n}.$$

Therefore $\chi_A(A) = 0_{n\times n}$. □

Remark 18 (Warning about "substituting A for λ")

One cannot prove Cayley–Hamilton by simply writing "$\chi_A(A) = \det(A - A\cdot I_n) = \det(0) = 0$." This is *fallacious*: $\chi_A(\lambda)$ is a polynomial in the *scalar* λ, while the substitution $\lambda = A$ places a *matrix* inside a determinant in an invalid way. The correct proof, as given above, requires careful bookkeeping with matrix polynomials.

Example 19 (Cayley–Hamilton for a 2×2 matrix)

Take $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. Then $\chi_A(\lambda) = \lambda^2 - 5\lambda - 2$. We verify:

$$A^2 - 5A - 2I_2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix} - \begin{pmatrix} 5 & 10 \\ 15 & 20 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

6.5 Spectrum of an endomorphism

Definition 20 (Spectrum)

The *spectrum* of an endomorphism $f \in \mathrm{End}(E)$ (or of a matrix $A \in \mathcal{M}_n(\mathbb{K})$) is the set of all its eigenvalues:

$$\mathrm{Spec}(f) := \{\, \lambda \in \mathbb{K} \mid \lambda \text{ is an eigenvalue of } f \,\}.$$

Remark 21 (Dependence on the base field)

The spectrum depends on the base field. For example, the rotation matrix $R_{\pi/2} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ has $\chi_{R_{\pi/2}}(\lambda) = \lambda^2+1$, which has no real roots, so $\mathrm{Spec}_{\mathbb{R}}(R_{\pi/2}) = \emptyset$. Over $\mathbb{C}$, $\mathrm{Spec}_{\mathbb{C}}(R_{\pi/2}) = \{i, -i\}$.

6.6 Algebraic and geometric multiplicity

Definition 22 (Algebraic multiplicity)

Let λ be an eigenvalue of f. The *algebraic multiplicity* of λ, denoted $m_a(\lambda)$, is the multiplicity of λ as a root of the characteristic polynomial χ_f. In other words, $m_a(\lambda)$ is the largest integer k such that $(\lambda_0 - \lambda)^k$ divides $\chi_f(\lambda_0)$, where we view χ_f as a polynomial in the variable λ_0.

Definition 23 (Geometric multiplicity)

The *geometric multiplicity* of an eigenvalue λ, denoted $m_g(\lambda)$, is the dimension of the eigenspace:

$$m_g(\lambda) := \dim E_\lambda(f) = \dim \mathrm{Ker}(f - \lambda\,\mathrm{Id}).$$

Theorem 24 (Inequality between multiplicities)

For every eigenvalue λ of f,

$$1 \le m_g(\lambda) \le m_a(\lambda).$$

Proof. The inequality $m_g(\lambda) \ge 1$ holds because $E_\lambda(f)$ contains at least one nonzero eigenvector.

For the inequality $m_g(\lambda) \le m_a(\lambda)$, let $d = m_g(\lambda) = \dim E_\lambda(f)$ and choose a basis $(v_1, \dots, v_d)$ of $E_\lambda(f)$. Extend it to a basis $\mathcal{B} = (v_1, \dots, v_d, v_{d+1}, \dots, v_n)$ of E. In this basis, the matrix of f has the block form

$$\mathcal{M}_{\mathcal{B}}(f) = \begin{pmatrix} \lambda I_d & C \\ 0 & D \end{pmatrix},$$

where $C \in \mathcal{M}_{d,n-d}(\mathbb{K})$ and $D \in \mathcal{M}_{n-d}(\mathbb{K})$. This is because $f(v_i) = \lambda v_i$ for $i = 1, \dots, d$. Then

$$\chi_f(\mu) = \det \begin{pmatrix} \lambda I_d - \mu I_d & C \\ 0 & D - \mu I_{n-d} \end{pmatrix} = (\lambda - \mu)^d \det(D - \mu I_{n-d}).$$

Therefore $(\lambda - \mu)^d$ divides $\chi_f(\mu)$, which means $m_a(\lambda) \ge d = m_g(\lambda)$. □

Example 25 (Strict inequality between multiplicities)

The matrix $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ has $\chi_A(\lambda) = (2-\lambda)^2$, so $\lambda = 2$ has algebraic multiplicity

$m_a(2) = 2$. However, $E_2(A) = \operatorname{Ker}\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \operatorname{Span}\left(\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)\right)$, which has dimension 1. So $m_g(2) = 1 < 2 = m_a(2)$.

6.7 Diagonalizability

Definition 26 (Diagonalizable endomorphism)

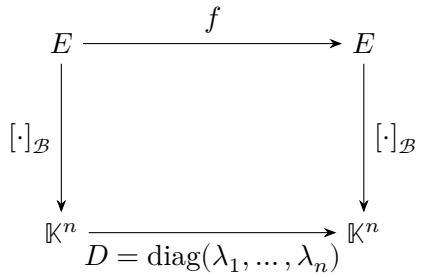
An endomorphism $f \in \operatorname{End}(E)$ is *diagonalizable* if there exists a basis of E consisting entirely of eigenvectors of f. Equivalently, f is diagonalizable if its matrix in some basis is diagonal.

Definition 27 (Diagonalizable matrix)

A matrix $A \in \mathcal{M}_n(\mathbb{K})$ is *diagonalizable* if it is similar to a diagonal matrix, i.e. if there exists an invertible matrix $P \in \mathrm{GL}_n(\mathbb{K})$ and a diagonal matrix $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$ such that

$$A = PDP^{-1}.$$

The columns of P are eigenvectors of A, and the diagonal entries of D are the corresponding eigenvalues.



In the eigenbasis $\mathcal{B}$, the map f acts as multiplication by λ_i on each coordinate axis.

Figure 6.2: Diagonalization: in the eigenbasis $\mathcal{B}$, the endomorphism f is represented by the diagonal matrix D.

Theorem 28 (Diagonalization criterion)

Let $f \in \operatorname{End}(E)$ with $\dim E = n$, and let $\operatorname{Spec}(f) = \{\lambda_1, \dots, \lambda_r\}$. The following conditions are equivalent:

(i) f is diagonalizable.

(ii) $E = E_{\lambda_1}(f) \oplus E_{\lambda_2}(f) \oplus \cdots \oplus E_{\lambda_r}(f)$.

(iii) $\sum_{i=1}^{r} \dim E_{\lambda_i}(f) = n$.

(iv) The characteristic polynomial χ_f splits over $\mathbb{K}$ (i.e. has all its roots in $\mathbb{K}$), *and* $m_g(\lambda_i) = m_a(\lambda_i)$ for every eigenvalue λ_i.

Proof. **(i) ⇒ (ii).** If f is diagonalizable, there is a basis $(v_1, \dots, v_n)$ of E with $f(v_j) = \mu_j v_j$ for some $\mu_j \in \mathbb{K}$. Each v_j belongs to $E_{\mu_j}(f)$. Since the v_j Span E, we have $E = \sum_{i=1}^{r} E_{\lambda_i}(f)$. This sum is direct by Proposition 10.

(ii) ⇒ (iii). If the direct sum decomposition holds, then $n = \dim E = \sum_{i=1}^{r} \dim E_{\lambda_i}(f)$ by the dimension formula for direct sums.

(iii) ⇒ (iv). From $\sum m_g(\lambda_i) = n$ and the inequality $m_g(\lambda_i) \leq m_a(\lambda_i)$ for each i, together with $\sum m_a(\lambda_i) \leq n$ (the sum of algebraic multiplicities is at most $\deg \chi_f = n$), we get

$$n = \sum_{i=1}^{r} m_g(\lambda_i) \leq \sum_{i=1}^{r} m_a(\lambda_i) \leq n.$$

All inequalities are equalities. In particular, $m_g(\lambda_i) = m_a(\lambda_i)$ for each i, and $\sum m_a(\lambda_i) = n$, which means χ_f splits over $\mathbb{K}$ (every root is in $\mathbb{K}$ and the multiplicities account for the full degree n).

(iv) ⇒ (i). If χ_f splits and $m_g(\lambda_i) = m_a(\lambda_i)$ for each i, then

$$\sum_{i=1}^{r} \dim E_{\lambda_i}(f) = \sum_{i=1}^{r} m_g(\lambda_i) = \sum_{i=1}^{r} m_a(\lambda_i) = n.$$

Since the sum of eigenspaces is direct (Proposition 10), we have $E = \bigoplus_{i=1}^{r} E_{\lambda_i}(f)$. Choosing a basis for each $E_{\lambda_i}(f)$ and concatenating gives a basis of E consisting of eigenvectors, so f is diagonalizable. □

Corollary 29 (Endomorphism with n distinct eigenvalues)

If $f \in \mathrm{End}(E)$ has $n = \dim E$ distinct eigenvalues, then f is diagonalizable.

Proof. Each eigenvalue has algebraic multiplicity 1 (since there are n eigenvalues and $\deg \chi_f = n$), and the geometric multiplicity satisfies $1 \leq m_g(\lambda) \leq m_a(\lambda) = 1$. Thus $m_g = m_a$ for all eigenvalues and χ_f splits, so f is diagonalizable by Theorem 28. □

Remark 30 (The converse is false)

Having n distinct eigenvalues is sufficient but not necessary for diagonalizability. For instance, the identity matrix I_n is diagonal (hence diagonalizable) but has a single eigenvalue $\lambda = 1$ with multiplicity n.

6.8 The diagonalization algorithm

Given $A \in \mathcal{M}_n(\mathbb{K})$, the following procedure determines whether A is diagonalizable and, if so, produces P and D such that $A = PDP^{-1}$.

Step 1. Compute the characteristic polynomial $\chi_A(\lambda) = \det(A - \lambda I_n)$.

Step 2. Find the eigenvalues by solving $\chi_A(\lambda) = 0$. If χ_A does not split over $\mathbb{K}$, then A is *not* diagonalizable over $\mathbb{K}$.

Step 3. For each eigenvalue λ_i, compute the eigenspace $E_{\lambda_i} = \mathrm{Ker}(A - \lambda_i I_n)$ by solving the homogeneous system $(A - \lambda_i I_n)X = \mathbf{0}$.

Step 4. Check the multiplicity condition: $\dim E_{\lambda_i} = m_a(\lambda_i)$ for each i. If this fails for any eigenvalue, A is *not* diagonalizable.

Step 5. Form P by placing the eigenvectors (bases of each eigenspace) as columns, and $D = \mathrm{diag}(\lambda_1, \dots, \lambda_1, \lambda_2, \dots, \lambda_2, \dots)$ with each λ_i repeated $m_a(\lambda_i)$ times.

Example 31 (Full diagonalization of a 3×3 matrix)

Diagonalize $A = \begin{pmatrix} 4 & 0 & 1 \\ 2 & 3 & 2 \\ 1 & 0 & 4 \end{pmatrix}$.

Step 1. The characteristic polynomial:

$$\begin{aligned} \chi_A(\lambda) &= \det \begin{pmatrix} 4-\lambda & 0 & 1 \\ 2 & 3-\lambda & 2 \\ 1 & 0 & 4-\lambda \end{pmatrix} \\ &= (4-\lambda)\big[(3-\lambda)(4-\lambda) - 0\big] - 0 + 1\big[0 - (3-\lambda)\big] \\ &= (4-\lambda)(3-\lambda)(4-\lambda) - (3-\lambda) \\ &= (3-\lambda)\big[(4-\lambda)^2 - 1\big] \\ &= (3-\lambda)(16 - 8\lambda + \lambda^2 - 1) \\ &= (3-\lambda)(\lambda^2 - 8\lambda + 15) \\ &= (3-\lambda)(\lambda-3)(\lambda-5) \\ &= -(3-\lambda)^2(\lambda-5) = -(\lambda-3)^2(\lambda-5). \end{aligned}$$

Step 2. Eigenvalues: $\lambda_1 = 3$ (algebraic multiplicity 2) and $\lambda_2 = 5$ (algebraic multiplicity 1).

Step 3. Eigenspaces:

For $\lambda_1 = 3$: solve $(A - 3I_3)X = \mathbf{0}$:

$$A - 3I_3 = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 2 \\ 1 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

So $x_1 = -x_3$, x_2 free, x_3 free. A basis of $E_3(A)$ is

$$\left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \right\}, \quad \dim E_3(A) = 2 = m_a(3).$$

For $\lambda_2 = 5$: solve $(A - 5I_3)X = \mathbf{0}$:

$$A - 5I_3 = \begin{pmatrix} -1 & 0 & 1 \\ 2 & -2 & 2 \\ 1 & 0 & -1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{pmatrix}.$$

So $x_1 = x_3$, $x_2 = 2x_3$, x_3 free. A basis of $E_5(A)$ is $\left\{ \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \right\}$, and $\dim E_5(A) = 1 = m_a(5)$.

Step 4. Since $m_g = m_a$ for both eigenvalues, A is diagonalizable.

Step 5. We obtain

$$P = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}, \qquad D = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix}, \qquad A = PDP^{-1}.$$

Example 32 (A non-diagonalizable matrix)

Consider $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$. Then $\chi_A(\lambda) = (2-\lambda)^2$, so $\lambda = 2$ is the only eigenvalue with $m_a(2) = 2$. But $E_2(A) = \operatorname{Ker}(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}) = \operatorname{Span}((\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}))$, so $m_g(2) = 1 < 2 = m_a(2)$. By Theorem 28, A is *not* diagonalizable.

6.9 Trigonalization

Definition 33 (Trigonalizable endomorphism)

An endomorphism $f \in \operatorname{End}(E)$ is *trigonalizable* (over $\mathbb{K}$) if there exists a basis of E in which the matrix of f is upper triangular. A matrix $A \in \mathcal{M}_n(\mathbb{K})$ is trigonalizable if it is similar to an upper triangular matrix.

Theorem 34 (Trigonalization over an algebraically closed field)

Let $f \in \operatorname{End}(E)$ with $\dim E = n$. Then f is trigonalizable over $\mathbb{K}$ if and only if χ_f splits over $\mathbb{K}$.
In particular, every endomorphism of a finite-dimensional complex vector space is trigonalizable (since $\mathbb{C}$ is algebraically closed).

Proof. ($\Leftarrow$) We proceed by induction on $n = \dim E$. The case $n = 1$ is trivial.

Since χ_f splits, f has at least one eigenvalue $\lambda_1 \in \mathbb{K}$. Let v_1 be a corresponding eigenvector and set $F = \operatorname{Span}(v_1)$. The quotient space $\bar{E} = E/F$ has dimension $n-1$, and f induces a well-defined endomorphism $\bar{f} \colon \bar{E} \to \bar{E}$ (since F is f-invariant). Moreover, $\chi_{\bar{f}}$ divides χ_f (up to a constant), so $\chi_{\bar{f}}$ also splits over $\mathbb{K}$.

By the induction hypothesis, $\bar{f}$ is trigonalizable: there exists a basis $(\bar{v}_2, \dots, \bar{v}_n)$ of $\bar{E}$ in which $\bar{f}$ is upper triangular. Choosing representatives $v_2, \dots, v_n \in E$ with $\bar{v}_i = v_i + F$, the family $(v_1, v_2, \dots, v_n)$ is a basis of E and the matrix of f in this basis is upper triangular with λ_1 in the $(1,1)$ position.

($\Rightarrow$) If f is trigonalizable with upper triangular matrix T, then $\chi_f(\lambda) = \chi_T(\lambda) = \prod_{i=1}^{n}(t_{ii} - \lambda)$, which splits over $\mathbb{K}$. □

Corollary 35 (Trigonalization over $\mathbb{C}$)

Every matrix $A \in \mathcal{M}_n(\mathbb{C})$ is trigonalizable over $\mathbb{C}$.

6.10 Minimal polynomial

Definition 36 (Annihilating polynomial)

A polynomial $p \in \mathbb{K}[\lambda]$ is an *annihilating polynomial* (or *annihilator*) of $f \in \operatorname{End}(E)$ if $p(f) = 0$ (the zero endomorphism). Similarly, p annihilates $A \in \mathcal{M}_n(\mathbb{K})$ if $p(A) = 0_{n\times n}$.

By the Cayley–Hamilton theorem (Theorem 17), χ_f is always an annihilating polynomial of f. The minimal polynomial is the "smallest" such polynomial.

Definition 37 (Minimal polynomial)

The *minimal polynomial* of $f \in \mathrm{End}(E)$, denoted μ_f, is the unique monic polynomial of smallest degree that annihilates f.

Proposition 38 (Existence and uniqueness of the minimal polynomial)

The minimal polynomial μ_f exists and is unique. Moreover, μ_f divides every annihilating polynomial of f.

Proof. Existence. The set of annihilating polynomials is nonempty (it contains χ_f by Cayley–Hamilton) and every polynomial has a nonnegative degree, so there is one of minimal degree. Normalising to be monic gives μ_f.

Divides every annihilator. Let p be an annihilating polynomial. Perform Euclidean division: $p = q\mu_f + r$ with $\deg r < \deg \mu_f$. Then $r(f) = p(f) - q(f)\mu_f(f) = 0 - 0 = 0$. If $r \neq 0$, then $r/\operatorname{lc}(r)$ would be a monic annihilator of smaller degree than μ_f, a contradiction. Hence $r = 0$ and $\mu_f \mid p$.

Uniqueness. If μ and μ' are both monic annihilating polynomials of minimal degree, then $\mu \mid \mu'$ and $\mu' \mid \mu$ (by the above), so $\mu = \mu'$ (both being monic). □

Proposition 39 (Properties of the minimal polynomial)

Let $f \in \mathrm{End}(E)$. Then:

(i) μ_f divides χ_f.

(ii) μ_f and χ_f have the same roots (i.e. the same eigenvalues), though possibly with different multiplicities.

(iii) If A and B are similar matrices, they have the same minimal polynomial.

Proof. (i) Cayley–Hamilton gives $\chi_f(f) = 0$, so $\mu_f \mid \chi_f$.

(ii) Since $\mu_f \mid \chi_f$, every root of μ_f is a root of χ_f. Conversely, if λ is an eigenvalue of f with eigenvector v, then $\mu_f(f)(v) = \mu_f(\lambda)v = \mathbf{0}$, so $\mu_f(\lambda) = 0$ (since $v \neq \mathbf{0}$).

(iii) If $B = P^{-1}AP$, then $p(B) = P^{-1}p(A)P$ for any polynomial p. Thus $p(A) = 0$ if and only if $p(B) = 0$. □

Theorem 40 (Diagonalizability via the minimal polynomial)

An endomorphism $f \in \mathrm{End}(E)$ is diagonalizable if and only if its minimal polynomial μ_f splits into distinct linear factors over $\mathbb{K}$:

$$\mu_f(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2)\cdots(\lambda - \lambda_r)$$

where $\lambda_1, \ldots, \lambda_r$ are pairwise distinct.

Proof. ($\Rightarrow$) Suppose f is diagonalizable with eigenvalues $\lambda_1, \ldots, \lambda_r$. Set $p(\lambda) = (\lambda - \lambda_1)\cdots(\lambda - \lambda_r)$. Since f is diagonalizable, there is a basis of eigenvectors. For any eigenvector v with eigenvalue λ_i, $p(f)(v) = \prod_{j \neq i}(\lambda_i - \lambda_j) \cdot 0 \cdot v = \mathbf{0}$. Wait—more carefully: $p(f)(v) = (f - \lambda_1 \operatorname{Id})\cdots(f - \lambda_r \operatorname{Id})(v)$. Since $(f - \lambda_i \operatorname{Id})(v) = \mathbf{0}$, the entire product gives $\mathbf{0}$. As this holds for every eigenvector and eigenvectors Span E, we get $p(f) = 0$. So $\mu_f \mid p$. Since the roots of μ_f include all eigenvalues (by Proposition 39(ii)) and μ_f divides a product of distinct linear factors, μ_f itself is a product of distinct linear factors.

($\Leftarrow$) Suppose $\mu_f(\lambda) = (\lambda - \lambda_1)\cdots(\lambda - \lambda_r)$ with distinct λ_i. We prove $E = \bigoplus_{i=1}^{r} E_{\lambda_i}(f)$ by induction on r.

For $r = 1$: $\mu_f(\lambda) = \lambda - \lambda_1$, so $f = \lambda_1 \operatorname{Id}$ and every nonzero vector is an eigenvector. Thus $E = E_{\lambda_1}(f)$.

For the inductive step, write $\mu_f = (\lambda - \lambda_r)\, q(\lambda)$ where $q(\lambda) = \prod_{i=1}^{r-1}(\lambda - \lambda_i)$. Since $\gcd(q, \lambda - \lambda_r) = 1$ (the λ_i are distinct), there exist polynomials $a, b \in \mathbb{K}[\lambda]$ with $a(\lambda)\, q(\lambda) + b(\lambda)(\lambda - \lambda_r) = 1$. Substituting f:

$$a(f) \circ q(f) + b(f) \circ (f - \lambda_r \operatorname{Id}) = \operatorname{Id}.$$

For any $v \in E$, write $v = a(f)(q(f)(v)) + b(f)((f - \lambda_r \operatorname{Id})(v))$. Let $u = q(f)(v)$ and $w = (f - \lambda_r \operatorname{Id})(v)$. Then $(f - \lambda_r \operatorname{Id})(u) = (f - \lambda_r \operatorname{Id})(q(f)(v)) = \mu_f(f)(v) = \mathbf{0}$, so $u \in E_{\lambda_r}(f)$. Similarly, $q(f)(w) = q(f)(f - \lambda_r \operatorname{Id})(v) = \mu_f(f)(v) = \mathbf{0}$, so $w \in \operatorname{Ker}(q(f))$.

Now $q(f)$ acts on $F = \operatorname{Ker}(q(f))$, and q annihilates $f|_F$. So $\mu_{f|_F}$ divides $q = \prod_{i=1}^{r-1}(\lambda - \lambda_i)$. By the induction hypothesis, $F = \bigoplus_{i=1}^{r-1} E_{\lambda_i}(f|_F) \subset \bigoplus_{i=1}^{r-1} E_{\lambda_i}(f)$.

Since $v = a(f)(u) + b(f)(w)$ and $u \in E_{\lambda_r}(f)$, $w \in F \subset \bigoplus_{i=1}^{r-1} E_{\lambda_i}(f)$, we see that every $v \in E$ lies in $\sum_{i=1}^{r} E_{\lambda_i}(f)$. The sum is direct by Proposition 10. □

6.11 Applications

6.11.1 Computing powers of a matrix

Proposition 41 (Powers of a diagonalizable matrix)

If $A = PDP^{-1}$ where $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$, then for every integer $k \geq 0$,

$$A^k = P \operatorname{diag}(\lambda_1^k, \dots, \lambda_n^k)\, P^{-1}.$$

Proof. By induction, $A^k = (PDP^{-1})^k = PD^kP^{-1}$, since $(PDP^{-1})(PDP^{-1}) = PD(P^{-1}P)DP^{-1} = PD^2P^{-1}$, and so on. Moreover, $D^k = \operatorname{diag}(\lambda_1^k, \dots, \lambda_n^k)$. □

6.11.2 Linear recurrences: the Fibonacci sequence

Example 42 (Fibonacci sequence via diagonalization)

The Fibonacci sequence is defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$. Set $V_n = \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}$. Then $V_{n+1} = AV_n$ where $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

The characteristic polynomial is $\chi_A(\lambda) = \lambda^2 - \lambda - 1$, with roots $\varphi = \frac{1+\sqrt{5}}{2}$ and $\psi = \frac{1-\sqrt{5}}{2}$. Eigenvectors: $v_1 = \begin{pmatrix} \varphi \\ 1 \end{pmatrix}$ for φ and $v_2 = \begin{pmatrix} \psi \\ 1 \end{pmatrix}$ for ψ. So $P = \left(\begin{smallmatrix} \varphi & \psi \\ 1 & 1 \end{smallmatrix}\right)$ and $A = P\left(\begin{smallmatrix} \varphi & 0 \\ 0 & \psi \end{smallmatrix}\right)P^{-1}$.

From $V_n = A^n V_0$ and $V_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, we extract:

$$F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

This is *Binet's formula*.

6.11.3 Markov chains and steady-state distributions

Example 43 (Steady-state of a Markov chain)

A weather model has two states: Sunny (S) and Rainy (R), with transition matrix

$$T = \begin{pmatrix} 0.8 & 0.4 \\ 0.2 & 0.6 \end{pmatrix},$$

where column j gives the transition probabilities from state j. If $\mathbf{p}_n$ is the state vector at time n, then $\mathbf{p}_{n+1} = T\mathbf{p}_n$, so $\mathbf{p}_n = T^n\mathbf{p}_0$.
The eigenvalues of T are $\lambda_1 = 1$ and $\lambda_2 = 0.4$. The eigenvector for $\lambda_1 = 1$ (normalised to sum to 1) is

$$= \begin{pmatrix} 2/3 \\ 1/3 \end{pmatrix}.$$

Since $|\lambda_2| < 1$, as $n \to \infty$ the component along the second eigenvector decays, and $\mathbf{p}_n \to$ regardless of $\mathbf{p}_0$. Thus the long-run probability of sunny weather is $2/3$.

6.11.4 Systems of linear ODEs

Example 44 (System of ODEs via diagonalization)

Consider the system $\mathbf{x}'(t) = A\mathbf{x}(t)$ with $A = \left(\begin{smallmatrix} -3 & 1 \\ 1 & -3 \end{smallmatrix}\right)$. The eigenvalues are $\lambda_1 = -2$ (eigenvector $v_1 = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$) and $\lambda_2 = -4$ (eigenvector $v_2 = \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right)$).
Setting $\mathbf{x}(t) = P\mathbf{y}(t)$ where $P = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, the system decouples to $\mathbf{y}'(t) = D\mathbf{y}(t)$ with $D = \operatorname{diag}(-2, -4)$. The solution is

$$\mathbf{y}(t) = \begin{pmatrix} c_1 e^{-2t} \\ c_2 e^{-4t} \end{pmatrix}, \qquad \mathbf{x}(t) = c_1 e^{-2t}\begin{pmatrix} 1 \\ 1 \end{pmatrix} + c_2 e^{-4t}\begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

where c_1, c_2 are determined by the initial condition $\mathbf{x}(0)$.

6.12 Exercises

Exercise 45 (Eigenvalues of a 2×2 matrix)

Find the eigenvalues and eigenvectors of $A = \begin{pmatrix} 5 & 4 \\ 1 & 2 \end{pmatrix}$. Is A diagonalizable? If so, find P and D such that $A = PDP^{-1}$.

Exercise 46 (Eigenvalues of a triangular matrix)

Let $A \in \mathcal{M}_n(\mathbb{K})$ be upper triangular. Show that the eigenvalues of A are exactly the diagonal entries $a_{11}, a_{22}, \dots, a_{nn}$.

Exercise 47 (Eigenvalues of a projection)

Let $p \in \operatorname{End}(E)$ be a projection, i.e. $p^2 = p$. Show that the only possible eigenvalues of p are 0 and 1, and that p is diagonalizable.
Hint: What is the minimal polynomial of p?

Exercise 48 (Eigenvalues and trace/determinant)

Let $A \in \mathcal{M}_2(\mathbb{K})$ with eigenvalues λ_1, λ_2. Show that $\operatorname{tr}(A) = \lambda_1 + \lambda_2$ and $\det(A) = \lambda_1 \lambda_2$. Generalise to $n \times n$ matrices.

Exercise 49 (Eigenvalues of A^2, A^{-1}, $A + cI$)

Let $A \in \mathcal{M}_n(\mathbb{K})$ with eigenvalue λ and eigenvector v.

(a) Show that λ^2 is an eigenvalue of A^2 with the same eigenvector v. Generalise to A^k.

(b) If A is invertible, show that λ^{-1} is an eigenvalue of A^{-1}.

(c) Show that $\lambda + c$ is an eigenvalue of $A + cI$ for any $c \in \mathbb{K}$.

Exercise 50 (Diagonalization of a 3×3 matrix)

Diagonalize the matrix $A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 3 & 0 \\ 2 & 1 & -1 \end{pmatrix}$.

Exercise 51 (Non-diagonalizable matrix)

Show that $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ is not diagonalizable over any field. What is its minimal polynomial?

Exercise 52 (Cayley–Hamilton application)

Let $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

(a) Find the characteristic polynomial χ_A.

(b) Use the Cayley–Hamilton theorem to express A^{-1} as a polynomial in A (i.e. in the form $aI + bA$).

(c) Compute A^5 using Cayley–Hamilton to reduce to lower powers.

Exercise 53 (Powers via diagonalization)

Let $A = \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$.

(a) Diagonalize A.

(b) Compute A^{100}.

Exercise 54 (Simultaneous diagonalization)

Let $A, B \in \mathcal{M}_n(\mathbb{K})$ be diagonalizable matrices that commute ($AB = BA$). Show that A and B are *simultaneously diagonalizable*: there exists an invertible P such that both $P^{-1}AP$ and $P^{-1}BP$ are diagonal.
Hint: Show that eigenspaces of A are invariant under B, then diagonalize the restriction of B to each eigenspace.

Exercise 55 (Computing the Fibonacci sequence)

(a) Diagonalize $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ over $\mathbb{R}$.

(b) Derive Binet's formula: $F_n = \dfrac{1}{\sqrt{5}}\left[\left(\dfrac{1+\sqrt{5}}{2}\right)^n - \left(\dfrac{1-\sqrt{5}}{2}\right)^n\right]$.

(c) Show that F_n is the nearest integer to $\dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^n$ for all $n \geq 0$.

Exercise 56 (Minimal polynomial)

For each of the following matrices, find the minimal polynomial and determine whether the matrix is diagonalizable.

(a) $A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix}$

(b) $B = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix}$

(c) $C = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}$

Exercise 57 (Markov chain steady state)

A rat in a maze has three rooms. At each time step, it moves according to the transition matrix

$$T = \begin{pmatrix} 0.5 & 0.25 & 0.25 \\ 0.25 & 0.5 & 0.25 \\ 0.25 & 0.25 & 0.5 \end{pmatrix}.$$

(a) Find the eigenvalues and eigenspaces of T.

(b) Determine the steady-state distribution satisfying $T = $, $\sum_i \pi_i = 1$.

(c) Compute T^n explicitly and verify that $T^n \to \mathbf{1}^\mathsf{T}$ as $n \to \infty$ (where $\mathbf{1} = (1,1,1)^\mathsf{T}/3$).

6.13 Chapter summary

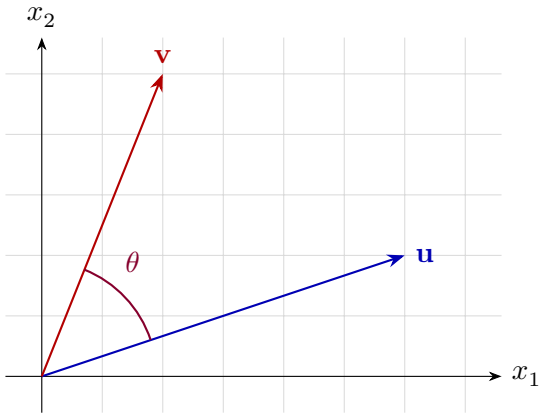
- An **eigenvalue** λ of $f \in \mathrm{End}(E)$ satisfies $f(v) = \lambda v$ for some nonzero v (the **eigenvector**). The **eigenspace** $E_\lambda(f) = \mathrm{Ker}(f - \lambda\,\mathrm{Id})$ is a subspace.
- The **characteristic polynomial** $\chi_f(\lambda) = \det(f - \lambda\,\mathrm{Id})$ has degree n; its roots in $\mathbb{K}$ are exactly the eigenvalues. The set of eigenvalues is the **spectrum** $\mathrm{Spec}(f)$.
- The **Cayley–Hamilton theorem**: every matrix satisfies its own characteristic polynomial, $\chi_A(A) = 0$.
- For each eigenvalue λ, the **geometric multiplicity** $m_g(\lambda) = \dim E_\lambda$ satisfies $1 \leq m_g(\lambda) \leq m_a(\lambda)$ (the **algebraic multiplicity**).
- f is **diagonalizable** if and only if χ_f splits over $\mathbb{K}$ and $m_g = m_a$ for every eigenvalue. Equivalently, $E = \bigoplus_{\lambda \in \mathrm{Spec}(f)} E_\lambda(f)$.
- **Diagonalization algorithm**: compute χ_f, find eigenvalues, compute eigenspaces, check $m_g = m_a$, form the change-of-basis matrix P.
- Every endomorphism whose characteristic polynomial splits is **trigonalizable**. Over $\mathbb{C}$, every endomorphism is trigonalizable.
- The **minimal polynomial** μ_f is the monic polynomial of smallest degree annihilating f. It divides χ_f and shares its roots. f is diagonalizable if and only if μ_f splits into distinct linear factors.
- **Applications**: if $A = PDP^{-1}$ then $A^k = PD^kP^{-1}$, which allows efficient computation of matrix powers, closed-form solutions of linear recurrences (Fibonacci), steady-state analysis of Markov chains, and explicit solutions of linear systems of ODEs.

Chapter 7

Inner Product Spaces and Orthogonality

Up to this point, our study of linear algebra has been purely *algebraic*: we have manipulated vector spaces, linear maps, and matrices without ever measuring a length, an angle, or a distance. Yet geometry—in the intuitive sense of Euclidean space—depends critically on such measurements. How long is a vector? What angle do two vectors enclose? Which vector in a subspace is closest to a given point?

The tool that answers all these questions at once is the *inner product*: a function that takes two vectors and returns a scalar, generalising the familiar dot product on $\mathbb{R}^n$. Once an inner product is fixed, the underlying vector space acquires a rich geometric structure—norms, distances, angles, orthogonality, projections—and many powerful theorems become available.



$$\cos\theta \;=\; \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{u}\|\,\|\mathbf{v}\|}$$

Figure 7.1: The inner product encodes the angle between two vectors. All of Euclidean geometry follows.

This chapter develops the theory systematically, starting from the general notion of bilinear forms, specialising to inner products, and building up the machinery of orthogonality, projections, and orthonormal bases. We then study the linear maps that preserve inner products (orthogonal and unitary matrices) and those that are "self-dual" with respect to the inner product (adjoint operators).

Throughout, $\mathbb{K}$ denotes $\mathbb{R}$ or $\mathbb{C}$, and E denotes a finite-dimensional $\mathbb{K}$-vector space unless stated otherwise. We use the convention that inner products on $\mathbb{C}$ are linear in the *first* argument and conjugate-linear in the second (the *physics convention*).

7.1 Bilinear forms

Definition 1 (Bilinear form)

Let E be a vector space over $\mathbb{K}$. A *bilinear form* on E is a map $\varphi\colon E \times E \to \mathbb{K}$ that is linear in each argument:

(i) For all $u, v, w \in E$ and $\lambda \in \mathbb{K}$:

$$\varphi(u + \lambda v,\, w) = \varphi(u, w) + \lambda\, \varphi(v, w).$$

(ii) For all $u, v, w \in E$ and $\lambda \in \mathbb{K}$:

$$\varphi(u,\, v + \lambda w) = \varphi(u, v) + \lambda\, \varphi(u, w).$$

Definition 2 (Symmetric and antisymmetric bilinear forms)

A bilinear form φ on E is called:

- *symmetric* if $\varphi(u, v) = \varphi(v, u)$ for all $u, v \in E$;
- *antisymmetric* (or *skew-symmetric*) if $\varphi(u, v) = -\varphi(v, u)$ for all $u, v \in E$.

Definition 3 (Matrix of a bilinear form)

Let $\mathcal{B} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ be a basis of E and let φ be a bilinear form on E. The *matrix of φ in the basis $\mathcal{B}$* is the matrix $G \in \mathcal{M}_n(\mathbb{K})$ defined by

$$G_{ij} := \varphi(\mathbf{e}_i, \mathbf{e}_j), \qquad 1 \le i, j \le n.$$

If $u = \sum_i x_i\, \mathbf{e}_i$ and $v = \sum_j y_j\, \mathbf{e}_j$, then

$$\varphi(u, v) = X^{\mathsf{T}}\, G\, Y,$$

where $X = (x_1, \dots, x_n)^{\mathsf{T}}$ and $Y = (y_1, \dots, y_n)^{\mathsf{T}}$ are the coordinate vectors.

Proposition 4 (Change of basis for bilinear forms)

If P is the change-of-basis matrix from $\mathcal{B}$ to $\mathcal{B}'$, and G is the matrix of φ in $\mathcal{B}$, then the matrix of φ in $\mathcal{B}'$ is

$$G' = P^{\mathsf{T}}\, G\, P.$$

In particular, φ is symmetric if and only if G is symmetric ($G = G^{\mathsf{T}}$).

Proof. Let $u, v \in E$ with coordinates X' in $\mathcal{B}'$ and $X = PX'$ in $\mathcal{B}$ (similarly $Y = PY'$). Then

$$\varphi(u, v) = X^{\mathsf{T}}\, G\, Y = (PX')^{\mathsf{T}}\, G\, (PY') = X'^{\mathsf{T}}\, (P^{\mathsf{T}}\, G\, P)\, Y'.$$

Since this holds for all X', Y', we have $G' = P^{\mathsf{T}}\, G\, P$. □

Definition 5 (Non-degenerate bilinear form)

A bilinear form φ on E is *non-degenerate* if

$$\big(\,\forall v \in E,\ \varphi(u, v) = 0\big) \implies u = \mathbf{0}.$$

Equivalently, the matrix G of φ in any basis is invertible.

7.2 Quadratic forms

Definition 6 (Quadratic form)

Let E be a $\mathbb{K}$-vector space. A *quadratic form* on E is a map $q\colon E \to \mathbb{K}$ such that

(i) $q(\lambda v) = \lambda^2\, q(v)$ for all $\lambda \in \mathbb{K}$, $v \in E$;

(ii) the map $\varphi\colon E \times E \to \mathbb{K}$ defined by

$$\varphi(u, v) := \frac{1}{2}\big[q(u+v) - q(u) - q(v)\big]$$

is bilinear (this is called the *polar form* of q).

Conversely, every symmetric bilinear form φ defines a quadratic form $q(v) = \varphi(v, v)$.

Proposition 7 (Polarization identity)

If $\operatorname{char}(\mathbb{K}) \neq 2$ and φ is a symmetric bilinear form with associated quadratic form $q(v) = \varphi(v, v)$, then

$$\varphi(u, v) = \frac{1}{2}\big[q(u+v) - q(u) - q(v)\big] = \frac{1}{4}\big[q(u+v) - q(u-v)\big].$$

Thus, q and φ determine each other uniquely.

Proof. Expanding $q(u+v) = \varphi(u+v,\, u+v) = q(u) + 2\varphi(u, v) + q(v)$ gives the first identity. For the second, note that $q(u-v) = q(u) - 2\varphi(u, v) + q(v)$, so subtracting yields $q(u+v) - q(u-v) = 4\varphi(u, v)$. □

Theorem 8 (Sylvester's law of inertia)

Let q be a quadratic form on a real vector space E of dimension n. There exists a basis of E in which the matrix of the associated bilinear form is diagonal with entries $+1$, -1, and 0:

$$G = \operatorname{diag}(\underbrace{1, \dots, 1}_{p},\ \underbrace{-1, \dots, -1}_{r-p},\ \underbrace{0, \dots, 0}_{n-r}).$$

The integers p (the number of $+1$'s), $r - p$ (the number of -1's), and $n - r$ (the number of 0's) depend only on q, not on the choice of basis. The pair $(p,\, r-p)$ is called the *signature* of q, and $r = \operatorname{rank}(q)$.

Remark 9 (Positive definiteness from the signature)

A real quadratic form q is *positive definite* (i.e. $q(v) > 0$ for all $v \neq \mathbf{0}$) if and only if its signature is $(n, 0)$, i.e. all signs are $+1$.

7.3 Inner products

Definition 10 (Inner product (real case))

Let E be a real vector space. An *inner product* on E is a bilinear form $\langle \cdot, \cdot \rangle \colon E \times E \to \mathbb{R}$ that is

(i) *symmetric*: $\langle u, v \rangle = \langle v, u \rangle$ for all $u, v \in E$;

(ii) *positive definite*: $\langle v, v \rangle > 0$ for all $v \neq \mathbf{0}$.

A real vector space equipped with an inner product is called a *Euclidean space*.

Definition 11 (Sesquilinear form)

Let E be a complex vector space. A *sesquilinear form* on E is a map $\varphi \colon E \times E \to \mathbb{C}$ that is linear in the first argument and conjugate-linear in the second:

(i) $\varphi(\alpha u + \beta v,\, w) = \alpha\, \varphi(u, w) + \beta\, \varphi(v, w)$;

(ii) $\varphi(u,\, \alpha v + \beta w) = \bar{\alpha}\, \varphi(u, v) + \bar{\beta}\, \varphi(u, w)$.

A sesquilinear form is *Hermitian* if $\varphi(u, v) = \overline{\varphi(v, u)}$ for all $u, v \in E$.

Definition 12 (Inner product (complex case))

Let E be a complex vector space. A *Hermitian inner product* (or simply *inner product*) on E is a sesquilinear form $\langle \cdot, \cdot \rangle \colon E \times E \to \mathbb{C}$ that is

(i) *Hermitian symmetric*: $\langle u, v \rangle = \overline{\langle v, u \rangle}$ for all $u, v \in E$;

(ii) *positive definite*: $\langle v, v \rangle > 0$ for all $v \neq \mathbf{0}$ (note that $\langle v, v \rangle \in \mathbb{R}$ by (i)).

A complex vector space equipped with a Hermitian inner product is called a *unitary space* (or *pre-Hilbert space*).

Remark 13 (Unified notation)

Over $\mathbb{R}$, a Hermitian inner product reduces to a symmetric bilinear form (since conjugation is trivial). We therefore write $\langle u, v \rangle$ in both cases and speak simply of an "inner product space".

7.4 Examples

Example 14 (Standard dot product on $\mathbb{R}^n$)

The *standard inner product* on $\mathbb{R}^n$ is

$$\langle x, y \rangle := \sum_{i=1}^{n} x_i\, y_i = x^{\mathsf{T}}\, y, \qquad x, y \in \mathbb{R}^n.$$

Its matrix in the standard basis is $G = I_n$.

Example 15 (Hermitian product on $\mathbb{C}^n$)

The *standard Hermitian inner product* on $\mathbb{C}^n$ is

$$\langle z, w\rangle := \sum_{i=1}^{n} z_i\,\bar{w}_i = w^{*}\,z, \qquad z, w \in \mathbb{C}^n.$$

This is linear in the first argument and conjugate-linear in the second.

Example 16 (L^2 inner product on $\mathcal{C}([a,b])$)

On the space $\mathcal{C}([a,b],\mathbb{R})$ of continuous real-valued functions on $[a,b]$, the map

$$\langle f, g\rangle := \int_a^b f(t)\,g(t)\,\mathrm{d}t$$

is an inner product. Symmetry and bilinearity are immediate from the properties of the integral; positive definiteness follows because $\langle f, f\rangle = \int_a^b f(t)^2\,\mathrm{d}t \geq 0$, with equality if and only if $f = 0$ (by continuity).
The complex analogue on $\mathcal{C}([a,b],\mathbb{C})$ is $\langle f, g\rangle = \int_a^b f(t)\,\overline{g(t)}\,\mathrm{d}t$.

Example 17 (Weighted inner product)

Let $w_1, \dots, w_n > 0$ be positive reals. Then

$$\langle x, y\rangle_w := \sum_{i=1}^{n} w_i\,x_i\,y_i$$

defines an inner product on $\mathbb{R}^n$. Its matrix in the standard basis is $G = \operatorname{diag}(w_1, \dots, w_n)$.

Example 18 (Frobenius inner product)

On the space $\mathcal{M}_n(\mathbb{R})$, the map

$$\langle A, B\rangle := \operatorname{tr}(A^{\mathsf{T}}\,B) = \sum_{i,j} a_{ij}\,b_{ij}$$

defines an inner product (the *Frobenius inner product*).

7.5 Norm and distance

Definition 19 (Norm induced by an inner product)

Let $(E, \langle\cdot,\cdot\rangle)$ be an inner product space. The *norm* of $v \in E$ is

$$\|v\| := \sqrt{\langle v, v\rangle}.$$

Definition 20 (Distance)

The *distance* between u and v in an inner product space is

$$d(u, v) := \|u - v\|.$$

Proposition 21 (Basic properties of the norm)

Let $(E, \langle \cdot, \cdot \rangle)$ be an inner product space. For all $u, v \in E$ and $\lambda \in \mathbb{K}$:

(i) $\|v\| \geq 0$, with equality if and only if $v = \mathbf{0}$;

(ii) $\|\lambda v\| = |\lambda| \, \|v\|$ (absolute homogeneity);

(iii) $\|u + v\|^2 + \|u - v\|^2 = 2\|u\|^2 + 2\|v\|^2$ (parallelogram law).

Proof. Parts (i) and (ii) follow directly from the definition and the properties of the inner product. For (iii), expand using bilinearity:

$$\|u + v\|^2 + \|u - v\|^2 = \langle u + v, u + v \rangle + \langle u - v, u - v \rangle = 2\langle u, u \rangle + 2\langle v, v \rangle = 2\|u\|^2 + 2\|v\|^2. \quad \square$$

7.6 The Cauchy–Schwarz inequality

Theorem 22 (Cauchy–Schwarz inequality)

Let $(E, \langle \cdot, \cdot \rangle)$ be an inner product space over $\mathbb{K}$. For all $u, v \in E$,

$$|\langle u, v \rangle| \leq \|u\| \, \|v\|,$$

with equality if and only if u and v are linearly dependent (i.e. one is a scalar multiple of the other).

Proof. If $v = \mathbf{0}$, both sides are zero and the result is trivial. Assume $v \neq \mathbf{0}$.

Real case ($\mathbb{K} = \mathbb{R}$). For any $t \in \mathbb{R}$, the positive definiteness of the inner product gives

$$0 \leq \|u - tv\|^2 = \langle u - tv, \, u - tv \rangle = \|u\|^2 - 2t\langle u, v \rangle + t^2\|v\|^2.$$

This is a quadratic polynomial in t that is non-negative for all t. A real quadratic $at^2 + bt + c \geq 0$ for all t requires the discriminant to satisfy $b^2 - 4ac \leq 0$. Here $a = \|v\|^2$, $b = -2\langle u, v \rangle$, $c = \|u\|^2$, so

$$4\langle u, v \rangle^2 - 4\|u\|^2\|v\|^2 \leq 0,$$

which gives $\langle u, v \rangle^2 \leq \|u\|^2\|v\|^2$, and taking square roots yields $|\langle u, v \rangle| \leq \|u\| \, \|v\|$.

Equality holds if and only if the discriminant is zero, i.e. the minimum of the quadratic is zero, which occurs at $t_0 = \langle u, v \rangle / \|v\|^2$, giving $u = t_0 v$.

Complex case ($\mathbb{K} = \mathbb{C}$). For any $t \in \mathbb{R}$ and any $\alpha \in \mathbb{C}$ with $|\alpha| = 1$, consider

$$0 \leq \|u - t\alpha v\|^2 = \|u\|^2 - 2t \, \Re(\alpha \, \langle v, u \rangle) + t^2\|v\|^2.$$

Choose α so that $\alpha \, \langle v, u \rangle = |\langle u, v \rangle|$ (this is possible by writing $\langle u, v \rangle = |\langle u, v \rangle| \, e^{i\theta}$ and setting $\alpha = e^{-i\theta}$). Then $\Re(\alpha \, \langle v, u \rangle) = |\langle u, v \rangle|$, and the above becomes

$$0 \leq \|u\|^2 - 2t|\langle u, v \rangle| + t^2\|v\|^2.$$

This is again a non-negative real quadratic in t, and the discriminant argument gives

$$4|\langle u, v\rangle|^2 - 4\|u\|^2\|v\|^2 \leq 0,$$

i.e. $|\langle u, v\rangle| \leq \|u\|\,\|v\|$. Equality analysis is identical: it holds if and only if $u = t_0 \alpha v$ for the optimal t_0, i.e. u and v are linearly dependent. □

Corollary 23 (Triangle inequality)

For all $u, v \in E$,

$$\|u + v\| \leq \|u\| + \|v\|.$$

In particular, $d(\cdot, \cdot)$ satisfies the triangle inequality and defines a metric on E.

Proof. We compute

$$\begin{aligned}\|u + v\|^2 = \langle u + v,\, u + v\rangle &= \|u\|^2 + 2\Re\langle u, v\rangle + \|v\|^2 \\ &\leq \|u\|^2 + 2|\langle u, v\rangle| + \|v\|^2 \\ &\leq \|u\|^2 + 2\|u\|\,\|v\| + \|v\|^2 = (\|u\| + \|v\|)^2,\end{aligned}$$

where the last inequality uses Cauchy–Schwarz. Taking square roots gives the result. □

Definition 24 (Angle between vectors)

In a real inner product space, for nonzero $u, v \in E$, the *angle* $\theta \in [0, \pi]$ between u and v is defined by

$$\cos\theta := \frac{\langle u, v\rangle}{\|u\|\,\|v\|}.$$

This is well-defined by the Cauchy–Schwarz inequality, which ensures $|\cos\theta| \leq 1$.

7.7 Orthogonality

Definition 25 (Orthogonal vectors)

Two vectors u, v in an inner product space are *orthogonal*, written $u \perp v$, if $\langle u, v\rangle = 0$.

Proposition 26 (Pythagorean theorem)

If $u \perp v$, then $\|u + v\|^2 = \|u\|^2 + \|v\|^2$.

Proof. $\|u + v\|^2 = \|u\|^2 + 2\Re\langle u, v\rangle + \|v\|^2 = \|u\|^2 + \|v\|^2$, since $\langle u, v\rangle = 0$. □

Definition 27 (Orthogonal complement)

Let F be a subset (or subspace) of an inner product space E. The *orthogonal complement* of F is

$$F^{\perp} := \{\, v \in E \mid \langle v, w\rangle = 0 \text{ for all } w \in F \,\}.$$

Theorem 28 (Properties of the orthogonal complement)

Let $(E, \langle\cdot,\cdot\rangle)$ be a finite-dimensional inner product space and let F be a subspace of E. Then:

(i) $F^\perp$ is a subspace of E.

(ii) $E = F \oplus F^\perp$ (orthogonal direct sum).

(iii) $\dim F^\perp = \dim E - \dim F$.

(iv) $(F^\perp)^\perp = F$.

(v) $F \cap F^\perp = \{\mathbf{0}\}$.

Proof. **(i)** $F^\perp$ is clearly non-empty ($\mathbf{0} \in F^\perp$) and closed under addition and scalar multiplication by linearity of the inner product.

(v) If $v \in F \cap F^\perp$, then $\langle v, v\rangle = 0$, so $v = \mathbf{0}$ by positive definiteness.

(ii)–(iv) We prove these after establishing orthogonal projection (Theorem 30). Once we know that every $v \in E$ can be written as $v = p + p^\perp$ with $p \in F$ and $p^\perp \in F^\perp$, the direct sum decomposition follows from (v). Part (iii) then follows by counting dimensions, and (iv) is immediate from $E = F \oplus F^\perp$ and the observation that $F \subset (F^\perp)^\perp$ together with the dimension count $\dim (F^\perp)^\perp = n - \dim F^\perp = \dim F$. □

Proposition 29 (Orthogonal complement of sums and intersections)

Let F_1, F_2 be subspaces of a finite-dimensional inner product space E. Then:

(i) $(F_1 + F_2)^\perp = F_1^\perp \cap F_2^\perp$.

(ii) $(F_1 \cap F_2)^\perp = F_1^\perp + F_2^\perp$.

Proof. **(i)** $v \in (F_1 + F_2)^\perp$ iff $\langle v, w\rangle = 0$ for all $w \in F_1 + F_2$, which (since $F_1, F_2 \subset F_1 + F_2$) is equivalent to $v \in F_1^\perp$ and $v \in F_2^\perp$.

(ii) Take orthogonal complements in (i) and use $(F^\perp)^\perp = F$. □

7.8 Orthogonal projection

Theorem 30 (Orthogonal projection)

Let $(E, \langle\cdot,\cdot\rangle)$ be a finite-dimensional inner product space and let F be a subspace of E. For every $v \in E$, there exists a unique vector $p \in F$ such that

$$v - p \in F^\perp.$$

The vector p is called the *orthogonal projection* of v onto F, denoted $p = \operatorname{proj}_F(v)$. The map $\operatorname{proj}_F \colon E \to E$ is a linear map satisfying $\operatorname{proj}_F^2 = \operatorname{proj}_F$, $\operatorname{Im}(\operatorname{proj}_F) = F$, and $\operatorname{Ker}(\operatorname{proj}_F) = F^\perp$.

Proof. **Existence.** Let $(e_1, \dots, e_k)$ be an orthonormal basis of F (which exists by Gram–Schmidt, Theorem 33). Set

$$p := \sum_{i=1}^{k} \langle v, e_i\rangle\, e_i.$$

Then $p \in F$, and for each basis vector e_j we have

$$\langle v - p,\, e_j \rangle = \langle v, e_j \rangle - \sum_{i=1}^{k} \langle v, e_i \rangle \langle e_i, e_j \rangle = \langle v, e_j \rangle - \langle v, e_j \rangle = 0.$$

By linearity, $\langle v - p,\, w \rangle = 0$ for all $w \in F$, so $v - p \in F^{\perp}$.

Uniqueness. If p' is another such vector, then $p - p' \in F$ and $p - p' \in F^{\perp}$, so $p - p' \in F \cap F^{\perp} = \{\mathbf{0}\}$.

Linearity is clear from the formula. The remaining properties $\mathrm{proj}_F^2 = \mathrm{proj}_F$, $\mathrm{Im}(\mathrm{proj}_F) = F$, and $\mathrm{Ker}(\mathrm{proj}_F) = F^{\perp}$ follow directly from the construction and uniqueness. □

Theorem 31 (Best approximation)

Let F be a subspace of a finite-dimensional inner product space E and let $v \in E$. The orthogonal projection $p = \mathrm{proj}_F(v)$ is the unique element of F closest to v:

$$\|v - p\| < \|v - w\| \qquad \text{for all } w \in F,\ w \neq p.$$

Proof. Let $w \in F$. Since $v - p \in F^{\perp}$ and $p - w \in F$, the Pythagorean theorem gives

$$\|v - w\|^2 = \|(v - p) + (p - w)\|^2 = \|v - p\|^2 + \|p - w\|^2 \geq \|v - p\|^2,$$

with equality if and only if $p = w$. □

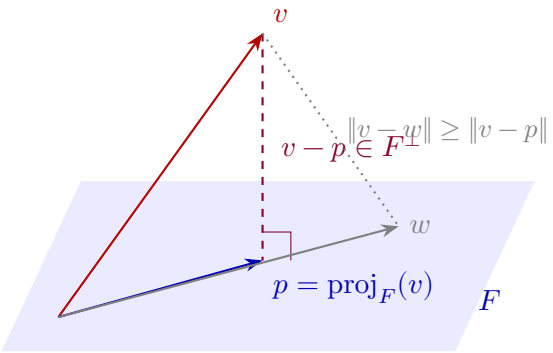


Figure 7.2: Orthogonal projection onto a subspace F. The projection $p = \mathrm{proj}_F(v)$ is the closest point in F to v.

Proposition 32 (Projection formula with an orthonormal basis)

If $(e_1, \dots, e_k)$ is an orthonormal basis of a subspace F, then

$$\mathrm{proj}_F(v) = \sum_{i=1}^{k} \langle v, e_i \rangle\, e_i.$$

In particular, if $(e_1, \dots, e_n)$ is an orthonormal basis of the full space E, then $v = \sum_{i=1}^{n} \langle v, e_i \rangle\, e_i$.

7.9 Gram–Schmidt orthogonalization

Theorem 33 (Gram–Schmidt process)

Let $(v_1, \dots, v_k)$ be a linearly independent family in an inner product space E. There exists a unique orthonormal family $(e_1, \dots, e_k)$ such that for each $j = 1, \dots, k$:

(i) $\operatorname{Span}(e_1, \dots, e_j) = \operatorname{Span}(v_1, \dots, v_j)$;

(ii) $\langle v_j, e_j \rangle > 0$ (i.e. the "leading coefficient" is positive).

The family $(e_1, \dots, e_k)$ is constructed by the **Gram–Schmidt algorithm**:

$$w_1 := v_1, \qquad e_1 := \frac{w_1}{\|w_1\|},$$

$$w_j := v_j - \sum_{i=1}^{j-1} \langle v_j, e_i \rangle \, e_i, \qquad e_j := \frac{w_j}{\|w_j\|}, \qquad j = 2, \dots, k.$$

Proof. We proceed by induction on j.

Base case ($j = 1$). Set $w_1 = v_1$. Since $v_1 \neq \mathbf{0}$ (linear independence), $\|w_1\| > 0$ and $e_1 = w_1/\|w_1\|$ is well-defined with $\|e_1\| = 1$. Clearly $\operatorname{Span}(e_1) = \operatorname{Span}(v_1)$ and $\langle v_1, e_1 \rangle = \|v_1\| > 0$.

Inductive step. Assume that $(e_1, \dots, e_{j-1})$ is an orthonormal family with $\operatorname{Span}(e_1, \dots, e_{j-1}) = \operatorname{Span}(v_1, \dots, v_{j-1})$ and $\langle v_i, e_i \rangle > 0$ for $i < j$. Define

$$w_j = v_j - \sum_{i=1}^{j-1} \langle v_j, e_i \rangle \, e_i.$$

This is exactly $v_j - \operatorname{proj}_{F_{j-1}}(v_j)$, where $F_{j-1} = \operatorname{Span}(e_1, \dots, e_{j-1})$. Hence $w_j \perp e_i$ for all $i < j$ (by construction of the orthogonal projection).

We must show $w_j \neq \mathbf{0}$. If $w_j = \mathbf{0}$, then $v_j = \sum_{i=1}^{j-1} \langle v_j, e_i \rangle \, e_i \in F_{j-1} = \operatorname{Span}(v_1, \dots, v_{j-1})$, contradicting the linear independence of $(v_1, \dots, v_k)$.

Set $e_j = w_j/\|w_j\|$. Then $\|e_j\| = 1$, and $e_j \perp e_i$ for all $i < j$ since $w_j \perp e_i$. Moreover,

$$\operatorname{Span}(e_1, \dots, e_j) = \operatorname{Span}(e_1, \dots, e_{j-1}, \, w_j) = \operatorname{Span}(e_1, \dots, e_{j-1}, \, v_j) = \operatorname{Span}(v_1, \dots, v_j),$$

using the induction hypothesis and the definition of w_j. Finally, $\langle v_j, e_j \rangle = \langle v_j, w_j/\|w_j\| \rangle = \|w_j\| > 0$ (since $\langle v_j, w_j \rangle = \langle w_j + \sum_i c_i e_i, \, w_j \rangle = \|w_j\|^2 > 0$).

Uniqueness. Suppose $(\tilde{e}_1, \dots, \tilde{e}_k)$ also satisfies conditions (i)–(ii). By (i), $\operatorname{Span}(\tilde{e}_1) = \operatorname{Span}(v_1)$, so $\tilde{e}_1 = \pm e_1$; condition (ii) forces $\tilde{e}_1 = e_1$. Inductively, the orthogonal complement of $\operatorname{Span}(\tilde{e}_1, \dots, \tilde{e}_{j-1})$ within $\operatorname{Span}(v_1, \dots, v_j)$ is one-dimensional, Spanned by w_j. Normalisation with a positive leading coefficient forces $\tilde{e}_j = e_j$. □

Example 34 (Gram–Schmidt in $\mathbb{R}^3$)

Apply Gram–Schmidt to $v_1 = (1, 1, 0)$, $v_2 = (1, 0, 1)$, $v_3 = (0, 1, 1)$ with the standard inner product.

Step 1. $w_1 = v_1 = (1, 1, 0)$, $\quad e_1 = w_1/\|w_1\| = \frac{1}{\sqrt{2}}(1, 1, 0)$.

Step 2. $\langle v_2, e_1 \rangle = \frac{1}{\sqrt{2}}(1 \cdot 1 + 0 \cdot 1 + 1 \cdot 0) = \frac{1}{\sqrt{2}}$.

$w_2 = v_2 - \langle v_2, e_1 \rangle \, e_1 = (1, 0, 1) - \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}}(1, 1, 0) = (1, 0, 1) - (\frac{1}{2}, \frac{1}{2}, 0) = (\frac{1}{2}, -\frac{1}{2}, 1)$.

$\|w_2\| = \sqrt{\frac{1}{4} + \frac{1}{4} + 1} = \sqrt{\frac{3}{2}} = \frac{\sqrt{6}}{2}$, $\quad$ so $e_2 = \frac{1}{\sqrt{6}}(1, -1, 2)$.

Step 3. $\langle v_3, e_1 \rangle = \frac{1}{\sqrt{2}}(0 + 1 + 0) = \frac{1}{\sqrt{2}}$, $\quad \langle v_3, e_2 \rangle = \frac{1}{\sqrt{6}}(0 - 1 + 2) = \frac{1}{\sqrt{6}}$.

$w_3 = v_3 - \frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}}(1,1,0) - \frac{1}{\sqrt{6}}\cdot\frac{1}{\sqrt{6}}(1,-1,2) = (0,1,1) - (\tfrac12,\tfrac12,0) - (\tfrac16,-\tfrac16,\tfrac13) = (-\tfrac23,\tfrac23,\tfrac23)$.
$\|w_3\| = \frac{2}{3}\sqrt{3}$, so $e_3 = \frac{1}{\sqrt{3}}(-1,1,1)$.

The resulting orthonormal basis is:

$$e_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\end{pmatrix}, \quad e_2 = \frac{1}{\sqrt{6}}\begin{pmatrix}1\\-1\\2\end{pmatrix}, \quad e_3 = \frac{1}{\sqrt{3}}\begin{pmatrix}-1\\1\\1\end{pmatrix}.$$

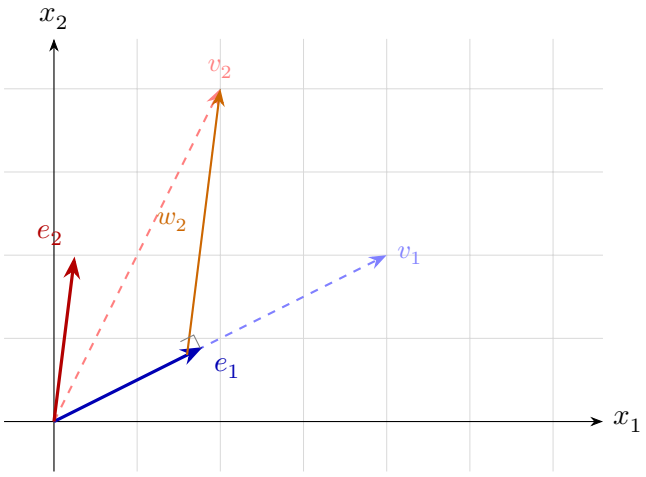


Figure 7.3: Gram–Schmidt in $\mathbb{R}^2$: v_2 is orthogonalised against e_1 to produce w_2, then normalised to give e_2.

7.10 Orthonormal bases

Definition 35 (Orthogonal and orthonormal families)

A family $(e_1, \dots, e_k)$ in an inner product space is:

- *orthogonal* if $\langle e_i, e_j\rangle = 0$ for all $i \neq j$;
- *orthonormal* if it is orthogonal and $\|e_i\| = 1$ for all i.

An orthonormal family that is also a basis of E is called an *orthonormal basis* (ONB).

Proposition 36 (Orthogonal families are linearly independent)

Every orthogonal family of nonzero vectors is linearly independent.

Proof. Let $(e_1, \dots, e_k)$ be orthogonal with each $e_i \neq \mathbf{0}$. Suppose $\sum_{i=1}^{k} \alpha_i\, e_i = \mathbf{0}$. Taking the inner product with e_j:

$$0 = \left\langle \sum_i \alpha_i\, e_i,\, e_j \right\rangle = \sum_i \alpha_i \langle e_i, e_j\rangle = \alpha_j \langle e_j, e_j\rangle = \alpha_j \|e_j\|^2.$$

Since $\|e_j\| > 0$, we get $\alpha_j = 0$ for all j. □

Corollary 37 (Existence of orthonormal bases)

Every finite-dimensional inner product space admits an orthonormal basis.

Proof. Apply the Gram–Schmidt process (Theorem 33) to any basis of E. □

Theorem 38 (Parseval's identity)

Let $(e_1, \dots, e_n)$ be an orthonormal basis of an inner product space E. Then for all $u, v \in E$:

$$\langle u, v \rangle = \sum_{i=1}^{n} \langle u, e_i \rangle \, \overline{\langle v, e_i \rangle}.$$

In particular, taking $v = u$:

$$\|u\|^2 = \sum_{i=1}^{n} |\langle u, e_i \rangle|^2.$$

Proof. Write $u = \sum_{i=1}^{n} \alpha_i \, e_i$ and $v = \sum_{j=1}^{n} \beta_j \, e_j$ where $\alpha_i = \langle u, e_i \rangle$ and $\beta_j = \langle v, e_j \rangle$. Then

$$\langle u, v \rangle = \left\langle \sum_i \alpha_i \, e_i, \sum_j \beta_j \, e_j \right\rangle = \sum_{i,j} \alpha_i \, \bar{\beta}_j \, \langle e_i, e_j \rangle = \sum_i \alpha_i \, \bar{\beta}_i = \sum_i \langle u, e_i \rangle \, \overline{\langle v, e_i \rangle}.$$ □

Theorem 39 (Bessel's inequality)

Let $(e_1, \dots, e_k)$ be an orthonormal family (not necessarily a basis) in an inner product space E. Then for all $v \in E$:

$$\sum_{i=1}^{k} |\langle v, e_i \rangle|^2 \leq \|v\|^2,$$

with equality if and only if $v \in \operatorname{Span}(e_1, \dots, e_k)$.

Proof. Let $p = \sum_{i=1}^{k} \langle v, e_i \rangle \, e_i$ be the orthogonal projection of v onto $F = \operatorname{Span}(e_1, \dots, e_k)$. Then $v = p + (v - p)$ with $p \perp (v - p)$, so by the Pythagorean theorem:

$$\|v\|^2 = \|p\|^2 + \|v - p\|^2 \geq \|p\|^2 = \sum_{i=1}^{k} |\langle v, e_i \rangle|^2.$$

Equality holds iff $\|v - p\| = 0$, i.e. $v = p \in F$. □

Definition 40 (Gram matrix)

Let $(v_1, \dots, v_k)$ be a family of vectors in an inner product space. The *Gram matrix* is the $k \times k$ matrix G defined by

$$G_{ij} := \langle v_i, v_j \rangle.$$

The family is orthonormal if and only if $G = I_k$. The family is linearly independent if and only if $\det(G) \neq 0$.

7.11 Orthogonal and unitary matrices

Definition 41 (Orthogonal matrix)

A matrix $Q \in \mathcal{M}_n(\mathbb{R})$ is *orthogonal* if

$$Q^{\mathsf{T}} Q = I_n,$$

or equivalently $Q^{-1} = Q^{\mathsf{T}}$. The set of all $n \times n$ orthogonal matrices is denoted $\mathrm{O}(n)$ and forms a group under matrix multiplication, called the *orthogonal group*.

Definition 42 (Unitary matrix)

A matrix $U \in \mathcal{M}_n(\mathbb{C})$ is *unitary* if

$$U^{*} U = I_n,$$

or equivalently $U^{-1} = U^{*}$. The set of all $n \times n$ unitary matrices is the *unitary group* $U(n)$.

Proposition 43 (Characterizations of orthogonal/unitary matrices)

Let $Q \in \mathcal{M}_n(\mathbb{R})$. The following are equivalent:

(i) Q is orthogonal.

(ii) The columns of Q form an orthonormal basis of $\mathbb{R}^n$.

(iii) The rows of Q form an orthonormal basis of $\mathbb{R}^n$.

(iv) Q preserves the inner product: $\langle Qx, Qy \rangle = \langle x, y \rangle$ for all x, y.

(v) Q preserves norms: $\|Qx\| = \|x\|$ for all x (i.e. Q is an *isometry*).

The analogous statements hold for unitary matrices over $\mathbb{C}$.

Proof. **(i)⇔(ii).** $Q^{\mathsf{T}}Q = I$ means $\langle q_i, q_j \rangle = \delta_{ij}$, where $q_1, \dots, q_n$ are the columns of Q.
(i)⇔(iii). $QQ^{\mathsf{T}} = I$ (which follows from $Q^{\mathsf{T}}Q = I$ since both are square) means the rows are orthonormal.
(i)⇒(iv). $\langle Qx, Qy \rangle = (Qx)^{\mathsf{T}} Qy = x^{\mathsf{T}} Q^{\mathsf{T}} Q y = x^{\mathsf{T}} y = \langle x, y \rangle$.
(iv)⇒(v). Take $y = x$.
(v)⇒(i). $\|Qx\|^2 = \|x\|^2$ for all x means $x^{\mathsf{T}} Q^{\mathsf{T}} Q x = x^{\mathsf{T}} x$, so $x^{\mathsf{T}}(Q^{\mathsf{T}}Q - I)x = 0$ for all x. Since $Q^{\mathsf{T}}Q - I$ is symmetric, this implies $Q^{\mathsf{T}}Q = I$. □

Proposition 44 (Determinant of orthogonal matrices)

If $Q \in \mathrm{O}(n)$, then $\det(Q) = \pm 1$.

Proof. $1 = \det(I) = \det(Q^{\mathsf{T}}Q) = \det(Q^{\mathsf{T}})\det(Q) = \det(Q)^2$, so $\det(Q) = \pm 1$. □

Definition 45 (Special orthogonal group)

The *special orthogonal group* is $\mathrm{SO}(n) := \{\, Q \in \mathrm{O}(n) \mid \det(Q) = 1 \,\}$. Its elements are the orthogonal matrices that preserve orientation (rotations in the geometric sense).

Example 46 (Orthogonal matrices in dimension 2)

Every matrix in $\mathrm{SO}(2)$ is a rotation:

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \qquad \theta \in [0, 2\pi).$$

The matrices in $\mathrm{O}(2) \setminus \mathrm{SO}(2)$ are reflections:

$$S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Example 47 (Permutation matrices)

Every permutation matrix (obtained by permuting the columns of I_n) is orthogonal. Its determinant is $+1$ for even permutations and -1 for odd permutations.

7.12 The adjoint operator

Definition 48 (Adjoint of a linear map)

Let $(E, \langle\cdot,\cdot\rangle)$ be a finite-dimensional inner product space and let $f \in \mathrm{End}(E)$. The *adjoint* of f is the unique linear map $f^* \in \mathrm{End}(E)$ satisfying

$$\langle f(u), v\rangle = \langle u, f^*(v)\rangle \qquad \text{for all } u, v \in E.$$

Theorem 49 (Existence and uniqueness of the adjoint)

For every $f \in \mathrm{End}(E)$ on a finite-dimensional inner product space, the adjoint f^* exists and is unique. If $(e_1, \dots, e_n)$ is an orthonormal basis and $A = \mathcal{M}_{\mathcal{B}}(f)$ is the matrix of f in this basis, then

$$\mathcal{M}_{\mathcal{B}}(f^*) = A^* \quad (\text{i.e. } \bar{A}^{\mathsf{T}} \text{ over } \mathbb{C}, \text{ or } A^{\mathsf{T}} \text{ over } \mathbb{R}).$$

Proof. **Uniqueness.** Suppose $g, h \in \mathrm{End}(E)$ both satisfy $\langle f(u), v\rangle = \langle u, g(v)\rangle = \langle u, h(v)\rangle$ for all u, v. Then $\langle u, g(v) - h(v)\rangle = 0$ for all u, which by non-degeneracy gives $g(v) = h(v)$ for all v.

Existence. Let $(e_1, \dots, e_n)$ be an orthonormal basis and $A = (a_{ij})$ the matrix of f in this basis, so $f(e_j) = \sum_i a_{ij}\, e_i$. Define $g \in \mathrm{End}(E)$ by the matrix $B = A^*$, i.e. $b_{ij} = \bar{a}_{ji}$. Then for any two basis vectors:

$$\langle f(e_j), e_k\rangle = a_{kj}, \qquad \langle e_j, g(e_k)\rangle = \overline{b_{jk}} = \overline{\bar{a}_{kj}} = a_{kj}.$$

By linearity, $\langle f(u), v\rangle = \langle u, g(v)\rangle$ for all u, v, so $f^* = g$ and $\mathcal{M}_{\mathcal{B}}(f^*) = A^*$. □

Proposition 50 (Properties of the adjoint)

Let $f, g \in \mathrm{End}(E)$ and $\alpha \in \mathbb{K}$. Then:

(i) $(f + g)^* = f^* + g^*$.

(ii) $(\alpha f)^* = \bar{\alpha}\, f^*$.

(iii) $(f \circ g)^* = g^* \circ f^*$.

(iv) $(f^*)^* = f$.

(v) $\operatorname{Ker}(f^*) = (\operatorname{Im} f)^\perp$.

(vi) $\operatorname{Im}(f^*) = (\operatorname{Ker} f)^\perp$.

Proof. Properties (i)–(iv) follow from the characterizing identity $\langle f(u), v\rangle = \langle u, f^*(v)\rangle$ and uniqueness of the adjoint.

(v). $v \in \operatorname{Ker}(f^*)$ iff $f^*(v) = \mathbf{0}$ iff $\langle u, f^*(v)\rangle = 0$ for all u iff $\langle f(u), v\rangle = 0$ for all u iff $v \in (\operatorname{Im} f)^\perp$.

(vi). Apply (v) to f^* to get $\operatorname{Ker}(f) = (\operatorname{Im} f^*)^\perp$, then take orthogonal complements: $\operatorname{Im}(f^*) = (\operatorname{Im} f^*)^{\perp\perp} = (\operatorname{Ker} f)^\perp$. □

Definition 51 (Self-adjoint, normal, and skew-adjoint operators)

An operator $f \in \operatorname{End}(E)$ is called:

- *self-adjoint* (or *Hermitian*) if $f^* = f$;
- *skew-adjoint* (or *anti-Hermitian*) if $f^* = -f$;
- *normal* if $f^* \circ f = f \circ f^*$.

In matrix terms (in an ONB): self-adjoint means $A = A^*$ (symmetric if $\mathbb{K} = \mathbb{R}$), and normal means $A^*A = AA^*$.

Remark 52 (Orthogonal/unitary operators via the adjoint)

An operator $f \in \operatorname{End}(E)$ satisfies $f^* \circ f = \mathrm{Id}$ (equivalently, f preserves the inner product) if and only if its matrix in an orthonormal basis is orthogonal (over $\mathbb{R}$) or unitary (over $\mathbb{C}$). In particular, orthogonal and unitary operators are normal.

7.13 Applications

7.13.1 Least squares approximation

A fundamental application of orthogonal projection is the *least squares* method. Given a system $Ax = b$ that may have no exact solution (because $b \notin \operatorname{Im}(A)$), we seek the vector $\hat{x}$ that minimises $\|Ax - b\|$.

Theorem 53 (Normal equations)

Let $A \in \mathcal{M}_{m\times n}(\mathbb{R})$ with $m \geq n$ and $\operatorname{rank}(A) = n$. The least squares solution of $Ax = b$ is the unique vector $\hat{x}$ satisfying

$$A^{\mathsf{T}} A\, \hat{x} = A^{\mathsf{T}}\, b.$$

The minimum residual is $\|b - A\hat{x}\| = \|b - \operatorname{proj}_{\operatorname{Im} A}(b)\|$.

Proof. The vector $A\hat{x}$ must be the orthogonal projection of b onto $\operatorname{Im}(A)$, i.e. $b - A\hat{x} \perp \operatorname{Im}(A)$. This means $\langle A_j, b - A\hat{x}\rangle = 0$ for each column A_j of A, which is equivalent to $A^{\mathsf{T}}(b - A\hat{x}) = 0$, i.e. $A^{\mathsf{T}}A\hat{x} = A^{\mathsf{T}}b$. Since $\operatorname{rank}(A) = n$, the matrix $A^{\mathsf{T}}A$ is invertible (it is the Gram matrix of the columns of A), giving the unique solution $\hat{x} = (A^{\mathsf{T}}A)^{-1} A^{\mathsf{T}}\, b$. □

7.13.2 QR factorization

The Gram–Schmidt process has an elegant matrix interpretation. If $A \in \mathcal{M}_{m\times n}(\mathbb{R})$ has linearly independent columns $a_1, \dots, a_n$, then Gram–Schmidt produces orthonormal vectors $q_1, \dots, q_n$ such that

$$\operatorname{Span}(a_1, \dots, a_j) = \operatorname{Span}(q_1, \dots, q_j) \qquad \text{for each } j.$$

In matrix form, this means $A = QR$, where

- $Q \in \mathcal{M}_{m\times n}(\mathbb{R})$ has orthonormal columns $q_1, \dots, q_n$;
- $R \in \mathcal{M}_{n}(\mathbb{R})$ is upper triangular with positive diagonal entries, given by $r_{ij} = \langle a_j, q_i \rangle$ for $i \le j$.

This is the *QR factorization* (or QR decomposition) of A. It is numerically more stable than directly solving the normal equations and is a cornerstone of numerical linear algebra.

7.13.3 Fourier series

Consider the inner product space $\mathcal{C}([-\pi, \pi], \mathbb{R})$ with the L^2 inner product $\langle f, g \rangle = \int_{-\pi}^{\pi} f(t)\, g(t)\, \mathrm{d}t$. The family

$$\frac{1}{\sqrt{2\pi}}, \ \frac{\cos t}{\sqrt{\pi}}, \ \frac{\sin t}{\sqrt{\pi}}, \ \frac{\cos 2t}{\sqrt{\pi}}, \ \frac{\sin 2t}{\sqrt{\pi}}, \ \dots$$

is orthonormal. The orthogonal projection of a function f onto the Span of the first $2N+1$ elements is the *truncated Fourier series*:

$$S_N(f)(t) = \frac{a_0}{2} + \sum_{k=1}^{N} (a_k \cos kt + b_k \sin kt),$$

where $a_k = \frac{1}{\pi}\int_{-\pi}^{\pi} f(t)\cos kt\, \mathrm{d}t$ and $b_k = \frac{1}{\pi}\int_{-\pi}^{\pi} f(t)\sin kt\, \mathrm{d}t$ are the *Fourier coefficients*. By Theorem 31, this is the best approximation of f by trigonometric polynomials of degree $\le N$ in the L^2 norm. Bessel's inequality (Theorem 39) gives

$$\frac{a_0^2}{2} + \sum_{k=1}^{N} (a_k^2 + b_k^2) \le \frac{1}{\pi}\int_{-\pi}^{\pi} f(t)^2\, \mathrm{d}t,$$

and Parseval's identity (Theorem 38) asserts that equality holds in the limit $N \to \infty$ (for $f \in L^2$).

7.14 Exercises

Exercise 54 (Verifying inner product axioms)

Determine which of the following are inner products on $\mathbb{R}^2$:

(a) $\langle x, y \rangle = x_1 y_1 - x_1 y_2 - x_2 y_1 + 4 x_2 y_2$.

(b) $\langle x, y \rangle = x_1 y_1 + x_2 y_2 - x_1 y_2 - x_2 y_1$.

(c) $\langle x, y \rangle = 2 x_1 y_1 + x_1 y_2 + x_2 y_1 + 2 x_2 y_2$.

For each, write the matrix G and check symmetry and positive definiteness.

Exercise 55 (Cauchy–Schwarz for sums)

Using the standard inner product on $\mathbb{R}^n$, deduce from the Cauchy–Schwarz inequality that for all $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{R}$:

$$\Big(\sum_{i=1}^{n} a_i b_i\Big)^2 \le \Big(\sum_{i=1}^{n} a_i^2\Big)\Big(\sum_{i=1}^{n} b_i^2\Big).$$

When does equality hold?

Exercise 56 (Cauchy–Schwarz for integrals)

Deduce from the Cauchy–Schwarz inequality (applied to the L^2 inner product on $\mathcal{C}([a,b])$) that for continuous f, g:

$$\Big(\int_a^b f(t)\,g(t)\,\mathrm{d}t\Big)^2 \le \int_a^b f(t)^2\,\mathrm{d}t \cdot \int_a^b g(t)^2\,\mathrm{d}t.$$

Exercise 57 (Orthogonal complement in $\mathbb{R}^3$)

Let $F = \mathrm{Span}((1,1,0),(0,1,1)) \subset \mathbb{R}^3$ with the standard inner product. Find $F^\perp$ and verify that $\mathbb{R}^3 = F \oplus F^\perp$.

Exercise 58 (Gram–Schmidt in $\mathbb{R}^3$)

Apply the Gram–Schmidt process to the basis $v_1 = (1,0,1)$, $v_2 = (1,1,0)$, $v_3 = (0,1,1)$ of $\mathbb{R}^3$.

Exercise 59 (Orthogonal projection computation)

In $\mathbb{R}^3$ with the standard inner product, compute the orthogonal projection of $v = (1,2,3)$ onto the plane $F = \{\,(x_1,x_2,x_3) \in \mathbb{R}^3 \mid x_1 + x_2 + x_3 = 0\,\}$.

Exercise 60 (Orthogonal matrix properties)

Let $Q \in \mathrm{O}(n)$.

(a) Show that $\det(Q) = \pm 1$.

(b) Show that if λ is an eigenvalue of Q (possibly complex), then $|\lambda| = 1$.

(c) Show that if n is odd and $Q \in \mathrm{SO}(n)$, then 1 is an eigenvalue of Q (hence Q has a fixed axis).

Exercise 61 (Adjoint of a matrix)

Let $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$, viewed as an endomorphism of $(\mathbb{R}^2, \langle\cdot,\cdot\rangle)$ with the standard inner product.

(a) Find $A^* = A^{\mathsf{T}}$.

(b) Verify the identity $\langle Ax, y\rangle = \langle x, A^*y\rangle$ for $x = (1,0)$ and $y = (0,1)$.

(c) Is A self-adjoint? Is A normal?

Exercise 62 (Least squares line fitting)

Find the line $y = a + bx$ that best fits (in the least squares sense) the data points $(0,1)$, $(1,0)$, $(2,3)$, $(3,2)$.

Hint: Set up the system $Ax = b$ with $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{pmatrix}$, $b = (1,0,3,2)^{\mathsf{T}}$, and solve the normal equations.

Exercise 63 (QR factorization)

Compute the QR factorization of the matrix

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

by applying the Gram–Schmidt process to the columns of A. Verify that $A = QR$.

Exercise 64 (Isometries of $\mathbb{R}^2$)

Show that every $Q \in \mathrm{O}(2)$ is either a rotation $R_\theta \in \mathrm{SO}(2)$ or a reflection. Describe the geometric action in each case.

Exercise 65 (Self-adjoint operators have real eigenvalues)

Let $(E, \langle\cdot,\cdot\rangle)$ be a complex inner product space and $f \in \mathrm{End}(E)$ self-adjoint ($f^* = f$).

(a) Show that all eigenvalues of f are real.

(b) Show that eigenvectors corresponding to distinct eigenvalues are orthogonal.

Exercise 66 (Polarization identity)

Let E be a real inner product space. Prove that the inner product is completely determined by the norm via the *polarization identity*:

$$\langle u, v\rangle = \frac{1}{4}\left(\|u+v\|^2 - \|u-v\|^2\right).$$

In the complex case, show the analogous identity:

$$\langle u, v\rangle = \frac{1}{4}\sum_{k=0}^{3} i^k \,\|u + i^k v\|^2.$$

Exercise 67 (Orthogonal projection onto a line)

Let $a \in \mathbb{R}^n$ be nonzero. Show that the matrix of the orthogonal projection onto $\operatorname{Span}(a)$ is

$$P = \frac{a\,a^{\mathsf{T}}}{a^{\mathsf{T}}\,a}.$$

Verify that $P^2 = P$, $P^{\mathsf{T}} = P$, and $\operatorname{rank}(P) = 1$.

Exercise 68 (Unitary diagonalization of Hermitian matrices)

Let $A = \begin{pmatrix} 2 & 1-i \\ 1+i & 3 \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$.

(a) Verify that A is Hermitian.

(b) Find the eigenvalues of A and show they are real.

(c) Find an orthonormal eigenbasis and write $A = UDU^{*}$ for a unitary matrix U and diagonal matrix D.

Exercise 69 (Fourier coefficients and best approximation)

Let $f(t) = t$ on $[-\pi, \pi]$.

(a) Compute the Fourier coefficients a_k and b_k for $k = 0, 1, 2, 3$.

(b) Write the best trigonometric polynomial approximation of degree ≤ 3 in the L^2 norm.

(c) Verify Bessel's inequality for $N = 3$.

7.15 Chapter summary

- A **bilinear form** $\varphi\colon E \times E \to \mathbb{K}$ is linear in each argument. It is **symmetric** if $\varphi(u,v) = \varphi(v,u)$ and **non-degenerate** if its matrix is invertible. The associated **quadratic form** is $q(v) = \varphi(v,v)$.
- **Sylvester's law of inertia**: every real quadratic form can be reduced to diagonal form $\operatorname{diag}(+1,\dots,+1,-1,\dots,-1,0,\dots,0)$; the **signature** $(p, r-p)$ is an invariant.
- An **inner product** is a positive definite symmetric bilinear form (real case) or a positive definite Hermitian sesquilinear form (complex case).
- The **norm** $\|v\| = \sqrt{\langle v, v\rangle}$ satisfies the **Cauchy–Schwarz inequality** $|\langle u, v\rangle| \le \|u\|\|v\|$ and the **triangle inequality** $\|u+v\| \le \|u\| + \|v\|$.
- Two vectors are **orthogonal** if $\langle u, v\rangle = 0$. The **orthogonal complement** $F^{\perp}$ satisfies $E = F \oplus F^{\perp}$.
- The **orthogonal projection** $\operatorname{proj}_F(v)$ is the unique closest point to v in a subspace F (**best approximation property**).
- The **Gram–Schmidt process** turns any linearly independent family into an orthonormal one while preserving the successive Spans. Every inner product space has an **orthonormal basis**.

- **Parseval's identity**: in an ONB, $\langle u, v\rangle = \sum_i \langle u, e_i\rangle\overline{\langle v, e_i\rangle}$. **Bessel's inequality**: partial sums of Fourier coefficients are bounded by $\|v\|^2$.
- **Orthogonal matrices** ($Q^\mathsf{T}Q = I$) preserve inner products and norms; they form the group $\mathrm{O}(n)$, with the subgroup $\mathrm{SO}(n)$ (rotations, $\det = 1$). Over $\mathbb{C}$, the analogues are **unitary matrices**.
- The **adjoint** f^* of a linear map satisfies $\langle f(u), v\rangle = \langle u, f^*(v)\rangle$; in an ONB, its matrix is A^*. Key identities: $\ker(f^*) = (\operatorname{Im} f)^\perp$ and $\operatorname{Im}(f^*) = (\ker f)^\perp$.
- **Applications**: *least squares* (solve overdetermined systems via $A^\mathsf{T}A\hat{x} = A^\mathsf{T}b$), *QR factorization* (matrix form of Gram–Schmidt), and *Fourier series* (orthogonal projection onto trigonometric polynomials).

Chapter 8

Spectral Theorem and Symmetric Matrices

In the preceding chapters we studied eigenvalues, eigenvectors, and diagonalization of general linear maps. We saw that not every matrix is diagonalizable, and that when diagonalization succeeds the change-of-basis matrix need not enjoy any particular geometric property. In this chapter we restrict our attention to a distinguished class of operators — *self-adjoint* (symmetric or Hermitian) operators — for which the theory becomes strikingly clean: every self-adjoint operator is diagonalizable, all eigenvalues are real, and one can find an *orthonormal* basis of eigenvectors.

This is the content of the *Spectral Theorem*, one of the most important results in all of linear algebra. Its applications pervade mathematics, science, and engineering:

- **Covariance matrices.** In statistics and data science, the covariance matrix of a random vector is symmetric and positive semidefinite; its eigenvectors are the *principal components*, and PCA amounts to the spectral decomposition of this matrix.
- **Hessians and optimization.** The Hessian of a twice differentiable function $f\colon \mathbb{R}^n \to \mathbb{R}$ is a real symmetric matrix; its eigenvalues determine whether a critical point is a local minimum, maximum, or saddle point.
- **Quadratic forms.** The classification of quadratic forms (ellipses, hyperbolas, etc.) relies on the signs of the eigenvalues of the associated symmetric matrix.
- **Vibrations and normal modes.** The natural frequencies of a vibrating system are the square roots of the eigenvalues of a symmetric matrix, and the normal modes are its eigenvectors.
- **Quantum mechanics.** Observables are Hermitian operators on a Hilbert space; the Spectral Theorem guarantees that measurement outcomes (eigenvalues) are real numbers.

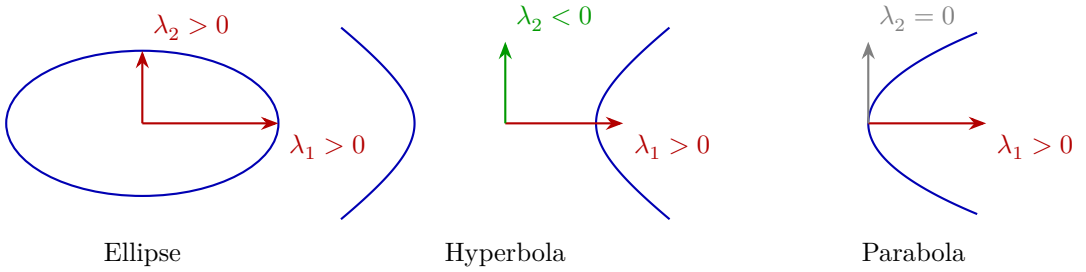


Figure 8.1: Classification of conics by the eigenvalues of the associated symmetric matrix. All eigenvalues positive: ellipse; mixed signs: hyperbola; one eigenvalue zero: parabola.

Throughout this chapter, E denotes a finite-dimensional inner product space over $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, with inner product $\langle \cdot, \cdot \rangle$ and induced norm $\|\cdot\|$. We write $\dim E = n$. Matrices are identified with their corresponding endomorphisms via a chosen basis whenever convenient.

8.1 Self-adjoint (symmetric and Hermitian) operators

Definition 1 (Adjoint of a linear map)

Let $(E, \langle \cdot, \cdot \rangle)$ be a finite-dimensional inner product space and $f \in \mathrm{End}(E)$. The *adjoint* of f is the unique linear map $f^* \in \mathrm{End}(E)$ satisfying

$$\langle f(u),\, v \rangle \;=\; \langle u,\, f^*(v) \rangle \qquad \text{for all } u, v \in E.$$

Remark 2 (Existence and uniqueness of the adjoint)

Existence and uniqueness follow from the Riesz representation theorem (or can be verified directly using an orthonormal basis). If $\mathcal{B}$ is an orthonormal basis and $A = \mathcal{M}_{\mathcal{B}}(f)$, then $\mathcal{M}_{\mathcal{B}}(f^*) = A^*$, the conjugate transpose. Over $\mathbb{R}$ this reduces to $\mathcal{M}_{\mathcal{B}}(f^*) = A^{\mathsf{T}}$.

Proposition 3 (Properties of the adjoint)

For $f, g \in \mathrm{End}(E)$ and $\alpha \in \mathbb{K}$:

(i) $(f + g)^* = f^* + g^*$.

(ii) $(\alpha f)^* = \bar{\alpha}\, f^*$.

(iii) $(f \circ g)^* = g^* \circ f^*$.

(iv) $(f^*)^* = f$.

(v) f is invertible if and only if f^* is, and then $(f^*)^{-1} = (f^{-1})^*$.

Proof. All properties follow from the definition and the sesquilinearity (or bilinearity over $\mathbb{R}$) of the inner product. We verify (iii): for all $u, v \in E$,

$$\langle (f \circ g)(u),\, v \rangle = \langle f(g(u)),\, v \rangle = \langle g(u),\, f^*(v) \rangle = \langle u,\, g^*(f^*(v)) \rangle = \langle u,\, (g^* \circ f^*)(v) \rangle,$$

so $(f \circ g)^* = g^* \circ f^*$ by uniqueness of the adjoint. The remaining items are proved similarly. $\square$

Definition 4 (Self-adjoint operator)

An endomorphism $f \in \mathrm{End}(E)$ is *self-adjoint* if $f^* = f$, i.e. $\langle f(u), v \rangle = \langle u, f(v) \rangle$ for all $u, v \in E$.
In matrix terms with respect to an orthonormal basis:

- Over $\mathbb{R}$: A is *symmetric*, i.e. $A^{\mathsf{T}} = A$.
- Over $\mathbb{C}$: A is *Hermitian*, i.e. $A^* = A$.

We denote the real vector space of $n \times n$ real symmetric matrices by $\mathrm{Sym}_n(\mathbb{R}) := \{\, A \in \mathcal{M}_n(\mathbb{R}) \mid A^{\mathsf{T}} = A \,\}$.

Example 5 (Symmetric matrices)

The matrix $A = \begin{pmatrix} 2 & -1 \\ -1 & 3 \end{pmatrix}$ is symmetric. The matrix $B = \begin{pmatrix} 1 & 2+i \\ 2-i & 3 \end{pmatrix}$ is Hermitian (the diagonal entries are real and the off-diagonal entries are complex conjugates).

Proposition 6 (Dimension of $\mathrm{Sym}_n(\mathbb{R})$)

$$\dim \mathrm{Sym}_n(\mathbb{R}) = \frac{n(n+1)}{2}.$$

Proof. A symmetric matrix is determined by its entries on and above the diagonal. There are n diagonal entries and $\binom{n}{2}$ entries strictly above the diagonal, giving $n + \binom{n}{2} = \frac{n(n+1)}{2}$. □

8.2 Eigenvalues of self-adjoint operators are real

Theorem 7 (Eigenvalues of self-adjoint operators are real)

Let f be a self-adjoint operator on an inner product space E (over $\mathbb{R}$ or $\mathbb{C}$). Then every eigenvalue of f is real.

Proof. Let λ be an eigenvalue and $v \neq \mathbf{0}$ an eigenvector: $f(v) = \lambda v$. Then

$$\lambda \langle v, v \rangle = \langle \lambda v,\, v \rangle = \langle f(v),\, v \rangle = \langle v,\, f(v) \rangle = \langle v,\, \lambda v \rangle = \bar{\lambda} \langle v, v \rangle.$$

Since $v \neq \mathbf{0}$, we have $\langle v, v \rangle > 0$, so dividing yields $\lambda = \bar{\lambda}$, which means $\lambda \in \mathbb{R}$. □

Remark 8 (Real eigenvalues over $\mathbb{R}$)

Over $\mathbb{R}$, one must be slightly careful: a real symmetric matrix might a priori have no eigenvalues in $\mathbb{R}$ (since the characteristic polynomial need not split). However, the Spectral Theorem will establish that it does. The above proof works directly if we allow eigenvalues in $\mathbb{C}$ and use the standard Hermitian inner product on $\mathbb{C}^n$. Concretely: if $A \in \mathrm{Sym}_n(\mathbb{R})$ and $\lambda \in \mathbb{C}$ satisfies $Av = \lambda v$ for some $v \in \mathbb{C}^n \setminus \{\mathbf{0}\}$, then $\lambda \in \mathbb{R}$.

8.3 Orthogonality of eigenvectors for distinct eigenvalues

Theorem 9 (Eigenvectors for distinct eigenvalues are orthogonal)

Let f be a self-adjoint operator on E, and let v_1, v_2 be eigenvectors of f associated with distinct eigenvalues $\lambda_1 \neq \lambda_2$. Then $\langle v_1, v_2 \rangle = 0$.

Proof. We compute $\langle f(v_1), v_2 \rangle$ in two ways:

$$\langle f(v_1),\, v_2 \rangle = \langle \lambda_1 v_1,\, v_2 \rangle = \lambda_1 \langle v_1, v_2 \rangle,$$

and, using the self-adjointness of f,

$$\langle f(v_1),\, v_2 \rangle = \langle v_1,\, f(v_2) \rangle = \langle v_1,\, \lambda_2 v_2 \rangle = \bar{\lambda}_2 \langle v_1, v_2 \rangle = \lambda_2 \langle v_1, v_2 \rangle,$$

where the last equality uses the fact that $\lambda_2 \in \mathbb{R}$ (Theorem 7). Subtracting:

$$(\lambda_1 - \lambda_2)\,\langle v_1, v_2\rangle = 0.$$

Since $\lambda_1 \neq \lambda_2$, we conclude $\langle v_1, v_2\rangle = 0$. □

Corollary 10 (Eigenspaces of a self-adjoint operator are mutually orthogonal)

If f is self-adjoint with distinct eigenvalues $\lambda_1, \dots, \lambda_r$, then

$$E_{\lambda_i} \perp E_{\lambda_j} \qquad \text{for all } i \neq j,$$

where $E_{\lambda_k} = \operatorname{Ker}(f - \lambda_k \operatorname{Id})$ is the eigenspace for λ_k.

Proof. Every vector in E_{λ_i} is an eigenvector for λ_i (or zero), and likewise for E_{λ_j}. The result follows from Theorem 9 applied to each pair of nonzero vectors. □

8.4 The Spectral Theorem for real symmetric matrices

We now prove the central result of this chapter.

Lemma 11 (Invariance of the orthogonal complement)

Let f be a self-adjoint operator on E and let $W \subseteq E$ be a subspace invariant under f (i.e. $f(W) \subseteq W$). Then the orthogonal complement $W^{\perp}$ is also invariant under f.

Proof. Let $v \in W^{\perp}$. We must show $f(v) \in W^{\perp}$, i.e. $\langle f(v), w\rangle = 0$ for all $w \in W$. Since f is self-adjoint,

$$\langle f(v),\, w\rangle = \langle v,\, f(w)\rangle.$$

Now $w \in W$ and $f(W) \subseteq W$, so $f(w) \in W$. Since $v \in W^{\perp}$, we get $\langle v, f(w)\rangle = 0$. Hence $\langle f(v), w\rangle = 0$. □

Lemma 12 (A self-adjoint operator over $\mathbb{R}$ has a real eigenvalue)

Let $A \in \operatorname{Sym}_n(\mathbb{R})$. Then A has at least one (real) eigenvalue.

Proof. The characteristic polynomial $\chi_A(\lambda) = \det(A - \lambda I_n)$ has degree n with real coefficients. Over $\mathbb{C}$ it has a root $\lambda_0 \in \mathbb{C}$, and by Theorem 7 (applied in the Hermitian setting) λ_0 is real. Hence A has a real eigenvalue. □

Theorem 13 (Spectral Theorem for real symmetric matrices)

Let $A \in \operatorname{Sym}_n(\mathbb{R})$ be a real symmetric matrix. Then:

(i) All eigenvalues of A are real.

(ii) There exists an orthogonal matrix $P \in \mathrm{O}(n)$ (i.e. $P^{\mathsf{T}}P = I_n$) such that

$$P^{\mathsf{T}}\, A\, P = \operatorname{diag}(\lambda_1, \dots, \lambda_n),$$

where $\lambda_1, \dots, \lambda_n$ are the eigenvalues of A (counted with multiplicity).

(iii) Equivalently, $\mathbb{R}^n$ has an orthonormal basis of eigenvectors of A.

Proof. We prove by strong induction on n.

Base case ($n = 1$). A 1×1 matrix $A = (a)$ is already diagonal with eigenvalue $a \in \mathbb{R}$, and $P = (1) \in \mathrm{O}(1)$.

Inductive step. Assume the theorem holds for all real symmetric matrices of size less than n. Let $A \in \mathrm{Sym}_n(\mathbb{R})$.

Step 1: Find a real eigenvalue and unit eigenvector. By Lemma 12, A has a real eigenvalue $\lambda_1 \in \mathbb{R}$. Let v_1 be an eigenvector for λ_1 with $\|v_1\| = 1$.

Step 2: Set up the orthogonal complement. Let $W = \mathrm{Span}(v_1)$. Since $Av_1 = \lambda_1 v_1$, the subspace W is A-invariant. By Lemma 11, $W^\perp$ is also A-invariant, and $\dim W^\perp = n - 1$.

Step 3: Restrict and apply the induction hypothesis. Let $g = f|_{W^\perp}$, where f is the linear map $x \mapsto Ax$. Since $f(W^\perp) \subseteq W^\perp$, the map g is a well-defined endomorphism of $W^\perp$. Moreover, g is self-adjoint on $W^\perp$ (the inner product is the restriction of the standard one, and the self-adjointness condition is inherited).

Choose any orthonormal basis of $W^\perp$ and let B be the matrix of g in this basis. Then $B \in \mathrm{Sym}_{n-1}(\mathbb{R})$. By the induction hypothesis, there exists an orthonormal basis $(v_2, \dots, v_n)$ of $W^\perp$ consisting of eigenvectors of g (equivalently, of f), with real eigenvalues $\lambda_2, \dots, \lambda_n$.

Step 4: Assemble the orthonormal eigenbasis. The family $(v_1, v_2, \dots, v_n)$ is orthonormal:

- $v_1 \perp v_j$ for $j \geq 2$, since $v_j \in W^\perp$;
- $(v_2, \dots, v_n)$ is orthonormal by the induction hypothesis;
- $\|v_1\| = 1$ by construction.

Each v_j is an eigenvector of A with eigenvalue λ_j. Let $P = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \end{pmatrix}$. Then $P \in \mathrm{O}(n)$ and $P^\intercal AP = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$. □

Remark 14 (Spectral decomposition form)

The Spectral Theorem can be rephrased as follows. If $A \in \mathrm{Sym}_n(\mathbb{R})$ has distinct eigenvalues $\mu_1, \dots, \mu_r$ with orthogonal projections P_i onto the eigenspace E_{μ_i}, then

$$A = \mu_1 P_1 + \mu_2 P_2 + \cdots + \mu_r P_r,$$

where $P_1 + \cdots + P_r = I_n$ and $P_i P_j = 0$ for $i \neq j$. This is called the *spectral decomposition* of A.

8.5 The Spectral Theorem for Hermitian matrices

The real Spectral Theorem extends naturally to the complex setting.

Theorem 15 (Spectral Theorem for Hermitian matrices)

Let $A \in \mathcal{M}_n(\mathbb{C})$ be Hermitian, i.e. $A^* = A$. Then:

(i) All eigenvalues of A are real.

(ii) There exists a unitary matrix $U \in \mathcal{M}_n(\mathbb{C})$ (i.e. $U^*U = I_n$) such that

$$U^* A U = \mathrm{diag}(\lambda_1, \dots, \lambda_n),$$

with $\lambda_1, \dots, \lambda_n \in \mathbb{R}$.

(iii) Equivalently, $\mathbb{C}^n$ has an orthonormal basis of eigenvectors of A.

Proof. The proof is identical to the real case: over $\mathbb{C}$ the characteristic polynomial always splits, so the base step of the induction is guaranteed. The self-adjointness condition $A^* = A$ ensures that eigenvalues are real (Theorem 7), eigenvectors for distinct eigenvalues are orthogonal (Theorem 9), and the orthogonal complement of an invariant subspace is invariant (Lemma 11). The inductive argument carries over verbatim, with "orthogonal matrix" replaced by "unitary matrix" and "transpose" replaced by "conjugate transpose." □

8.6 Orthogonal diagonalization: procedure and examples

The Spectral Theorem provides both a theoretical guarantee and a practical algorithm for orthogonally diagonalizing a symmetric matrix.

Remark 16 (Orthogonal diagonalization procedure)

Given $A \in \mathrm{Sym}_n(\mathbb{R})$:

1. Compute the characteristic polynomial $\chi_A(\lambda) = \det(A - \lambda I_n)$.
2. Find all eigenvalues $\lambda_1, \dots, \lambda_r$ (they are real).
3. For each λ_i, solve $(A - \lambda_i I_n)X = \mathbf{0}$ to find a basis of the eigenspace E_{λ_i}.
4. Apply the Gram–Schmidt process within each eigenspace to obtain an orthonormal basis of E_{λ_i}. (Eigenvectors from *different* eigenspaces are automatically orthogonal, so Gram–Schmidt is only needed within a single eigenspace when $\dim E_{\lambda_i} \geq 2$.)
5. Form P by placing the orthonormal eigenvectors as columns. Then $P \in \mathrm{O}(n)$ and $P^{\mathsf{T}}AP = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$.

Example 17 (Orthogonal diagonalization of a 2×2 matrix)

Diagonalize $A = \begin{pmatrix} 5 & 2 \\ 2 & 2 \end{pmatrix}$ orthogonally.

Step 1. $\chi_A(\lambda) = (5-\lambda)(2-\lambda) - 4 = \lambda^2 - 7\lambda + 6 = (\lambda - 1)(\lambda - 6)$.

Step 2. Eigenvalues: $\lambda_1 = 1$, $\lambda_2 = 6$.

Step 3. For $\lambda_1 = 1$: $(A - I_2)X = \mathbf{0}$ gives $\begin{pmatrix} 4 & 2 \\ 2 & 1 \end{pmatrix} X = \mathbf{0}$, so $2x + y = 0$. Eigenvector: $v_1 = \left(\begin{smallmatrix} 1 \\ -2 \end{smallmatrix}\right)$.

For $\lambda_2 = 6$: $(A - 6I_2)X = \mathbf{0}$ gives $\begin{pmatrix} -1 & 2 \\ 2 & -4 \end{pmatrix} X = \mathbf{0}$, so $x = 2y$. Eigenvector: $v_2 = \left(\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right)$.

Step 4. Normalise: $\hat{v}_1 = \frac{1}{\sqrt{5}}\left(\begin{smallmatrix} 1 \\ -2 \end{smallmatrix}\right)$, $\hat{v}_2 = \frac{1}{\sqrt{5}}\left(\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right)$.

Step 5. $P = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$ satisfies $P^{\mathsf{T}}AP = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$.

Example 18 (Orthogonal diagonalization of a 3×3 matrix)

Let $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$. One verifies that $A^{\mathsf{T}} = A$.

Characteristic polynomial: $\chi_A(\lambda) = -(\lambda - 4)(\lambda - 1)^2$.

Eigenvalues: $\lambda_1 = 4$ (multiplicity 1), $\lambda_2 = 1$ (multiplicity 2).

For $\lambda_1 = 4$*:* $(A - 4I_3)X = \mathbf{0}$ gives $x_1 = x_2 = x_3$, so $E_4 = \mathrm{Span}\left(\begin{pmatrix}1\\1\\1\end{pmatrix}\right)$. Normalise: $u_1 = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\1\end{pmatrix}$.

For $\lambda_2 = 1$*:* $(A - I_3)X = \mathbf{0}$ gives $x_1 + x_2 + x_3 = 0$, so $E_1 = \mathrm{Span}\left(\begin{pmatrix}1\\-1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\-1\end{pmatrix}\right)$. Apply Gram–Schmidt: $w_1 = \begin{pmatrix}1\\-1\\0\end{pmatrix}$, $w_2 = \begin{pmatrix}1\\0\\-1\end{pmatrix} - \frac{\langle w_1, \begin{pmatrix}1\\0\\-1\end{pmatrix}\rangle}{\langle w_1, w_1\rangle} w_1 = \begin{pmatrix}1/2\\1/2\\-1\end{pmatrix}$.

Normalise: $u_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\\0\end{pmatrix}$, $u_3 = \frac{1}{\sqrt{6}}\begin{pmatrix}1\\1\\-2\end{pmatrix}$.

The orthogonal matrix is $P = \begin{pmatrix}\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}}\\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}}\\ \frac{1}{\sqrt{3}} & 0 & -\frac{2}{\sqrt{6}}\end{pmatrix}$, and $P^{\mathsf{T}}AP = \mathrm{diag}(4, 1, 1)$.

8.7 Normal operators

Self-adjoint operators are a special case of a broader class.

Definition 19 (Normal operator)

An operator $f \in \mathrm{End}(E)$ is *normal* if it commutes with its adjoint:

$$f \circ f^* = f^* \circ f.$$

A matrix $A \in \mathcal{M}_n(\mathbb{C})$ is *normal* if $AA^* = A^*A$.

Example 20 (Classes of normal operators)

The following are all normal:

- Self-adjoint (symmetric / Hermitian) operators: $f^* = f$.
- Skew-adjoint operators: $f^* = -f$ (equivalently, $A^{\mathsf{T}} = -A$ over $\mathbb{R}$ or $A^* = -A$ over $\mathbb{C}$).
- Orthogonal / unitary operators: $f^* = f^{-1}$.

Proposition 21 (Characterization of normality)

Let $f \in \mathrm{End}(E)$ where E is a finite-dimensional inner product space over $\mathbb{C}$. The following are equivalent:

(i) f is normal.

(ii) $\|f(v)\| = \|f^*(v)\|$ for all $v \in E$.

(iii) If $f(v) = \lambda v$, then $f^*(v) = \bar{\lambda} v$. (That is, v is an eigenvector of f if and only if it is an eigenvector of f^*, with conjugate eigenvalue.)

Proof. (i)⇒(ii): $\|f(v)\|^2 = \langle f(v), f(v)\rangle = \langle f^*f(v), v\rangle = \langle ff^*(v), v\rangle = \langle f^*(v), f^*(v)\rangle = \|f^*(v)\|^2$.

(ii)⇒(iii): Assume $f(v) = \lambda v$. Apply (ii) to $f - \lambda\,\mathrm{Id}$ (which is also normal, as one verifies): $\|(f - \lambda\,\mathrm{Id})(v)\| = \|(f - \lambda\,\mathrm{Id})^*(v)\| = \|(f^* - \bar{\lambda}\,\mathrm{Id})(v)\|$. The left side is 0, so $f^*(v) = \bar{\lambda} v$.

(iii)⇒(i): We show $f^*f = ff^*$ by checking on an eigenbasis. Over $\mathbb{C}$, every normal operator is unitarily diagonalizable (see the next theorem), so this direction also follows. Alternatively, one can verify $\langle (f^*f - ff^*)(v), v\rangle = 0$ for all v using (iii) and polarization. □

Theorem 22 (Spectral Theorem for normal operators over $\mathbb{C}$)

Let $A \in \mathcal{M}_n(\mathbb{C})$ be normal. Then there exists a unitary matrix U such that

$$U^* A U = \operatorname{diag}(\lambda_1, \dots, \lambda_n),$$

where $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ are the eigenvalues of A.
Conversely, every unitarily diagonalizable matrix is normal.

Proof. Forward direction. By induction on n. The case $n = 1$ is trivial. For the inductive step, since $\mathbb{C}$ is algebraically closed, A has an eigenvalue λ_1 with unit eigenvector v_1. Let $W = \operatorname{Span}(v_1)$.

Claim: $W^\perp$ is A-invariant. Let $u \in W^\perp$. We need $Au \perp v_1$, i.e. $\langle Au, v_1\rangle = 0$. Now $\langle Au, v_1\rangle = \langle u, A^*v_1\rangle = \langle u, \bar{\lambda}_1 v_1\rangle = \lambda_1 \langle u, v_1\rangle = 0$, where we used Proposition 21 (iii): since $Av_1 = \lambda_1 v_1$, we have $A^*v_1 = \bar{\lambda}_1 v_1$.

The restriction $A|_{W^\perp}$ is normal on the $(n-1)$-dimensional space $W^\perp$. By the induction hypothesis it is unitarily diagonalizable. Assembling the eigenvectors gives a unitary matrix U diagonalizing A.

Converse. If $A = UDU^*$ with D diagonal and U unitary, then $A^* = U\bar{D}U^*$. Since diagonal matrices commute, $AA^* = UD\bar{D}U^* = U\bar{D}DU^* = A^*A$. □

Remark 23 (Normal operators over $\mathbb{R}$)

Over $\mathbb{R}$, normal operators need not be orthogonally diagonalizable. For instance, the rotation matrix $R_\theta = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right)$ is normal (in fact orthogonal) but has no real eigenvalues when $\theta \notin \{0, \pi\}$. The real spectral theorem for normal operators states that such a matrix can be brought to a block-diagonal form with 1×1 real blocks and 2×2 rotation blocks.

8.8 Positive definite and positive semidefinite matrices

Definition 24 (Positive definite and positive semidefinite matrices)

A real symmetric matrix $A \in \operatorname{Sym}_n(\mathbb{R})$ is:

- *positive definite* if $x^{\mathsf{T}}Ax > 0$ for all $x \in \mathbb{R}^n \setminus \{\mathbf{0}\}$;
- *positive semidefinite* if $x^{\mathsf{T}}Ax \geq 0$ for all $x \in \mathbb{R}^n$;
- *negative definite* if $-A$ is positive definite;
- *negative semidefinite* if $-A$ is positive semidefinite;
- *indefinite* if $x^{\mathsf{T}}Ax$ takes both positive and negative values.

Theorem 25 (Characterizations of positive definiteness)

For $A \in \operatorname{Sym}_n(\mathbb{R})$ the following are equivalent:

(i) A is positive definite.

(ii) All eigenvalues of A are strictly positive.

(iii) All leading principal minors of A are strictly positive (*Sylvester's criterion*).

(iv) There exists an invertible matrix $L \in \mathcal{M}_n(\mathbb{R})$ such that $A = L^{\mathsf{T}} L$.

(v) A admits a *Cholesky decomposition*: there exists a unique lower triangular matrix L with strictly positive diagonal entries such that $A = LL^{\mathsf{T}}$.

Proof. (i)⇒(ii): If λ is an eigenvalue with eigenvector v, then $0 < v^{\mathsf{T}}Av = \lambda v^{\mathsf{T}}v = \lambda\|v\|^2$, so $\lambda > 0$.

(ii)⇒(i): By the Spectral Theorem, $A = P\,D\,P^{\mathsf{T}}$ with P orthogonal and $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$. For $x \neq \mathbf{0}$, let $y = P^{\mathsf{T}}x \neq \mathbf{0}$. Then $x^{\mathsf{T}}Ax = y^{\mathsf{T}}Dy = \sum_{i=1}^{n} \lambda_i y_i^2 > 0$ since all $\lambda_i > 0$ and $y \neq \mathbf{0}$.

(i)⇒(iii) (*Sylvester's criterion*): The k-th leading principal minor Δ_k equals the determinant of the $k \times k$ upper-left submatrix A_k. But A_k is itself symmetric, and for any $x \in \mathbb{R}^k \setminus \{\mathbf{0}\}$ we have $x^{\mathsf{T}}A_k x = \tilde{x}^{\mathsf{T}}A\tilde{x} > 0$, where $\tilde{x} = (x_1, \dots, x_k, 0, \dots, 0)^T$. Hence A_k is positive definite, so its eigenvalues are positive, so $\Delta_k = \det(A_k) > 0$.

(iii)⇒(i): By induction on n. For $n = 1$, $\Delta_1 = a_{11} > 0$, so $A = (a_{11})$ is positive definite. For the inductive step, write $A = \left(\begin{smallmatrix} A_{n-1} & b \\ b^{\mathsf{T}} & a_{nn} \end{smallmatrix}\right)$. By induction, A_{n-1} is positive definite. Performing one step of block Gaussian elimination (valid since $\det(A_{n-1}) = \Delta_{n-1} > 0$):

$$A = \begin{pmatrix} I & 0 \\ b^{\mathsf{T}}{A_{n-1}}^{-1} & 1 \end{pmatrix} \begin{pmatrix} A_{n-1} & 0 \\ 0 & s \end{pmatrix} \begin{pmatrix} I & {A_{n-1}}^{-1}b \\ 0 & 1 \end{pmatrix},$$

where $s = a_{nn} - b^{\mathsf{T}}{A_{n-1}}^{-1}b = \det(A)/\det(A_{n-1}) = \Delta_n/\Delta_{n-1} > 0$. This expresses $A = M^{\mathsf{T}}\left(\begin{smallmatrix} A_{n-1} & 0 \\ 0 & s \end{smallmatrix}\right)M$ with M invertible. For $x \neq \mathbf{0}$, $x^{\mathsf{T}}Ax = (Mx)^{\mathsf{T}}\left(\begin{smallmatrix} A_{n-1} & 0 \\ 0 & s \end{smallmatrix}\right)(Mx) > 0$ since the block-diagonal matrix is positive definite.

(ii)⇒(iv): By the Spectral Theorem, $A = PDP^{\mathsf{T}}$, so $A = PD^{1/2}(PD^{1/2})^{\mathsf{T}} = L^{\mathsf{T}}L$ where $L = D^{1/2}P^{\mathsf{T}}$.

(iv)⇒(i): $x^{\mathsf{T}}Ax = x^{\mathsf{T}}L^{\mathsf{T}}Lx = \|Lx\|^2 > 0$ since L is invertible and $x \neq \mathbf{0}$.

The existence and uniqueness of the Cholesky factorization (v) is proved by an explicit recursive construction using the positive leading principal minors (we omit the details). □

Example 26 (Testing positive definiteness)

Consider $A = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$.

Via eigenvalues: $\chi_A(\lambda) = (\lambda - 1)(\lambda - 3)$, so $\lambda_1 = 1 > 0$ and $\lambda_2 = 3 > 0$. Hence A is positive definite.

Via Sylvester's criterion: $\Delta_1 = 2 > 0$, $\Delta_2 = \det(A) = 3 > 0$. Positive definite.

Cholesky decomposition: $A = \begin{pmatrix} \sqrt{2} & 0 \\ -\frac{1}{\sqrt{2}} & \frac{\sqrt{3}}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \sqrt{2} & -\frac{1}{\sqrt{2}} \\ 0 & \frac{\sqrt{3}}{\sqrt{2}} \end{pmatrix} = LL^{\mathsf{T}}$.

Proposition 27 (Characterization of positive semidefiniteness)

For $A \in \operatorname{Sym}_n(\mathbb{R})$ the following are equivalent:

(i) A is positive semidefinite.

(ii) All eigenvalues of A are nonnegative.

(iii) There exists a matrix $B \in \mathcal{M}_n(\mathbb{R})$ such that $A = B^{\mathsf{T}}B$.

(iv) All principal minors of A are nonnegative.

Proof. The proofs are analogous to Theorem 25, with strict inequalities relaxed to non-strict ones. For (ii)⇒(iii), use the spectral decomposition $A = PDP^{\mathsf{T}}$ and set $B = D^{1/2}P^{\mathsf{T}}$ (noting $D^{1/2}$ is well-defined since all diagonal entries are nonnegative). □

8.9 Singular Value Decomposition

The Spectral Theorem applies to symmetric (or Hermitian) matrices. The *Singular Value Decomposition* (SVD) extends the idea of diagonalization to *arbitrary* matrices, including rectangular ones.

Definition 28 (Singular values)

Let $A \in \mathcal{M}_{m\times n}(\mathbb{R})$. The *singular values* of A are the nonnegative square roots of the eigenvalues of the positive semidefinite matrix $A^{\mathsf{T}}A \in \mathrm{Sym}_n(\mathbb{R})$:

$$\sigma_i := \sqrt{\lambda_i(A^{\mathsf{T}}A)}, \qquad i = 1, \dots, n,$$

ordered so that $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n \geq 0$.

Theorem 29 (Singular Value Decomposition)

Let $A \in \mathcal{M}_{m\times n}(\mathbb{R})$ with $\mathrm{rank}(A) = r$. Then there exist:

- an orthogonal matrix $U \in \mathrm{O}(m)$ (left singular vectors),
- an orthogonal matrix $V \in \mathrm{O}(n)$ (right singular vectors),
- a "diagonal" matrix $\Sigma \in \mathcal{M}_{m\times n}(\mathbb{R})$ with $\Sigma_{ii} = \sigma_i$ for $i = 1, \dots, \min(m, n)$ and all other entries zero,

such that

$$A = U\,\Sigma\,V^{\mathsf{T}}.$$

The nonzero singular values $\sigma_1 \geq \cdots \geq \sigma_r > 0$ are uniquely determined. Moreover,

$$A = \sum_{i=1}^{r} \sigma_i\, u_i\, v_i^{\mathsf{T}},$$

where u_i and v_i are the i-th columns of U and V.

Proof sketch. The matrix $A^{\mathsf{T}}A \in \mathrm{Sym}_n(\mathbb{R})$ is positive semidefinite (Proposition 27). By the Spectral Theorem, there exists an orthogonal matrix V such that $V^{\mathsf{T}}A^{\mathsf{T}}AV = \mathrm{diag}(\sigma_1^2, \dots, \sigma_n^2)$ with $\sigma_1 \geq \cdots \geq \sigma_r > 0 = \sigma_{r+1} = \cdots = \sigma_n$.

Define $u_i = \frac{1}{\sigma_i}Av_i$ for $i = 1, \dots, r$. These are orthonormal:

$$\langle u_i, u_j\rangle = \frac{1}{\sigma_i\sigma_j}\langle Av_i, Av_j\rangle = \frac{1}{\sigma_i\sigma_j} v_i^{\mathsf{T}}A^{\mathsf{T}}Av_j = \frac{\sigma_j^2}{\sigma_i\sigma_j}\delta_{ij} = \delta_{ij}.$$

Extend $(u_1, \dots, u_r)$ to an orthonormal basis $(u_1, \dots, u_m)$ of $\mathbb{R}^m$, and set $U = \begin{pmatrix} u_1 & \cdots & u_m \end{pmatrix}$.

By construction, $AV = U\Sigma$ (checking on each column of V), so $A = U\Sigma V^{\mathsf{T}}$. □

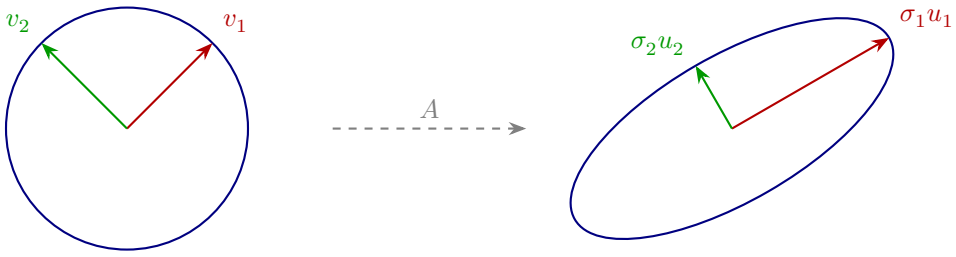


Figure 8.2: Geometric interpretation of the SVD. The linear map A sends the unit sphere to an ellipsoid. The right singular vectors v_i are mapped to the principal axes $\sigma_i u_i$ of the ellipsoid.

Example 30 (SVD of a 2×2 matrix)

Let $A = \begin{pmatrix} 3 & 0 \\ 0 & -2 \end{pmatrix}$. Then $A^\mathsf{T} A = \begin{pmatrix} 9 & 0 \\ 0 & 4 \end{pmatrix}$, with eigenvalues 9 and 4, so $\sigma_1 = 3$, $\sigma_2 = 2$.
The right singular vectors are $v_1 = \mathbf{e}_1$, $v_2 = \mathbf{e}_2$. The left singular vectors are $u_1 = \frac{1}{3} A v_1 = \mathbf{e}_1$, $u_2 = \frac{1}{2} A v_2 = -\mathbf{e}_2$.
Thus $A = U \Sigma V^\mathsf{T}$ with $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $\Sigma = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, $V = I_2$.

Proposition 31 (Properties of the SVD)

Let $A = U \Sigma V^\mathsf{T}$ be the SVD of $A \in \mathcal{M}_{m \times n}(\mathbb{R})$ with $\operatorname{rank}(A) = r$.

(i) $\operatorname{rank}(A)$ equals the number of nonzero singular values.

(ii) $\|A\|_2 = \sigma_1$ (operator norm) and $\|A\|_F = \sqrt{\sigma_1^2 + \cdots + \sigma_r^2}$ (Frobenius norm).

(iii) $\operatorname{Im}(A) = \operatorname{Span}(u_1, \dots, u_r)$ and $\operatorname{Ker}(A) = \operatorname{Span}(v_{r+1}, \dots, v_n)$.

(iv) If A is square and invertible, $A^{-1} = V \Sigma^{-1} U^\mathsf{T}$ and the condition number is $\kappa(A) = \sigma_1 / \sigma_n$.

Proof. (i) follows from $\operatorname{rank}(A) = \operatorname{rank}(A^\mathsf{T} A)$ (the nonzero eigenvalues of $A^\mathsf{T} A$ are $\sigma_1^2, \dots, \sigma_r^2$). (ii)–(iv) follow directly from the decomposition $A = U \Sigma V^\mathsf{T}$. □

8.10 Applications

8.10.1 Principal Component Analysis

Given data points $x_1, \dots, x_N \in \mathbb{R}^n$ (centered so that $\sum x_i = \mathbf{0}$), the *sample covariance matrix* is

$$S = \frac{1}{N-1} \sum_{i=1}^{N} x_i x_i^\mathsf{T} \in \operatorname{Sym}_n(\mathbb{R}).$$

Since S is symmetric and positive semidefinite, the Spectral Theorem gives $S = P \operatorname{diag}(\lambda_1, \dots, \lambda_n) P^\mathsf{T}$ with $\lambda_1 \geq \cdots \geq \lambda_n \geq 0$. The columns of P are the *principal components*: the first principal component p_1 maximizes the variance $p^\mathsf{T} S p$ over unit vectors p, the second maximizes the variance orthogonally to p_1, and so on.

Dimensionality reduction to k components amounts to projecting onto $\operatorname{Span}(p_1, \dots, p_k)$, retaining a fraction $\frac{\lambda_1 + \cdots + \lambda_k}{\lambda_1 + \cdots + \lambda_n}$ of the total variance.

8.10.2 Classification of quadratic forms

A *quadratic form* on $\mathbb{R}^n$ is a function $Q(x) = x^{\mathsf{T}} A x$ where $A \in \mathrm{Sym}_n(\mathbb{R})$ (since only the symmetric part of a matrix contributes to the quadratic form). By the Spectral Theorem, there is an orthogonal change of variables $x = Py$ that diagonalizes Q:

$$Q(x) = y^{\mathsf{T}} \operatorname{diag}(\lambda_1, \dots, \lambda_n)\, y = \lambda_1 y_1^2 + \cdots + \lambda_n y_n^2.$$

The *signature* (p, q) — where p is the number of positive λ_i and q the number of negative ones — classifies the quadratic form up to congruence (Sylvester's law of inertia).

8.10.3 Second-order optimality conditions

Let $f\colon \mathbb{R}^n \to \mathbb{R}$ be C^2. At a critical point x_0 ($\nabla f(x_0) = \mathbf{0}$), the Hessian $H = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}(x_0)\right)$ is symmetric. By the Spectral Theorem:

- H positive definite $\Rightarrow$ x_0 is a strict local minimum.
- H negative definite $\Rightarrow$ x_0 is a strict local maximum.
- H indefinite $\Rightarrow$ x_0 is a saddle point.

8.10.4 Vibrations and normal modes

A coupled system of n harmonic oscillators (masses connected by springs) leads to the equation $M\ddot{x} + Kx = \mathbf{0}$, where $M, K \in \mathrm{Sym}_n(\mathbb{R})$ are the mass and stiffness matrices (both positive definite). Setting $y = M^{1/2}x$ transforms this into $\ddot{y} + M^{-1/2} K M^{-1/2} y = \mathbf{0}$.

The symmetric matrix $\tilde{K} = M^{-1/2} K M^{-1/2}$ has positive eigenvalues $\omega_1^2 \le \cdots \le \omega_n^2$; the ω_i are the *natural frequencies* and the corresponding eigenvectors (transformed back via $M^{-1/2}$) are the *normal modes* of the system.

8.11 Exercises

Exercise 32 (Eigenvalues of a symmetric matrix)

Let $A = \begin{pmatrix} 4 & 2 \\ 2 & 1 \end{pmatrix}$.

(a) Find the eigenvalues of A and verify they are real.

(b) Find an orthonormal basis of eigenvectors.

(c) Write $A = PDP^{\mathsf{T}}$ with P orthogonal and D diagonal.

Exercise 33 (Orthogonal diagonalization)

Orthogonally diagonalize $A = \begin{pmatrix} 6 & -2 \\ -2 & 3 \end{pmatrix}$.

Exercise 34 (A 3×3 symmetric matrix)

Let $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$. Find the eigenvalues, eigenspaces, and an orthogonal matrix P such that $P^{\mathsf{T}}AP$ is diagonal.

Exercise 35 (Proof practice: eigenvalues of A^2)

Let $A \in \mathrm{Sym}_n(\mathbb{R})$ with eigenvalues $\lambda_1, \dots, \lambda_n$. Prove that the eigenvalues of A^2 are $\lambda_1^2, \dots, \lambda_n^2$.

Exercise 36 (Positive definiteness tests)

Determine whether each matrix is positive definite, positive semidefinite, or neither:

(a) $A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$.

(b) $B = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

(c) $C = \begin{pmatrix} 4 & 2 & 0 \\ 2 & 5 & 3 \\ 0 & 3 & 6 \end{pmatrix}$.

Exercise 37 (Cholesky decomposition)

Compute the Cholesky decomposition $A = LL^{\mathsf{T}}$ for $A = \begin{pmatrix} 4 & 2 \\ 2 & 5 \end{pmatrix}$. Verify your answer.

Exercise 38 (SVD computation)

Compute the SVD of $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Exercise 39 (Spectral decomposition)

Let $A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$. Write A in spectral decomposition form $A = \lambda_1 P_1 + \lambda_2 P_2$, where P_1, P_2 are the orthogonal projections onto the eigenspaces. Verify that $P_1 + P_2 = I_2$ and $P_1 P_2 = 0$.

Exercise 40 (Normal but not self-adjoint)

Let $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

(a) Show that A is normal.

(b) Show that A has no real eigenvalues, hence is not orthogonally diagonalizable over $\mathbb{R}$.

(c) Find the eigenvalues over $\mathbb{C}$ and a unitary matrix U such that U^*AU is diagonal.

Exercise 41 (Simultaneous diagonalization)

Let $A, B \in \mathrm{Sym}_n(\mathbb{R})$ with $AB = BA$. Prove that A and B can be *simultaneously* orthogonally diagonalized, i.e. there exists $P \in \mathrm{O}(n)$ such that both $P^{\mathsf{T}}AP$ and $P^{\mathsf{T}}BP$ are diagonal.
Hint: Show that each eigenspace of A is invariant under B, then apply the Spectral Theorem to the restriction of B to each eigenspace.

Exercise 42 (Low-rank approximation via SVD)

Let $A \in \mathcal{M}_{m\times n}(\mathbb{R})$ with SVD $A = \sum_{i=1}^{r} \sigma_i\, u_i v_i^{\mathsf{T}}$. Define $A_k = \sum_{i=1}^{k} \sigma_i\, u_i v_i^{\mathsf{T}}$ for $k \le r$.

(a) Show that $\operatorname{rank}(A_k) = k$.

(b) Prove the Eckart–Young theorem: among all matrices of rank at most k, A_k minimises $\|A - B\|_F$, and the minimum value is $\sqrt{\sigma_{k+1}^2 + \cdots + \sigma_r^2}$.

Exercise 43 (Rayleigh quotient and eigenvalue bounds)

For $A \in \mathrm{Sym}_n(\mathbb{R})$, the *Rayleigh quotient* is $R(x) = \frac{x^{\mathsf{T}}Ax}{x^{\mathsf{T}}x}$ for $x \neq \mathbf{0}$.

(a) Prove that $\lambda_{\min}(A) \le R(x) \le \lambda_{\max}(A)$.

(b) Prove that $\max_{x\neq\mathbf{0}} R(x) = \lambda_{\max}(A)$ and $\min_{x\neq\mathbf{0}} R(x) = \lambda_{\min}(A)$, and identify the optimisers.

(c) (*Courant–Fischer minimax theorem*) Prove that the k-th largest eigenvalue satisfies

$$\lambda_k = \max_{\dim W = k}\ \min_{x\in W,\, x\neq\mathbf{0}} R(x) = \min_{\dim W = n-k+1}\ \max_{x\in W,\, x\neq\mathbf{0}} R(x).$$

8.12 Chapter summary

1. **Self-adjoint operators.** An operator f is self-adjoint if $f^* = f$; in an orthonormal basis, this corresponds to symmetric ($A^{\mathsf{T}} = A$) or Hermitian ($A^* = A$) matrices.

2. **Eigenvalues are real.** Every eigenvalue of a self-adjoint operator is a real number.

3. **Orthogonal eigenvectors.** Eigenvectors corresponding to distinct eigenvalues of a self-adjoint operator are orthogonal.

4. **Spectral Theorem (real).** Every real symmetric matrix is orthogonally diagonalizable: $A = P\,\mathrm{diag}(\lambda_1, \dots, \lambda_n)P^{\mathsf{T}}$ with $P \in \mathrm{O}(n)$.

5. **Spectral Theorem (complex).** Every Hermitian matrix is unitarily diagonalizable with real eigenvalues.

6. **Normal operators.** An operator is normal if $ff^* = f^*f$. Over $\mathbb{C}$, normal operators are precisely the unitarily diagonalizable ones.

7. **Positive definiteness.** $A \in \mathrm{Sym}_n(\mathbb{R})$ is positive definite if and only if all eigenvalues are positive, if and only if all leading principal minors are positive (Sylvester's criterion).

8. **SVD.** Every $m \times n$ matrix admits a decomposition $A = U\Sigma V^{\mathsf{T}}$ with U, V orthogonal and Σ "diagonal." The singular values are the square roots of the eigenvalues of $A^{\mathsf{T}}A$.

9. **Applications.** The Spectral Theorem underlies PCA, quadratic form classification, second-order optimality conditions, and the analysis of coupled vibrations.

Chapter 9

Jordan Normal Form

In Chapter 6 we saw that a matrix is diagonalizable if and only if the algebraic and geometric multiplicities of every eigenvalue coincide. When they do, one obtains the simplest possible matrix representation — a diagonal matrix. But what happens when diagonalization *fails*?

Consider the matrix $A = \left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right)$. Its only eigenvalue is $\lambda = 2$ with algebraic multiplicity 2, yet the eigenspace $E_2(A) = \operatorname{Span}\left(\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)\right)$ has dimension 1. There is no basis of $\mathbb{R}^2$ consisting of eigenvectors of A, so A is not diagonalizable. Nevertheless, A is already in a rather pleasant form: it is "almost diagonal," differing from $\operatorname{diag}(2, 2)$ by a single off-diagonal entry. Is this an accident, or can every matrix be brought into a similarly nice shape?

The answer is provided by the *Jordan normal form*, one of the most powerful results in linear algebra. It asserts that over an algebraically closed field (such as $\mathbb{C}$), every square matrix is similar to an essentially unique matrix built from simple building blocks called *Jordan blocks*. This canonical form completely determines the matrix up to similarity and provides a systematic way to handle all the phenomena that arise when diagonalization fails.

The Jordan form has far-reaching applications: it yields explicit formulas for matrix powers and matrix exponentials, it explains the structure of solutions to linear systems of differential equations with non-diagonalizable coefficient matrices, and it clarifies the relationship between the characteristic and minimal polynomials.

Throughout this chapter, unless stated otherwise, $\mathbb{K}$ denotes an algebraically closed field (typically $\mathbb{K} = \mathbb{C}$), E is a finite-dimensional $\mathbb{K}$-vector space with $\dim E = n$, and $f \in \operatorname{End}(E)$. We freely use results from Chapter 6, especially the notions of eigenvalue, eigenspace, characteristic polynomial, and minimal polynomial.

9.1 Nilpotent endomorphisms

The key to understanding non-diagonalizable maps is to understand a special class of endomorphisms that are "as far from diagonalizable as possible" (aside from the zero map): the *nilpotent* endomorphisms.

Definition 1 (Nilpotent endomorphism)

An endomorphism $f \in \operatorname{End}(E)$ is called *nilpotent* if there exists an integer $p \geq 1$ such that $f^p = 0$ (the zero endomorphism). A matrix $A \in \mathcal{M}_n(\mathbb{K})$ is *nilpotent* if $A^p = 0$ for some $p \geq 1$.

Definition 2 (Index of nilpotency)

If $f \in \mathrm{End}(E)$ is nilpotent, the *index of nilpotency* (or *nilpotency index*) of f is the smallest positive integer r such that $f^r = 0$. We then have

$$f^{r-1} \neq 0 \quad \text{and} \quad f^r = 0.$$

Proposition 3 (Basic properties of nilpotent endomorphisms)

Let $f \in \mathrm{End}(E)$ be nilpotent with $\dim E = n$. Then:

(i) The only eigenvalue of f is $\lambda = 0$.

(ii) $\mathrm{tr}(f) = 0$.

(iii) $\det(f) = 0$; in particular, f is not invertible.

(iv) The characteristic polynomial of f is $\chi_f(\lambda) = (-\lambda)^n$.

(v) The index of nilpotency satisfies $r \leq n$.

(vi) The minimal polynomial of f is $\mu_f(\lambda) = (-\lambda)^r$, where r is the index of nilpotency.

Proof. (i) Suppose $f(v) = \lambda v$ for some $v \neq 0$. Then $f^p(v) = \lambda^p v$, so $f^p = 0$ implies $\lambda^p v = 0$, hence $\lambda^p = 0$ (since $v \neq 0$), so $\lambda = 0$.

(ii) and (iii) Since f is trigonalizable (every endomorphism over $\mathbb{C}$ is, and the argument extends because all eigenvalues are 0), there exists a basis in which the matrix of f is upper triangular with all diagonal entries equal to 0. Hence $\mathrm{tr}(f) = 0$ and $\det(f) = 0$.

(iv) From the triangular form, $\chi_f(\lambda) = (0 - \lambda)^n = (-\lambda)^n$.

(v) By Cayley–Hamilton, $\chi_f(f) = 0$, i.e. $(-1)^n f^n = 0$, so $f^n = 0$. The index of nilpotency, being the smallest such exponent, satisfies $r \leq n$.

(vi) Since $\chi_f(\lambda) = (-\lambda)^n$ and the minimal polynomial divides the characteristic polynomial and has the same roots, we have $\mu_f(\lambda) = (-\lambda)^s$ for some $1 \leq s \leq n$. By definition, $\mu_f(f) = 0$ means $f^s = 0$, and s is minimal with this property. Hence $s = r$. □

Example 4 (Nilpotent matrices)

(a) The matrix $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ satisfies $N^2 = 0$, so it is nilpotent with index 2.

(b) The matrix $N = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ satisfies $N^2 \neq 0$ but $N^3 = 0$, so it is nilpotent with index 3.

(c) The zero matrix 0_n is nilpotent with index 1.

(d) The matrix $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ is nilpotent with index 2.

Proposition 5 (Kernel filtration of a nilpotent endomorphism)

Let $f \in \mathrm{End}(E)$ be nilpotent with index of nilpotency r. Then

$$\{\mathbf{0}\} \subsetneq \mathrm{Ker}(f) \subsetneq \mathrm{Ker}(f^2) \subsetneq \cdots \subsetneq \mathrm{Ker}(f^{r-1}) \subsetneq \mathrm{Ker}(f^r) = E.$$

In particular, each inclusion is strict, and $\dim \mathrm{Ker}(f^k) \geq k$ for all $1 \leq k \leq r$.

Proof. The inclusions $\mathrm{Ker}(f^k) \subseteq \mathrm{Ker}(f^{k+1})$ follow from the fact that $f^k(v) = 0$ implies $f^{k+1}(v) = f(f^k(v)) = f(0) = 0$. Since $f^r = 0$, we have $\mathrm{Ker}(f^r) = E$. It remains to show that each inclusion is strict.

Suppose for contradiction that $\mathrm{Ker}(f^k) = \mathrm{Ker}(f^{k+1})$ for some $k < r$. We claim this forces $\mathrm{Ker}(f^k) = \mathrm{Ker}(f^{k+j})$ for all $j \geq 0$. Indeed, let $v \in \mathrm{Ker}(f^{k+2})$, so $f^{k+2}(v) = 0$, meaning $f(v) \in \mathrm{Ker}(f^{k+1}) = \mathrm{Ker}(f^k)$, hence $f^{k+1}(v) = f^k(f(v)) = 0$, so $v \in \mathrm{Ker}(f^{k+1}) = \mathrm{Ker}(f^k)$. By induction, $\mathrm{Ker}(f^k) = \mathrm{Ker}(f^m)$ for all $m \geq k$. In particular, $\mathrm{Ker}(f^k) = \mathrm{Ker}(f^r) = E$, so $f^k = 0$, contradicting the minimality of r since $k < r$.

Since the inclusions are strict in a space of dimension n, at each step the dimension increases by at least 1, giving $\dim \mathrm{Ker}(f^k) \geq k$. □

9.2 Invariant subspaces

Definition 6 (Invariant subspace)

Let $f \in \mathrm{End}(E)$ and let $F \subseteq E$ be a subspace. We say that F is *f-invariant* (or *invariant under f*) if $f(F) \subseteq F$, i.e. $f(v) \in F$ for every $v \in F$.

Remark 7 (Restriction to an invariant subspace)

If F is f-invariant, then f restricts to a well-defined endomorphism $f|_F \in \mathrm{End}(F)$. This simple observation is the key to decomposing endomorphisms into simpler pieces.

Proposition 8 (Examples of invariant subspaces)

Let $f \in \mathrm{End}(E)$. The following are f-invariant subspaces:

(i) $\{\mathbf{0}\}$ and E (trivial invariant subspaces).

(ii) $\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$.

(iii) More generally, $\mathrm{Ker}(f^k)$ and $\mathrm{Im}(f^k)$ for every $k \geq 1$.

(iv) Every eigenspace $E_\lambda(f) = \mathrm{Ker}(f - \lambda \,\mathrm{Id})$.

(v) $\mathrm{Ker}(P(f))$ for any polynomial $P \in \mathbb{K}[\lambda]$.

Proof. We prove (v), which implies the others as special cases. Let $P \in \mathbb{K}[\lambda]$ and $v \in \mathrm{Ker}(P(f))$, so $P(f)(v) = 0$. Since f commutes with $P(f)$ (both are polynomials in f), we have

$$P(f)(f(v)) = f(P(f)(v)) = f(0) = 0,$$

so $f(v) \in \mathrm{Ker}(P(f))$. □

Proposition 9 (Block-diagonal structure from invariant decomposition)

Let $E = F_1 \oplus F_2 \oplus \cdots \oplus F_s$ where each F_i is f-invariant. If $\mathcal{B}_i$ is a basis of F_i and $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_s$ is the resulting basis of E, then the matrix of f in $\mathcal{B}$ is block-diagonal:

$$\mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_s \end{pmatrix},$$

where $A_i = \mathrm{Mat}_{\mathcal{B}_i}(f|_{F_i})$. Moreover, $\chi_f = \chi_{f|_{F_1}} \cdots \chi_{f|_{F_s}}$.

Proof. Since each F_i is f-invariant, f maps basis vectors of $\mathcal{B}_i$ to linear combinations of vectors in $\mathcal{B}_i$ only. Hence the matrix has the stated block-diagonal form. The factorization of the characteristic polynomial follows from the multiplicativity of determinants for block-diagonal matrices. □

9.3 Generalized eigenspaces

When the ordinary eigenspace $E_\lambda(f) = \mathrm{Ker}(f - \lambda\,\mathrm{Id})$ is too small (i.e. $\dim E_\lambda(f) < m_a(\lambda)$), we enlarge it by looking at the kernels of higher powers of $f - \lambda\,\mathrm{Id}$.

Definition 10 (Generalized eigenvector and generalized eigenspace)

Let $f \in \mathrm{End}(E)$ and $\lambda \in \mathbb{K}$. A nonzero vector $v \in E$ is a *generalized eigenvector* of f for the eigenvalue λ if there exists an integer $k \geq 1$ such that

$$(f - \lambda\,\mathrm{Id})^k(v) = 0.$$

The *generalized eigenspace* of f for λ is

$$G_\lambda(f) := \bigcup_{k=1}^{\infty} \mathrm{Ker}((f - \lambda\,\mathrm{Id})^k).$$

Remark 11 (Stabilization of the kernel chain)

Since $\dim E = n$ is finite, the ascending chain $\mathrm{Ker}(f - \lambda\,\mathrm{Id}) \subseteq \mathrm{Ker}(f - \lambda\,\mathrm{Id})^2 \subseteq \cdots$ must stabilize at some index $k_0 \leq n$. Therefore

$$G_\lambda(f) = \mathrm{Ker}((f - \lambda\,\mathrm{Id})^{k_0})$$

for some $k_0 \leq n$, and the union in the definition is in fact achieved at a finite stage.

Proposition 12 (Properties of generalized eigenspaces)

Let $f \in \mathrm{End}(E)$ and suppose χ_f splits over $\mathbb{K}$ as

$$\chi_f(\lambda) = \prod_{i=1}^{s} (\lambda_i - \lambda)^{n_i},$$

where $\lambda_1, \ldots, \lambda_s$ are the distinct eigenvalues and $n_i = m_a(\lambda_i)$ is the algebraic multiplicity. Then:

(i) Each $G_{\lambda_i}(f)$ is f-invariant.

(ii) $\dim G_{\lambda_i}(f) = n_i$.

(iii) $G_{\lambda_i}(f) = \operatorname{Ker}((f - \lambda_i \operatorname{Id})^{n_i})$.

(iv) The restriction $(f - \lambda_i \operatorname{Id})|_{G_{\lambda_i}(f)}$ is nilpotent.

(v) The generalized eigenspaces are in direct sum:

$$E = G_{\lambda_1}(f) \oplus G_{\lambda_2}(f) \oplus \cdots \oplus G_{\lambda_s}(f).$$

Proof. (i) This follows from Proposition 8, since $G_\lambda(f) = \operatorname{Ker}((f-\lambda \operatorname{Id})^k)$ for sufficiently large k, and the kernel of any polynomial in f is f-invariant.

We prove (ii), (iii), and (v) together using the primary decomposition theorem.

Write $\chi_f(\lambda) = \prod_{i=1}^{s}(\lambda_i - \lambda)^{n_i}$. Define the polynomials $P_i(\lambda) = (\lambda_i - \lambda)^{n_i}$ and $Q_i(\lambda) = \prod_{j\neq i}(\lambda_j - \lambda)^{n_j}$. Then $\gcd(P_i, Q_i) = 1$ since the λ_j are distinct. By Bézout's identity in $\mathbb{K}[\lambda]$, there exist polynomials U_i, V_i such that $U_iP_i + V_iQ_i = 1$.

By Cayley–Hamilton, $\chi_f(f) = 0$, i.e. $P_i(f)\,Q_i(f) = 0$ on $G_{\lambda_i}(f)$, and indeed $\prod_{i=1}^{s} P_i(f) = 0$ on all of E.

From $U_i(f)P_i(f)+V_i(f)Q_i(f) = \operatorname{Id}$, for any $v \in E$ we have $v = U_i(f)P_i(f)(v)+V_i(f)Q_i(f)(v)$. One checks that $V_i(f)Q_i(f)(v) \in \operatorname{Ker}(P_i(f)) = \operatorname{Ker}((f - \lambda_i \operatorname{Id})^{n_i})$ by applying $P_i(f)$ and using $P_i(f)Q_i(f) = \chi_f(f) = 0$. Similarly, $U_i(f)P_i(f)(v) \in \operatorname{Ker}(Q_i(f))$.

Define $\pi_i = V_i(f)Q_i(f)$. Then $\sum_{i=1}^{s} \pi_i = \operatorname{Id}$, each π_i maps E into $\operatorname{Ker}(P_i(f)) = G_{\lambda_i}(f)$, and $\pi_i\pi_j = 0$ for $i \neq j$. This gives the direct sum decomposition $E = \bigoplus_{i=1}^{s} G_{\lambda_i}(f)$.

For the dimensions, since $\chi_{f|_{G_{\lambda_i}(f)}}$ divides χ_f and the only eigenvalue of f on $G_{\lambda_i}(f)$ is λ_i, we get $\chi_{f|_{G_{\lambda_i}(f)}}(\lambda) = (\lambda_i - \lambda)^{d_i}$ with $d_i = \dim G_{\lambda_i}(f)$. Since $\chi_f = \prod_i \chi_{f|_{G_{\lambda_i}(f)}}$ (Proposition 9), comparing degrees gives $d_i = n_i$.

(iv) On $G_{\lambda_i}(f)$, by definition $(f - \lambda_i \operatorname{Id})^{n_i}|_{G_{\lambda_i}(f)} = 0$, so the restriction is nilpotent with index at most n_i. □

Theorem 13 (Primary decomposition theorem)

Let $f \in \operatorname{End}(E)$ and suppose χ_f splits over $\mathbb{K}$ as $\chi_f(\lambda) = \prod_{i=1}^{s}(\lambda_i - \lambda)^{n_i}$. Then

$$\boxed{E = G_{\lambda_1}(f) \oplus G_{\lambda_2}(f) \oplus \cdots \oplus G_{\lambda_s}(f),}$$

where $\dim G_{\lambda_i}(f) = n_i$ and each $G_{\lambda_i}(f)$ is f-invariant. Moreover, the restriction $f|_{G_{\lambda_i}(f)}$ has the unique eigenvalue λ_i.

Proof. This was established in the proof of Proposition 12. □

9.4 Jordan blocks and Jordan matrices

Definition 14 (Jordan block)

For $\lambda \in \mathbb{K}$ and $k \geq 1$, the *Jordan block* of size k associated with λ is the $k \times k$ matrix

$$J_k(\lambda) := \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} = \lambda I_k + N_k,$$

where N_k is the $k \times k$ nilpotent matrix with 1's on the superdiagonal and 0's elsewhere.

Remark 15 (Properties of a Jordan block)

Let $J = J_k(\lambda)$.

(i) $\chi_J(\mu) = (\lambda - \mu)^k$.

(ii) The only eigenvalue of J is λ, with algebraic multiplicity k and geometric multiplicity 1.

(iii) $J - \lambda I_k = N_k$ is nilpotent with index k.

(iv) $\mu_J(\mu) = (\lambda - \mu)^k$ (the minimal polynomial equals the characteristic polynomial).

Definition 16 (Jordan matrix)

A *Jordan matrix* is a block-diagonal matrix of the form

$$J = \begin{pmatrix} J_{k_1}(\lambda_1) & & & \\ & J_{k_2}(\lambda_2) & & \\ & & \ddots & \\ & & & J_{k_m}(\lambda_m) \end{pmatrix},$$

where each $J_{k_i}(\lambda_i)$ is a Jordan block. The eigenvalues $\lambda_1, \ldots, \lambda_m$ need not be distinct.

9.5 The Jordan Normal Form theorem

Theorem 17 (Jordan Normal Form)

Let E be a finite-dimensional vector space over an algebraically closed field $\mathbb{K}$ (e.g. $\mathbb{K} = \mathbb{C}$), and let $f \in \mathrm{End}(E)$. Then there exists a basis $\mathcal{B}$ of E in which the matrix of f is a Jordan matrix:

$$\mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} J_{k_1}(\lambda_1) & & & \\ & J_{k_2}(\lambda_2) & & \\ & & \ddots & \\ & & & J_{k_m}(\lambda_m) \end{pmatrix}.$$

Equivalently, every matrix $A \in \mathcal{M}_n(\mathbb{K})$ is similar to a Jordan matrix: $A = PJP^{-1}$ for some invertible P.

Moreover, the Jordan matrix is unique up to permutation of the blocks.

The proof occupies the next section. The overall strategy is:

1. Use the primary decomposition to reduce to the case where f has a single eigenvalue.
2. When f has a single eigenvalue λ, write $f = \lambda \operatorname{Id} + g$ where g is nilpotent.
3. Prove that every nilpotent endomorphism has a Jordan form (a direct sum of nilpotent Jordan blocks $J_k(0) = N_k$).

9.6 Proof of the Jordan Normal Form theorem

We begin with the nilpotent case, which is the heart of the proof.

Lemma 18 (Jordan form for nilpotent endomorphisms)

Let $g \in \operatorname{End}(E)$ be nilpotent with $\dim E = n$. Then there exist positive integers $k_1 \geq k_2 \geq \cdots \geq k_m$ with $k_1 + k_2 + \cdots + k_m = n$ and a basis of E in which the matrix of g is

$$\begin{pmatrix} N_{k_1} & & & \\ & N_{k_2} & & \\ & & \ddots & \\ & & & N_{k_m} \end{pmatrix},$$

where $N_k = J_k(0)$ is the $k \times k$ nilpotent Jordan block. The integers $k_1, \ldots, k_m$ are uniquely determined by g.

Proof. We proceed by strong induction on $n = \dim E$.

Base case. If $n = 1$, then $g = 0$ and the matrix is the 1×1 zero matrix N_1, which is already in Jordan form.

Inductive step. Assume $n \geq 2$ and the result holds for all spaces of dimension $< n$. Let r be the index of nilpotency of g, so $g^r = 0$ and $g^{r-1} \neq 0$.

If $r = 1$, then $g = 0$ and the matrix is the zero matrix, which is a direct sum of n copies of N_1.

Assume $r \geq 2$. Consider the subspace $F = \operatorname{Im}(g)$. Since $g \neq 0$, we have $F \neq \{\mathbf{0}\}$ and $\dim F < n$ (because g is not invertible). Moreover, F is g-invariant: for any $v \in E$, $g(g(v)) = g^2(v) \in \operatorname{Im}(g) = F$.

The restriction $g|_F$ is nilpotent on F, and $\dim F < n$. By the induction hypothesis, there exists a basis of F in which $g|_F$ has the form $\operatorname{diag}(N_{k_1-1}, N_{k_2-1}, \ldots, N_{k_p-1}, N_{k_{p+1}}, \ldots)$ (rearranging and shifting indices as needed).

Concretely, there exist *cyclic chains* for g. Choose a vector $v_1 \in E$ such that $g^{r-1}(v_1) \neq 0$. Then the vectors

$$v_1,\ g(v_1),\ g^2(v_1),\ \ldots,\ g^{r-1}(v_1)$$

are linearly independent (if $\sum_{j=0}^{r-1} \alpha_j g^j(v_1) = 0$, applying g^{r-1-j} for the smallest j with $\alpha_j \neq 0$ gives a contradiction). Write $W_1 = \operatorname{Span}(v_1, g(v_1), \ldots, g^{r-1}(v_1))$. In the basis $(g^{r-1}(v_1), g^{r-2}(v_1), \ldots, g(v_1), v_1)$, the matrix of $g|_{W_1}$ is N_r.

We now construct a complement. Set $d_j = \dim \operatorname{Ker}(g^j)$ for $0 \leq j \leq r$. Define $m_j = 2d_j - d_{j-1} - d_{j+1}$ for $1 \leq j \leq r-1$ and $m_r = 2d_r - d_{r-1} - d_r = d_r - d_{r-1}$. We claim that m_j equals the number of Jordan blocks of size j.

More precisely, we construct the full Jordan basis as follows. For each j from r down to 1, choose vectors v such that $g^{j-1}(v) \neq 0$ but $g^j(v) = 0$, and such that $v, g(v), \ldots, g^{j-1}(v)$ are

linearly independent of the vectors already chosen. The number of such chains of length j is $m_j = d_j - d_{j-1} -$ (number of chain elements of length $> j$ lying in $\operatorname{Ker}(g^j) \setminus \operatorname{Ker}(g^{j-1})$).

To be fully explicit, define $\ell_j = d_j - d_{j-1}$ (with $d_0 = 0$). One can show that $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_r \geq 1$ and that ℓ_j equals the number of Jordan blocks of size $\geq j$. Hence the number of blocks of size exactly j is $\ell_j - \ell_{j+1}$ (where $\ell_{r+1} = 0$).

We verify this by induction. The subspace W_1 Spanned by the first chain has the property that $g|_{W_1}$ corresponds to N_r, and $E = W_1 \oplus W_1'$ where W_1' is a g-stable complement. Such a complement exists: choose a complement C of $\operatorname{Ker}(g^{r-1})$ inside $\operatorname{Ker}(g^r) = E$, so $\dim C = \ell_r$. For each basis vector c of C, the chain $c, g(c), \ldots, g^{r-1}(c)$ Spans a cyclic subspace isomorphic to N_r. We can choose these chains so that their union is linearly independent. After removing these chains, the remaining space (a suitable complement) has a nilpotent restriction of strictly smaller dimension, and the induction hypothesis applies.

This procedure produces a basis of E consisting of cyclic chains, and in this basis the matrix of g is block-diagonal with nilpotent Jordan blocks.

Uniqueness. The sizes of the Jordan blocks are determined by the sequence $d_j = \dim \operatorname{Ker}(g^j)$: the number of blocks of size $\geq j$ is $d_j - d_{j-1}$, and the number of blocks of size exactly j is $(d_j - d_{j-1}) - (d_{j+1} - d_j)$. Since the dimensions d_j are invariants of g, the block sizes are uniquely determined. □

Proof of Theorem 17. **Existence.** By the primary decomposition theorem (Theorem 13),

$$E = G_{\lambda_1}(f) \oplus G_{\lambda_2}(f) \oplus \cdots \oplus G_{\lambda_s}(f),$$

where $\lambda_1, \ldots, \lambda_s$ are the distinct eigenvalues of f and $\dim G_{\lambda_i}(f) = n_i = m_a(\lambda_i)$.

On each $G_{\lambda_i}(f)$, define $g_i = (f - \lambda_i \operatorname{Id})|_{G_{\lambda_i}(f)}$, which is nilpotent. By Lemma 18, there is a basis of $G_{\lambda_i}(f)$ in which g_i has the form $\operatorname{diag}(N_{k_1^{(i)}}, \ldots, N_{k_{m_i}^{(i)}})$.

Since $f|_{G_{\lambda_i}(f)} = \lambda_i \operatorname{Id} + g_i$, the matrix of $f|_{G_{\lambda_i}(f)}$ in this basis is

$$\operatorname{diag}(J_{k_1^{(i)}}(\lambda_i), \ldots, J_{k_{m_i}^{(i)}}(\lambda_i)).$$

Concatenating the bases of all generalized eigenspaces gives a basis of E in which f has a Jordan matrix.

Uniqueness. On each generalized eigenspace $G_{\lambda_i}(f)$, the Jordan block sizes are determined by the dimensions $\dim \operatorname{Ker}((f - \lambda_i \operatorname{Id})^k)$ by Lemma 18. Since the eigenvalues, their algebraic multiplicities, and the kernel dimensions are similarity invariants, the Jordan form is unique up to the ordering of blocks. □

9.7 Computing the Jordan form

Given a matrix $A \in \mathcal{M}_n(\mathbb{K})$, the following algorithm computes its Jordan normal form.

Step 1: Find the eigenvalues. Compute $\chi_A(\lambda) = \det(A - \lambda I)$ and factor it: $\chi_A(\lambda) = \prod_{i=1}^{s} (\lambda_i - \lambda)^{n_i}$.

Step 2: For each eigenvalue λ_i, compute the kernel dimensions. Compute $d_k^{(i)} = \dim \operatorname{Ker}((A - \lambda_i I)^k)$ for $k = 1, 2, 3, \ldots$ until $d_k^{(i)} = n_i$ (which must happen for some $k \leq n_i$).

Step 3: Determine the Jordan block sizes. For each eigenvalue λ_i:

- The number of Jordan blocks for λ_i is $d_1^{(i)} = \dim \operatorname{Ker}(A - \lambda_i I)$ (the geometric multiplicity).

- The number of blocks of size $\geq k$ is $d_k^{(i)} - d_{k-1}^{(i)}$.
- The number of blocks of size exactly k is $(d_k^{(i)} - d_{k-1}^{(i)}) - (d_{k+1}^{(i)} - d_k^{(i)}) = 2d_k^{(i)} - d_{k-1}^{(i)} - d_{k+1}^{(i)}$.

Step 4: Assemble the Jordan matrix. Write $J = \operatorname{diag}(J_{k_1}(\lambda_1), J_{k_2}(\lambda_2), \ldots)$.

Remark 19 (Finding the transition matrix)

To find the invertible matrix P such that $A = PJP^{-1}$, one must compute a *Jordan basis*: for each Jordan block of size k associated with eigenvalue λ, find a chain of generalized eigenvectors $v_1, v_2, \ldots, v_k$ satisfying

$$(A - \lambda I)v_1 = 0, \quad (A - \lambda I)v_2 = v_1, \quad \ldots, \quad (A - \lambda I)v_k = v_{k-1}.$$

The columns of P are then these generalized eigenvectors $(v_k, v_{k-1}, \ldots, v_1)$ (note the reversed order: v_k comes first so that $AP = PJ$).

9.8 Worked examples

Example 20 (Jordan form of a 3×3 matrix)

Let

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

Step 1. $\chi_A(\lambda) = (2 - \lambda)^3$, so $\lambda = 2$ is the only eigenvalue with $n_1 = 3$.
Step 2. Compute the kernel dimensions.

$$A - 2I = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad (A - 2I)^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad (A - 2I)^3 = 0.$$

So $d_1 = \dim \operatorname{Ker}(A - 2I) = 1$, $d_2 = \dim \operatorname{Ker}(A - 2I)^2 = 2$, $d_3 = 3$.
Step 3. Number of blocks of size ≥ 1: $d_1 - d_0 = 1$. Number of blocks of size ≥ 2: $d_2 - d_1 = 1$. Number of blocks of size ≥ 3: $d_3 - d_2 = 1$. So there is exactly one block of size 3.
Step 4. The Jordan form is

$$J = J_3(2) = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Indeed, A is already in Jordan form.

Example 21 (Jordan form of a 4×4 matrix)

Let

$$A = \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 5 \end{pmatrix}.$$

Step 1. $\chi_A(\lambda) = (3-\lambda)^3(5-\lambda)$. Eigenvalues: $\lambda_1 = 3$ with $n_1 = 3$, and $\lambda_2 = 5$ with $n_2 = 1$.
Step 2. For $\lambda_1 = 3$:

$$A - 3I = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \quad (A-3I)^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

$d_1 = \dim \operatorname{Ker}(A-3I) = 2$ (the kernel is Spanned by e_1 and e_3), $d_2 = \dim \operatorname{Ker}(A-3I)^2 = 2$. Wait—we need $d_k = \dim \operatorname{Ker}(A-3I)^k$ restricted to the generalized eigenspace, or equivalently the rank of $(A-3I)^k$. Since $d_2 = 2$ and we need $d_k = 3 = n_1$, let us recompute. Actually, $\operatorname{rank}(A-3I) = 2$ (two independent rows), so $d_1 = 4-2 = 2$. For $(A-3I)^2$: rank $= 1$, so $d_2 = 4-1 = 3$.
Number of blocks for $\lambda_1 = 3$: $d_1 = 2$ blocks total. Blocks of size ≥ 2: $d_2 - d_1 = 1$. Blocks of size ≥ 3: $d_3 - d_2 = 0$ (since $d_3 = 3 = d_2$ for the generalized eigenspace dimension). So: one block of size 2 (from 1 of size ≥ 2, minus 0 of size ≥ 3), and one block of size 1 (from 2 total, minus 1 of size ≥ 2).
For $\lambda_2 = 5$: one block of size 1 (the algebraic multiplicity is 1).
Step 3. The Jordan form is

$$J = \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix} = \operatorname{diag}(J_2(3),\ J_1(3),\ J_1(5)).$$

Jordan basis. For the block $J_2(3)$: we need $v_1 \in \operatorname{Ker}(A-3I)$ and v_2 with $(A-3I)v_2 = v_1$. Take $v_1 = e_1$, then $(A-3I)v_2 = e_1$ gives $v_2 = e_2$ (since $(A-3I)e_2 = e_1$). For $J_1(3)$: take $v_3 = e_3 \in \operatorname{Ker}(A-3I)$. For $J_1(5)$: solve $(A-5I)v_4 = 0$; we find $v_4 = \begin{pmatrix} -1 \\ 0 \\ -1 \\ 2 \end{pmatrix}$ (after row reduction).
The transition matrix is $P = (v_2 \mid v_1 \mid v_3 \mid v_4)$:

$$P = \begin{pmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \qquad A = P\,J\,P^{-1}.$$

One may verify that $AP = PJ$.

Example 22 (A non-trivial 4×4 Jordan form)

Consider

$$A = \begin{pmatrix} 5 & 4 & 2 & 1 \\ 0 & 1 & -1 & -1 \\ -1 & -1 & 3 & 0 \\ 1 & 1 & -1 & 2 \end{pmatrix}.$$

One computes $\chi_A(\lambda) = (\lambda-1)^2(\lambda-3)^2$.
For $\lambda_1 = 1$: $\operatorname{rank}(A-I) = 2$, so $d_1 = 4-2 = 2 = n_1$. Since $d_1 = n_1$, the generalized eigenspace equals the eigenspace. Thus there are two blocks of size 1: $J_1(1) \oplus J_1(1)$.
For $\lambda_2 = 3$: $\operatorname{rank}(A-3I) = 3$, so $d_1 = 4-3 = 1$. Since $d_1 = 1 < 2 = n_2$, we need to go

further: $\operatorname{rank}(A-3I)^2 = 2$, so $d_2 = 4-2 = 2 = n_2$. Number of blocks: $d_1 = 1$. Size ≥ 2: $d_2 - d_1 = 1$. So there is one block of size 2: $J_2(3)$.
The Jordan form is:

$$J = \operatorname{diag}(J_1(1),\ J_1(1),\ J_2(3)) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

9.9 Jordan form and the minimal polynomial

The Jordan form makes the relationship between a matrix and its minimal polynomial completely transparent.

Theorem 23 (Minimal polynomial from the Jordan form)

Let $A \in \mathcal{M}_n(\mathbb{K})$ with Jordan form $J = \operatorname{diag}(J_{k_1}(\lambda_1), \dots, J_{k_m}(\lambda_m))$, where $\lambda_1, \dots, \lambda_s$ are the distinct eigenvalues. For each distinct eigenvalue λ_i, let r_i denote the *largest* Jordan block size associated with λ_i. Then the minimal polynomial of A is

$$\boxed{\mu_A(\lambda) = \prod_{i=1}^{s} (\lambda - \lambda_i)^{r_i}.}$$

Proof. A polynomial $P(\lambda)$ satisfies $P(A) = 0$ if and only if $P(J) = 0$ (since A and J are similar). Moreover, $P(J) = \operatorname{diag}(P(J_{k_1}(\lambda_1)), \dots, P(J_{k_m}(\lambda_m)))$, so $P(J) = 0$ if and only if $P(J_{k_j}(\lambda_j)) = 0$ for every block.

For a single Jordan block $J_k(\lambda)$, one computes

$$P(J_k(\lambda)) = \begin{pmatrix} P(\lambda) & P'(\lambda) & \frac{P''(\lambda)}{2!} & \cdots & \frac{P^{(k-1)}(\lambda)}{(k-1)!} \\ & P(\lambda) & P'(\lambda) & \cdots & \frac{P^{(k-2)}(\lambda)}{(k-2)!} \\ & & \ddots & \ddots & \vdots \\ & & & P(\lambda) & P'(\lambda) \\ & & & & P(\lambda) \end{pmatrix}.$$

Hence $P(J_k(\lambda)) = 0$ if and only if $P(\lambda) = P'(\lambda) = \cdots = P^{(k-1)}(\lambda) = 0$, which holds if and only if $(\lambda_0 - \lambda)^k \mid P(\lambda)$ where $\lambda_0 = \lambda$ is the eigenvalue.

Therefore, $P(J) = 0$ if and only if $(\lambda_i - x)^{r_i}$ divides $P(x)$ for every distinct eigenvalue λ_i, where r_i is the largest block for λ_i. The monic polynomial of smallest degree with this property is $\mu_A(\lambda) = \prod_{i=1}^{s} (\lambda - \lambda_i)^{r_i}$. □

Corollary 24 (Diagonalizability via the Jordan form)

A matrix is diagonalizable if and only if its Jordan form is diagonal, which happens if and only if all Jordan blocks have size 1. Equivalently, the minimal polynomial has no repeated roots.

Proof. All blocks have size 1 if and only if $r_i = 1$ for each eigenvalue, if and only if μ_A has only simple roots, if and only if A is diagonalizable. □

9.10 Cayley–Hamilton revisited

The Jordan form gives an elegant proof of the Cayley–Hamilton theorem.

Theorem 25 (Cayley–Hamilton theorem)

Let $A \in \mathcal{M}_n(\mathbb{K})$ with $\mathbb{K}$ algebraically closed. Then $\chi_A(A) = 0$.

Proof. Let $J = P^{-1}AP$ be the Jordan form. Then $\chi_A(A) = P\,\chi_A(J)\,P^{-1} = P\,\chi_J(J)\,P^{-1}$ (since $\chi_A = \chi_J$).

Write $J = \operatorname{diag}(J_{k_1}(\lambda_1), \dots, J_{k_m}(\lambda_m))$. Then $\chi_J(\lambda) = \prod_{j=1}^{m} (\lambda_j - \lambda)^{k_j}$, so

$$\chi_J(J) = \operatorname{diag}(\chi_J(J_{k_1}(\lambda_1)), \dots, \chi_J(J_{k_m}(\lambda_m))).$$

For each block $J_{k_j}(\lambda_j)$, the factor $(\lambda_j - \lambda)^{k_j}$ divides $\chi_J(\lambda)$, hence $\chi_J(J_{k_j}(\lambda_j)) = 0$ by the analysis in Theorem 23.

Therefore $\chi_J(J) = 0$, and so $\chi_A(A) = 0$. $\square$

9.11 Matrix exponential

One of the most important applications of the Jordan form is the computation of the *matrix exponential*, which plays a central role in the theory of linear differential equations.

Definition 26 (Matrix exponential)

For $A \in \mathcal{M}_n(\mathbb{C})$, the *matrix exponential* of A is defined by the power series

$$e^A := \exp(A) := \sum_{k=0}^{\infty} \frac{A^k}{k!} = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots.$$

This series converges absolutely for every $A \in \mathcal{M}_n(\mathbb{C})$.

Proposition 27 (Properties of the matrix exponential)

(i) $e^0 = I_n$.

(ii) If $AB = BA$, then $e^{A+B} = e^A e^B$.

(iii) e^A is always invertible, with $(e^A)^{-1} = e^{-A}$.

(iv) $e^{PAP^{-1}} = P\,e^A\,P^{-1}$ for any invertible P.

(v) $\det(e^A) = e^{\operatorname{tr}(A)}$.

Proof. (i) is clear. (ii) follows by expanding the product of power series, using $AB = BA$ to collect terms as in the scalar case. (iii) follows from (ii) with $B = -A$. (iv) follows from $(PAP^{-1})^k = PA^kP^{-1}$.

For (v), if $A = PJP^{-1}$ is in Jordan form, then $e^A = Pe^JP^{-1}$ and $\det(e^A) = \det(e^J)$. For a Jordan block $J_k(\lambda)$, the matrix $e^{J_k(\lambda)}$ is upper triangular with e^λ on the diagonal, so $\det(e^{J_k(\lambda)}) = e^{k\lambda}$. Thus $\det(e^J) = \prod_j e^{k_j\lambda_j} = e^{\sum_j k_j\lambda_j} = e^{\operatorname{tr}(J)} = e^{\operatorname{tr}(A)}$. $\square$

Proposition 28 (Exponential of a Jordan block)

For a Jordan block $J_k(\lambda) = \lambda I_k + N_k$, since λI_k and N_k commute:

$$e^{J_k(\lambda)} = e^{\lambda I_k}\, e^{N_k} = e^{\lambda}\, e^{N_k}.$$

Moreover, since $N_k^k = 0$:

$$e^{N_k} = I_k + N_k + \frac{N_k^2}{2!} + \cdots + \frac{N_k^{k-1}}{(k-1)!}.$$

Explicitly:

$$e^{J_k(\lambda)} = e^{\lambda} \begin{pmatrix} 1 & 1 & \frac{1}{2!} & \cdots & \frac{1}{(k-1)!} \\ 0 & 1 & 1 & \cdots & \frac{1}{(k-2)!} \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & & 1 & 1 \\ 0 & \cdots & & 0 & 1 \end{pmatrix}.$$

More generally, for the *matrix exponential of* tA (with $t \in \mathbb{R}$):

$$e^{tJ_k(\lambda)} = e^{\lambda t} \begin{pmatrix} 1 & t & \frac{t^2}{2!} & \cdots & \frac{t^{k-1}}{(k-1)!} \\ 0 & 1 & t & \cdots & \frac{t^{k-2}}{(k-2)!} \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & & 1 & t \\ 0 & \cdots & & 0 & 1 \end{pmatrix}.$$

Proof. Since λI_k and N_k commute, $e^{J_k(\lambda)} = e^{\lambda I_k + N_k} = e^{\lambda I_k} e^{N_k} = e^{\lambda} I_k \cdot e^{N_k}$. The entries of e^{N_k} follow from $(N_k^j)_{pq} = \delta_{p+j,q}$ (the matrix with 1's on the j-th superdiagonal), giving $(e^{N_k})_{pq} = \frac{1}{(q-p)!}$ for $q \geq p$ and 0 otherwise. The formula for $e^{tJ_k(\lambda)}$ is analogous, replacing N_k by tN_k. □

Example 29 (Computing e^{tA})

Let $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} = J_2(2)$. Then

$$e^{tA} = e^{2t} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} e^{2t} & te^{2t} \\ 0 & e^{2t} \end{pmatrix}.$$

9.12 Applications

9.12.1 Systems of linear ODEs

Consider the linear system of ordinary differential equations

$$\mathbf{x}'(t) = A\,\mathbf{x}(t), \qquad \mathbf{x}(0) = \mathbf{x}_0, \tag{9.1}$$

where $A \in \mathcal{M}_n(\mathbb{R})$ (or $\mathcal{M}_n(\mathbb{C})$) and $\mathbf{x}(t) \in \mathbb{R}^n$ (or $\mathbb{C}^n$).

The solution is $\mathbf{x}(t) = e^{tA}\mathbf{x}_0$. When A is diagonalizable, $A = P\,\mathrm{diag}(\lambda_1, \ldots, \lambda_n)P^{-1}$ and the solution is a superposition of pure exponentials $e^{\lambda_i t}$. When A is *not* diagonalizable, the Jordan form tells us exactly what happens.

Proposition 30 (Solution structure via Jordan form)

If $A = PJP^{-1}$ with Jordan form J, then $e^{tA} = P\,e^{tJ}\,P^{-1}$ and $\mathbf{x}(t) = P\,e^{tJ}\,P^{-1}\mathbf{x}_0$. For a Jordan block $J_k(\lambda)$, the corresponding components of the solution involve terms of the form

$$t^j e^{\lambda t}, \qquad 0 \le j \le k-1.$$

In particular, non-trivial Jordan blocks (size > 1) produce *polynomial-exponential* solutions (polynomial times exponential), not pure exponentials.

Example 31 (A 3×3 system of ODEs)

Consider $\mathbf{x}'(t) = A\mathbf{x}(t)$ with

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = J_3(1).$$

Then

$$e^{tA} = e^t \begin{pmatrix} 1 & t & \frac{t^2}{2} \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}.$$

With initial condition $\mathbf{x}_0 = \left(\begin{smallmatrix} 1 \\ 0 \\ 1 \end{smallmatrix}\right)$:

$$\mathbf{x}(t) = e^t \begin{pmatrix} 1 + \frac{t^2}{2} \\ t \\ 1 \end{pmatrix}.$$

Note the appearance of the polynomial factor $1 + t^2/2$ in the first component, which is characteristic of a 3×3 Jordan block.

9.12.2 Matrix functions via Jordan form

The Jordan form allows us to define and compute general matrix functions. If $h\colon \mathbb{C} \to \mathbb{C}$ is a function that is sufficiently smooth (or analytic) in a neighbourhood of each eigenvalue, we can define $h(A)$ as follows.

Definition 32 (Matrix function via Jordan form)

Let $A \in \mathcal{M}_n(\mathbb{C})$ with $A = PJP^{-1}$ and $J = \operatorname{diag}(J_{k_1}(\lambda_1), \dots, J_{k_m}(\lambda_m))$. Define

$$h(A) := P\,\operatorname{diag}(h(J_{k_1}(\lambda_1)), \dots, h(J_{k_m}(\lambda_m)))\,P^{-1},$$

where

$$h(J_k(\lambda)) := \begin{pmatrix} h(\lambda) & h'(\lambda) & \frac{h''(\lambda)}{2!} & \cdots & \frac{h^{(k-1)}(\lambda)}{(k-1)!} \\ & h(\lambda) & h'(\lambda) & \cdots & \frac{h^{(k-2)}(\lambda)}{(k-2)!} \\ & & \ddots & \ddots & \vdots \\ & & & h(\lambda) & h'(\lambda) \\ & & & & h(\lambda) \end{pmatrix}.$$

Example 33 (Computing A^k and $\sqrt{A}$)

For $A = \left(\begin{smallmatrix} 4 & 1 \\ 0 & 4 \end{smallmatrix}\right) = J_2(4)$ and $h(\lambda) = \lambda^k$:

$$A^k = \begin{pmatrix} 4^k & k \cdot 4^{k-1} \\ 0 & 4^k \end{pmatrix}.$$

For $h(\lambda) = \sqrt{\lambda}$ (choosing the principal square root):

$$\sqrt{A} = \begin{pmatrix} 2 & \frac{1}{4} \\ 0 & 2 \end{pmatrix},$$

since $h(4) = 2$ and $h'(4) = \frac{1}{2\sqrt{4}} = \frac{1}{4}$.

9.13 Exercises

Exercise 34 (Nilpotent matrices)

Determine whether each matrix is nilpotent. If so, find the index of nilpotency.

(a) $A = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & -3 \\ 0 & 0 & 0 \end{pmatrix}$

(b) $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

(c) $C = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

Exercise 35 (Properties of nilpotent endomorphisms)

Let $f \in \mathrm{End}(E)$ be nilpotent. Show that:

(a) $\mathrm{Id} + f$ is invertible. *Hint:* consider $(\mathrm{Id} + f)(\mathrm{Id} - f + f^2 - \cdots)$.

(b) If $g \in \mathrm{End}(E)$ is nilpotent and $fg = gf$, then $f + g$ is nilpotent.

Exercise 36 (Jordan form of 2×2 matrices)

Find the Jordan normal form of each matrix over $\mathbb{C}$:

(a) $A = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}$

(b) $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

(c) $C = \begin{pmatrix} 5 & 3 \\ -3 & -1 \end{pmatrix}$

Exercise 37 (Jordan form of a 3×3 matrix)

Find the Jordan normal form and a Jordan basis for

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Exercise 38 (A 4×4 matrix with repeated eigenvalues)

Find the Jordan normal form of

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

How many distinct Jordan forms are possible for a 4×4 matrix whose only eigenvalue is 2? List them all.

Exercise 39 (Uniqueness via kernel dimensions)

Let $A, B \in \mathcal{M}_n(\mathbb{C})$ be two matrices with the same characteristic polynomial. Show that A and B are similar if and only if $\operatorname{rank}(A - \lambda I)^k = \operatorname{rank}(B - \lambda I)^k$ for every eigenvalue λ and every $k \geq 1$.

Exercise 40 (Minimal polynomial from Jordan form)

For each of the following Jordan matrices, determine the minimal polynomial:

(a) $J = \operatorname{diag}(J_3(2), J_1(2))$

(b) $J = \operatorname{diag}(J_2(1), J_2(3))$

(c) $J = \operatorname{diag}(J_2(0), J_2(0), J_1(0))$

Exercise 41 (Matrix exponential)

Compute e^{tA} for:

(a) $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

(b) $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

(c) $A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix}$

Exercise 42 (Solving a non-diagonalizable ODE system)

Solve the initial value problem

$$\mathbf{x}'(t) = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix} \mathbf{x}(t), \qquad \mathbf{x}(0) = \begin{pmatrix} 1 \\ 2 \end{pmatrix}.$$

Exercise 43 (Cayley–Hamilton via Jordan form)

Let $A \in \mathcal{M}_n(\mathbb{C})$ with Jordan form J.

(a) Compute $\chi_A(J_k(\lambda))$ directly, showing each entry is zero.

(b) Deduce the Cayley–Hamilton theorem for matrices over $\mathbb{C}$.

(c) Explain why the result extends to matrices over any field $\mathbb{K}$. *Hint:* use the fact that $\chi_A(A) = 0$ is a polynomial identity in the entries of A.

Exercise 44 (Powers of nilpotent-plus-scalar matrices)

Let $A = \lambda I + N$ where N is nilpotent with index r.

(a) Show that for all $m \geq 0$,

$$A^m = \sum_{j=0}^{r-1} \binom{m}{j} \lambda^{m-j} N^j.$$

(b) Deduce the entries of $J_k(\lambda)^m$ explicitly.

(c) Use part (a) to give another proof that if A is nilpotent and $\operatorname{tr}(A^k) = 0$ for all $k \geq 1$, then A is nilpotent.

Exercise 45 (Jordan form and commuting matrices)

Let $A \in \mathcal{M}_n(\mathbb{C})$.

(a) Show that B commutes with $J_k(\lambda)$ if and only if B is an upper triangular Toeplitz matrix (i.e. B_{ij} depends only on $j - i$).

(b) Deduce that if A has n distinct eigenvalues, then every matrix commuting with A is a polynomial in A.

(c) Give an example showing this fails when A has repeated eigenvalues with multiple Jordan blocks.

Exercise 46 (Logarithm of a matrix)

Let $A \in \mathcal{M}_n(\mathbb{C})$ be invertible (so all eigenvalues are nonzero).

(a) For a Jordan block $J_k(\lambda)$ with $\lambda \neq 0$, show that $J_k(\lambda) = \lambda(I + \lambda^{-1} N_k)$ and use the power series $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$ (which terminates since N_k is nilpotent) to define $\log J_k(\lambda)$.

(b) Compute $\log J_k(\lambda)$ explicitly for $k = 2$ and $k = 3$.

(c) Verify that $e^{\log J_k(\lambda)} = J_k(\lambda)$.

Exercise 47 (Jordan form over $\mathbb{R}$)

The matrix $A = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ has characteristic polynomial $\chi_A(\lambda) = (\lambda^2+1)^2$.

(a) Find the Jordan form of A over $\mathbb{C}$.

(b) Show that A is not similar over $\mathbb{R}$ to a Jordan matrix.

(c) Find the *real Jordan form* of A, i.e. a block matrix with 2×2 "rotation-scaling" blocks $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ replacing complex eigenvalues $a \pm bi$.

9.14 Chapter summary

- **Nilpotent endomorphisms.** An endomorphism f is nilpotent if $f^r = 0$ for some $r \geq 1$. Its only eigenvalue is 0, $\chi_f(\lambda) = (-\lambda)^n$, and the index of nilpotency satisfies $r \leq n$.
- **Generalized eigenspaces.** For each eigenvalue λ of f, the generalized eigenspace $G_\lambda(f) = \operatorname{Ker}((f - \lambda \operatorname{Id})^{n_\lambda})$ has dimension equal to the algebraic multiplicity n_λ. The primary decomposition theorem gives $E = \bigoplus_{\lambda \in \operatorname{Spec}(f)} G_\lambda(f)$.
- **Jordan blocks.** $J_k(\lambda) = \lambda I_k + N_k$ is the basic building block. It has eigenvalue λ with algebraic multiplicity k and geometric multiplicity 1.
- **Jordan Normal Form.** Over an algebraically closed field, every endomorphism has a unique (up to block ordering) Jordan form. The block sizes are determined by the dimensions $\dim \operatorname{Ker}(f - \lambda \operatorname{Id})^k$.
- **Minimal polynomial.** $\mu_f(\lambda) = \prod_i (\lambda - \lambda_i)^{r_i}$, where r_i is the size of the *largest* Jordan block for eigenvalue λ_i. A matrix is diagonalizable iff μ_f has only simple roots.
- **Matrix exponential.** $e^{tJ_k(\lambda)} = e^{\lambda t} \cdot$ (upper triangular polynomial matrix in t). This gives the explicit solution $\mathbf{x}(t) = e^{tA}\mathbf{x}_0$ to $\mathbf{x}' = A\mathbf{x}$, even when A is not diagonalizable. Non-trivial Jordan blocks produce solutions of the form $t^j e^{\lambda t}$ (polynomial times exponential).
- **Matrix functions.** Any sufficiently smooth function h can be extended to matrices via the Jordan form: $h(J_k(\lambda))$ involves $h(\lambda), h'(\lambda), \ldots, h^{(k-1)}(\lambda)$.

Index