Caltech Division of the Humanities and Social Sciences

Quick Review of Matrix and Real Linear Algebra

KC Border

Subject to constant revision
Last major revision: April 1, 2020
v. 2020.03.29::12.55

Contents

Foreword

These notes have accreted piecemeal from courses in econometrics, statistics, and microeconomics I have taught over the last forty-something years, so the notation, hyphenation, and terminology may vary from section to section. I originally compiled them to be my personal centralized reference for finite-dimensional real vector spaces, but over the years I have added more expository material. While the notes concentrate on finite-dimensional real vector spaces, I occasionally mention complex or infinite-dimensional spaces. If you too find them useful, so much the better. There is a sketchy index, which I think is better than none.

For a thorough course on linear algebra I now recommend Axler [7]. My favorite reference for infinite-dimensional vector spaces is the *Hitchhiker's Guide* [2], but it needn't be your favorite.

1 Scalar fields

A **field** is a set of mathematical entities that we shall call **scalars**. There are two binary operations defined on scalars, **addition** and **multiplication**. We denote the **sum** of α and β by $\alpha + \beta$, and the **product** simply by $\alpha\beta$, or by occasionally $\alpha \cdot \beta$. These operations satisfy the following familiar properties:

F.1 (Commutativity of Addition and Multiplication) $\alpha + \beta = \beta + \alpha$, $\alpha\beta = \beta\alpha$.

F.2 (Associativity of Addition and Multiplication) $(\alpha\beta) + \gamma = \alpha + (\beta + \gamma)$, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

F.3 (Distributive Law) $\alpha(\beta + \gamma) = (\alpha\beta) + (\alpha\gamma)$.

F.4 (Existence of Additive and Multiplicative Identities) There are two distinct scalars, zero, 0, and 1, such that for every scalar α, we have $\alpha + 0 = \alpha$ and $1\alpha = \alpha$.

F.5 (Existence of Additive Inverse) For each scalar α there exists a scalar $-\alpha$ such that $\alpha + (-\alpha) = 0$. We usually write $\alpha - \beta$ for $\alpha + (-\beta)$.

F.5 (Existence of Multiplicative Inverse) For each *nonzero* scalar α there exists a scalar α^{-1} such that $\alpha\alpha^{-1} = 1$. We often write α/β for $\alpha\beta^{-1}$.

There are many elementary theorems that point out many things that you probably take for granted. For instance,

- $-\alpha$ and α^{-1} are unique. This justifies the notation, by the way.
- $-\alpha = (-1) \cdot \alpha$. (Here -1 is the scalar β that satisfies $1 + \beta = 0$.)
- $\alpha + \gamma = \beta + \gamma \iff \alpha = \beta$.
- $0 \cdot \alpha = 0$.
- $\alpha\beta = 0 \implies [\alpha = 0 \text{ or } \beta = 0 \text{ or both }]$.

There are many more. See, for instance, Apostol [5, p. 18].

The most important scalar fields are the **real numbers** $\boldsymbol{R}$, the **rational numbers** $\mathbb{Q}$, and the field of **complex numbers** $\mathbb{C}$. Computer scientists, e.g., Klein [15], are fond of the $\{0, 1\}$ field sometimes known as GF(2) or the **Boolean field**.

These notes are mostly concerned with the field of real numbers. This is not because the other fields are unimportant—it's because I myself have limited use for the others, which is probably a personal shortcoming.

2 Vector spaces

Let K be a field of **scalars**—usually either the real numbers $\boldsymbol{R}$ or the complex numbers $\mathbb{C}$, or occasionally the rationals $\mathbb{Q}$.

1 Definition *A* ***vector space*** *over K is a nonempty set V of* ***vectors*** *equipped with two operations, vector addition $(\boldsymbol{x}, \boldsymbol{y}) \mapsto \boldsymbol{x} + \boldsymbol{y}$, and scalar multiplication $(\alpha, \boldsymbol{x}) \mapsto \alpha\boldsymbol{x}$, where $\boldsymbol{x}, \boldsymbol{y} \in V$ and $\alpha \in K$. The operations satisfy:*

V.1 (Commutativity of Vector Addition) $\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x}$

V.2 (Associativity of Vector Addition) $(\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z} = \boldsymbol{x} + (\boldsymbol{y} + \boldsymbol{z})$

V.3 (Existence of Zero Vector) There is a vector $\mathbf{0}_V$, often denoted simply $\mathbf{0}$, satisfying $\boldsymbol{x} + \mathbf{0} = \boldsymbol{x}$ for every vector $\boldsymbol{x}$.

V.4 (Additive Inverse) $\boldsymbol{x} + (-1)\boldsymbol{x} = \mathbf{0}$

V.5 (Associativity of Scalar Multiplication) $\alpha(\beta\boldsymbol{x}) = (\alpha\beta)\boldsymbol{x}$

V.6 (Scalar Multiplication by 1) $1\boldsymbol{x} = \boldsymbol{x}$

V.7 (Distributive Law) $\alpha(\boldsymbol{x} + \boldsymbol{y}) = (\alpha\boldsymbol{x}) + (\alpha\boldsymbol{y})$

V.8 (Distributive Law) $(\alpha + \beta)\boldsymbol{x} = (\alpha\boldsymbol{x}) + (\beta\boldsymbol{x})$

The term **real vector space** refers to a vector space over the field of real numbers, and a **complex vector space** is a vector space over the field of complex numbers. The term **linear space** is a synonym for vector space.

2.1 The vector space $\boldsymbol{R}^{\mathrm{m}}$

By far the most important example of a vector space, and indeed the mother of all vector spaces, is the space $\boldsymbol{R}^{\mathrm{m}}$ of ordered lists of m real numbers. Given ordered lists $\boldsymbol{x} = (\xi_1, \dots, \xi_m)$ and $\boldsymbol{y} = (\eta_1, \dots, \eta_m)$ the vector sum $\boldsymbol{x} + \boldsymbol{y}$ is the ordered list $(\xi_1 + \eta_1, \dots, \xi_m + \eta_m)$. The scalar product is given by the ordered list $\alpha\boldsymbol{x} = (\alpha\xi_1, \dots, \alpha\xi_m)$. The zero of this vector space is the ordered list $\mathbf{0} = (0, \dots, 0)$. It is a trivial matter to verify that the axioms above are satisfied by these operations. As a special case, the set of real numbers $\boldsymbol{R}$ is a real vector space.

In $\boldsymbol{R}^{\mathrm{m}}$ we identify several special vectors, the **unit coordinate vectors**. These are the ordered lists $\boldsymbol{e}_i$ that consist of zeroes except for a single 1 in the i^{th} position. We use the notation $\boldsymbol{e}_i$ to denote this vector regardless of the dimension of the list.

2.2 Other examples of vector spaces

The following are also vector spaces. The definition of the vector operations is usually obvious.

- $\{\mathbf{0}\}$ is a vector space, called the **trivial** vector space. A nontrivial vector space contains at least one nonzero vector.
- The field K is a vector space over itself.
- The set $L_1(I)$ of integrable real-valued functions on an interval I of the real line,

$$\{f \colon I \to \boldsymbol{R} :\in t_I \, |f(x)| \; dx < \infty\}$$

  is a real vector space under the **pointwise operations**: $(f + g)(x) = f(x) + g(x)$ and $(\alpha f)(x) = \alpha f(x)$ for all $x \in I$.

Attempted notational conventions

As of the Great Social Distancing, in order to make these notes more compatible with other course notes, I have edited them to try to adhere to the following notational conventions. My guess is that it will take several iterations before they are really consistent.

Scalars will traditionally be denoted by lower case Greek letters. But there are certain notations, such as integrals, where $\in t_0^1 f(x)\,dx$ seems much more readable than $\in t_0^1 f(\xi)\,d\xi$.

Vectors are typically denoted by bold lower case Latin letters, such as $\boldsymbol{x}$. When I need to refer to a coordinate of $\boldsymbol{x}$ I may simply write x_i. Note the awkward difference between a vector of coordinates $\boldsymbol{x} = (x_1, \dots, x_m)$ and a finite sequence $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$ of vectors. I hope this is not too confusing. When I frequently need to refer to the coordinates of a vector in $\boldsymbol{R}^{\mathrm{m}}$, I will try to make them explicit, and use Greek letters corresponding to the Latin letter of the vector. For instance, $\boldsymbol{x} = (\xi_1, \dots, \xi_m)$, $\boldsymbol{y} = (\eta_1, \dots, \eta_m)$, $\boldsymbol{z} = (\zeta_1, \dots, \zeta_m)$.[a] But it is awkward to be consistent when referring to the coordinate vectors with respect to different bases.

Since many of my econometrics and statistics texts use bold upper case Latin letters to denote matrices, I will try to do likewise. Their entries will be denoted by the corresponding lower case Greek letters. But I (for now) am using non-bold upper case Latin Letters to denote linear transformations.

That said, these notes come from many different courses, and I may not have standardized everything. I'm sorry.

[a]The correspondence between Greek and Latin letters is somewhat arbitrary. For instance, one could make the case that Latin y corresponds to Greek υ, and not to Greek η. I should write out a guide.

- The set $L_2(P)$ of square-integrable random variables,

$$\boldsymbol{E}\, X^2 < \infty$$

  on the probability space $(S, \mathcal{E}, P)$ is a real vector space.

- The set of solutions to a homogeneous linear differential equation, e.g., $f'' + \alpha f' + \beta f = 0$, is a real vector space.

- The sequence spaces ℓ_p,

$$\ell_p = \Big\{ \boldsymbol{x} = (x_1, x_2, \dots) \in \boldsymbol{R}^{\mathbb{N}} : \sum_{n=1}^{\infty} |x_n|^p < \infty \Big\}, \quad 0 < p < \infty$$

$$\ell_\infty = \Big\{ \boldsymbol{x} = (x_1, x_2, \dots) : \sup_n |x_n| < \infty \Big\}$$

  are real vector spaces.[1]

[1]This is another example of where it seems inappropriate to use Greek letters for scalars.

- The set $\mathbf{M}(m,n)$ of $m \times n$ real matrices is a real vector space.
- The set of linear transformations from one vector space into another is a linear space. See Proposition 12 below.
- We can even consider the set $\boldsymbol{R}$ of real numbers as an (infinite-dimensional, see below) vector space over the field $\mathbb{Q}$ of rational numbers. This leads to some very interesting (counter-)examples.

3 Some elementary consequences

Here are some simple consequences of the axioms that we shall use repeatedly without further comment.

1. $\mathbf{0}$ is unique.
$$\mathbf{0}_2 \underbrace{=}_{\text{by V.3}} \mathbf{0}_2 + \mathbf{0}_1 \underbrace{=}_{\text{by V.1}} \mathbf{0}_1 + \mathbf{0}_2 \underbrace{=}_{\text{by V.3}} \mathbf{0}_1$$

2. $-\boldsymbol{x} = (-1)\boldsymbol{x}$ is the unique vector $\boldsymbol{z}$ satisfying $\boldsymbol{x} + \boldsymbol{z} = \mathbf{0}$. Suppose
$$\begin{aligned}
\boldsymbol{x} + \boldsymbol{y} &= \mathbf{0} \\
\underbrace{-\boldsymbol{x} + \boldsymbol{x}} + \boldsymbol{y} &= -\boldsymbol{x} \\
\mathbf{0} + \boldsymbol{y} &= -\boldsymbol{x} \\
\boldsymbol{y} &= -\boldsymbol{x}.
\end{aligned}$$

3. $0_K \boldsymbol{x} = \mathbf{0}_V$:
$$\mathbf{0}_V = 0_K \boldsymbol{x} + (-1)(0_K \boldsymbol{x}) = (0_K - 0_K)\boldsymbol{x} = 0_K \boldsymbol{x}.$$

4. $\underbrace{\boldsymbol{x} + \cdots + \boldsymbol{x}}_{n} = n\boldsymbol{x}$:
$$\boldsymbol{x} + \boldsymbol{x} = 1\boldsymbol{x} + 1\boldsymbol{x} = (1+1)\boldsymbol{x} = 2\boldsymbol{x}$$
$$\boldsymbol{x} + \boldsymbol{x} + \boldsymbol{x} = (\boldsymbol{x} + \boldsymbol{x}) + \boldsymbol{x} = 2\boldsymbol{x} + \boldsymbol{x} = 2\boldsymbol{x} + 1\boldsymbol{x} = (2+1)\boldsymbol{x} = 3\boldsymbol{x}$$
etc.

3.1 Linear combinations and subspaces

A **linear combination** of the vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$ is any sum of scalar multiples of vectors of the form $\alpha_1 \boldsymbol{x}_1 + \cdots + \alpha_m \boldsymbol{x}_m$, $\alpha_i \in K$, $\boldsymbol{x}_i \in V$. A **linear subspace** M of V is a nonempty subset of V that is closed under linear combinations. A linear subspace of a vector space is a vector space in its own right. A linear subspace may also be called a **vector subspace**.

Let $E \subset V$. The **span** of E, denoted $\operatorname{span} E$, is the set of all linear combinations from E. That is,
$$\operatorname{span} E = \Big\{ \sum_{i=1}^{m} \alpha_i \boldsymbol{x}_i : \alpha_i \in K, \boldsymbol{x}_i \in E, m \in \mathbb{N} \Big\}.$$

2 Exercise Prove the following.

1. $\{\mathbf{0}\}$ is a linear subspace.
2. If M is a linear subspace, then $\mathbf{0} \in M$.
3. The intersection of a family of linear subspaces is a linear subspace.
4. The set $\operatorname{span} E$ is the smallest (with respect to inclusion) linear subspace that includes E.

□

3.2 Linear independence

3 Definition *A set E of vectors is* ***linearly dependent*** *if there are distinct vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ belonging to E, and nonzero scalars $\alpha_1, \ldots, \alpha_m$, such that $\alpha_1 \boldsymbol{x}_1 + \cdots + \alpha_m \boldsymbol{x}_m = 0$. A set of vectors is* ***linearly independent*** *if it is not dependent. That is, E is independent if for every set $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ of distinct vectors in E, $\sum_{i=1}^m \alpha_i \boldsymbol{x}_i = 0$ implies $\alpha_1 = \cdots = \alpha_m = 0$. We also say that the vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ are independent instead of saying that the set $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\}$ is independent.*

4 Exercise Prove the following.

1. The empty set is independent.
2. If E is independent and $A \subset E$, then A is independent.
3. If $\mathbf{0} \in E$, then E is dependent.

□

5 Proposition (Uniqueness of linear combinations) *If E is a linearly independent set of vectors and $\boldsymbol{z}$ belongs to $\operatorname{span} E$, then $\boldsymbol{z}$ is a unique linear combination of elements of E.*

Proof: If $\boldsymbol{z}$ is zero, the conclusion follows by definition of independence. If $\boldsymbol{z}$ is nonzero, suppose

$$\boldsymbol{z} = \sum_{i=1}^{m} \alpha_i \boldsymbol{x}_i = \sum_{j=1}^{n} \beta_j \boldsymbol{y}_j,$$

where the $\boldsymbol{x}_i$'s are distinct elements of E, the $\boldsymbol{y}_j$'s are distinct are distinct elements of E (but may overlap with the $\boldsymbol{x}_i$'s), and $\alpha_i, \beta_j \neq 0$ for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. Enumerate $A = \{\boldsymbol{x}_i : i = 1, \ldots, m\} \cup \{\boldsymbol{y}_j : j = 1, \ldots, n\}$ as $A = \{\boldsymbol{z}_k : k = 1, \ldots, p\}$. (If $\boldsymbol{x}_i = \boldsymbol{y}_j$ for some i and j, then p is strictly less than $m + n$.) Then we can rewrite $\boldsymbol{z} = \sum_{k=1}^p \hat{\alpha}_k \boldsymbol{z}_k = \sum_{k=1}^p \hat{\beta}_k \boldsymbol{z}_k$, where

$$\hat{\alpha}_k = \begin{cases} \alpha_i & \text{if } \boldsymbol{z}_k = \boldsymbol{x}_i \\ 0 & \text{otherwise} \end{cases} \qquad \text{and} \qquad \hat{\beta}_k = \begin{cases} \beta_j & \text{if } \boldsymbol{z}_k = \boldsymbol{y}_j \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\mathbf{0} = \boldsymbol{z} - \boldsymbol{z} = \sum_{k=1}^{p} (\hat{\alpha}_k - \hat{\beta}_k) \boldsymbol{z}_k \implies \hat{\alpha}_k - \hat{\beta}_k = 0, \quad k = 1, \ldots, p$$

since E is independent. Therefore $\hat{\alpha}_k = \hat{\beta}_k$, $k = 1, \ldots, p$, which in turn implies $m = n = p$ and $\{\boldsymbol{x}_i : i = 1, \ldots, m\} = \{\boldsymbol{y}_j : j = 1, \ldots, n\}$, and the proposition is proved. ■

The coefficients of this linear combination are called the **coordinates of $\boldsymbol{x}$ with respect to the set $\boldsymbol{E}$**.

3.3 Bases and dimension

6 Definition *A **Hamel basis**, or more succinctly, a **basis** for the linear space V is a linearly independent set B such that* $\operatorname{span} B = V$. *The plural of* basis *is* bases.

The next result is immediate from Proposition 5.

7 Proposition *Every element of the vector space V is a* unique *linear combination of basis vectors.*

8 Example (The standard basis for $\boldsymbol{R}^{\mathrm{m}}$) The set of unit coordinate vectors $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m$ in $\boldsymbol{R}^{\mathrm{m}}$ is a basis for $\boldsymbol{R}^{\mathrm{m}}$, called the **standard basis**.

Observe that the vector $\boldsymbol{x} = (\xi_1, \ldots, \xi_m)$ can be written uniquely as $\sum_{j=1}^{m} \xi_j e_j$. □

The fundamental facts about bases are these. For a proof of the first assertion, see the *Hitchhiker's Guide* [2, Theorem 1.8, p. 15].

9 Fact *Every nontrivial vector space has a basis. Any two bases have the same cardinality, called the **dimension** of V.*

Prove the second half for finite-dimensional case.

Mostly these notes deal with finite-dimensional vector spaces. The next result summarizes Theorems 1.5, 1.6, and 1.7 in Apostol [6, pp. 10–12]]

10 Theorem *In an n-dimensional space, every set of more than n vectors is dependent. Consequently, any independent set of n vectors is a basis.*

3.4 Linear transformations

11 Definition *Let V, W be vector spaces. A function $T \colon V \to W$ is a **linear transformation** or **linear operator** or **homomorphism** if*

$$T(\alpha\boldsymbol{x} + \beta\boldsymbol{y}) = \alpha T(\boldsymbol{x}) + \beta T(\boldsymbol{y}).$$

The set of linear transformations from the vector space V into the vector space W is denoted

$$\mathsf{L}(V, W).$$

*If T is a linear transformation from a vector space into the reals $\boldsymbol{R}$, then it is customary to call T a **linear functional**.*

*The set $\mathsf{L}(V, \boldsymbol{R})$ of linear functionals on V is called the **dual space** of V, and is denoted V'. When there is a notion of continuity, we shall let V^* denote the vector space of continuous linear functionals on V.*

*The set V' is often called the **algebraic dual** of V and V^* is the **topological dual** of V.*

Note that if T is linear, then $T\mathbf{0}_V = \mathbf{0}_W$. We shall use this fact without any special mention. It is traditional to write a linear transformation without parentheses, that is, to write $T\boldsymbol{x}$ rather than $T(\boldsymbol{x})$.

12 Proposition $\mathsf{L}(V, W)$ *is itself a vector space under the usual pointwise addition and scalar multiplication of functions.*

3.5 The coordinate mapping

In an m-dimensional space V, if we fix a basis in some particular order, we have an **ordered basis** or **frame**. Given this ordered basis the coordinates of a vector comprise an ordered list, and so correspond to an element in $\boldsymbol{R}^{\mathrm{m}}$. This mapping from vectors to their coordinates is called the **coordinate mapping** for the ordered basis. The coordinate mapping preserves all the vector operations. The mathematicians' term for this is isomorphism. If two vector spaces are isomorphic, then for many purposes we can think of them as being the same space, the only difference being that the names of the points have been changed.

13 Definition *An* ***isomorphism*** *between vector spaces is a bijective linear transformation. That is, a function $\varphi\colon V \to W$ between vector spaces is an isomorphism if φ is one-to-one and onto, and*

$$\varphi(\boldsymbol{x} + \boldsymbol{y}) = \varphi(\boldsymbol{x}) + \varphi(\boldsymbol{y}) \quad \textit{and} \quad \varphi(\alpha\boldsymbol{x}) = \alpha\varphi(\boldsymbol{x}).$$

In this case we say that V and W are ***isomorphic****.*

We have just argued the following.

14 Proposition *Given an ordered basis $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ for an m-dimensional vector space V, the coordinate mapping is an isomorphism from V to $\boldsymbol{R}^{\mathrm{m}}$.*

If any n-dimensional vector space is isomorphic to $\boldsymbol{R}^{\mathrm{m}}$, is there any reason to consider n-dimensional vector spaces other than $\boldsymbol{R}^{\mathrm{m}}$? The answer, I believe, is yes. Sometimes there is no "natural" ordered basis for a vector space, so there is no "natural" way to treat it as $\boldsymbol{R}^{\mathrm{m}}$. For instance, let V be the set of vectors $\boldsymbol{x} = (x_1, \ldots, x_3)$ in $\boldsymbol{R}^3$, such that $x_1 + x_2 + x_3 = 0$. This is a 2-dimensional vector space, and there are infinitely many isomorphisms of V onto $\boldsymbol{R}^2$, but I assert that there is no unique obvious, natural way to identify points in V with points in $\boldsymbol{R}^2$.

4 Metrics and Norms

A metric on a vector space can be used to define convergence, open, and closed sets. That is, it turns the vector space into a **topological vector space**.

15 Definition *A* ***metric*** *d on a set V is a nonnegative real function on $V \times V$ that satisfies:*

M.1 $d(x, y) \geqslant 0$.

M.2 $d(x, y) = 0 \implies x = y$.

M.3 $d(x, y) = d(y, x)$.

M.4 (Triangle inequality) $d(x, y) \leqslant d(x, z) + d(z, y)$.

On vector spaces, a metric is usually defined in terms of a norm, which can be interpreted as the length of a vector.

16 Definition *A **norm** $\|\boldsymbol{x}\|$ is a nonnegative real function on a vector space that satisfies:*

N.1 $\|\mathbf{0}\| = 0$.

N.2 $\|\boldsymbol{x}\| > 0$ *if* $\boldsymbol{x} \neq \mathbf{0}$.

N.3 $\|\alpha\boldsymbol{x}\| = |\alpha| \; \|\boldsymbol{x}\|$.

N.4 $\|\boldsymbol{x} + \boldsymbol{y}\| \leqslant \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$ *with equality if and only if* $\boldsymbol{x} = 0$ *or* $\boldsymbol{y} = 0$ *or* $\boldsymbol{y} = \alpha\boldsymbol{x}$, $\alpha > 0$.

17 Proposition *If* $\|\cdot\|$ *is a norm, then*

$$d(x, y) = \|x - y\|$$

is a metric.

There are several commonly used norms on $\boldsymbol{R}^{\mathrm{m}}$.

18 Definition *The function defined by*

$$\|x\|_p = \left(\sum_{i=1}^{m} |x_i|^p\right)^{\frac{1}{p}}$$

is a norm on $\boldsymbol{R}^{\mathrm{m}}$ *called the **p-norm**. The function*

$$\|x\|_\infty = \max_i |x_i|$$

is a norm on $\boldsymbol{R}^{\mathrm{m}}$ *called the **∞-norm**.*

This definition also includes elements of a lemma, since it asserts that the functions so defined are norms. The 2-norm $\|\cdot\|_2$ is the usual **Euclidean norm**. The 1-norm is sometimes called the “taxicab” norm, since taxis are confined to rectangular street grids. The ∞-norm is also called the max-norm or the sup-norm.

5 Inner product

An inner product is related to angles between vectors, see Section 5.3.

19 Definition *A real linear space V has an **inner product** if for each pair of vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ there is a real number, traditionally denoted $(\boldsymbol{x}, \boldsymbol{y})$, satisfying the following properties.*

IP.1 $(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{y}, \boldsymbol{x})$.

IP.2 $(\boldsymbol{x}, \boldsymbol{y} + \boldsymbol{z}) = (\boldsymbol{x}, \boldsymbol{y}) + (\boldsymbol{x}, \boldsymbol{z})$.

IP.3 $\alpha(\boldsymbol{x}, \boldsymbol{y}) = (\alpha\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}, \alpha\boldsymbol{y})$.

IP.4 $(\boldsymbol{x}, \boldsymbol{x}) > 0$ *if* $\boldsymbol{x} \neq \boldsymbol{0}$.

A vector space V equipped with an inner product is called an ***inner product space****.*

For a complex vector space, the inner product is complex-valued, and property (1) is replaced by $(\boldsymbol{x}, \boldsymbol{y}) = \overline{(\boldsymbol{y}, \boldsymbol{x})}$, where the bar denotes complex conjugation, and (3) is replaced by $\alpha(\boldsymbol{x}, \boldsymbol{y}) = (\alpha\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}, \overline{\alpha}\boldsymbol{y})$.

The next results are straightforward and will be used without any explicit mention.

20 Lemma *For any x, we have $(\boldsymbol{x}, \boldsymbol{x}) \geqslant 0$, and $(\boldsymbol{0}, \boldsymbol{x}) = (\boldsymbol{x}, \boldsymbol{0}) = 0$. Consequently, $(\boldsymbol{x}, \boldsymbol{y}) = 0$ for all $\boldsymbol{y}$ if and only if $\boldsymbol{x} = \boldsymbol{0}$.*

21 Proposition *In a real inner product space, the inner product is* ***bilinear****. That is,*

$$(\alpha\boldsymbol{x} + \beta\boldsymbol{y}, \boldsymbol{z}) = \alpha(\boldsymbol{x}, \boldsymbol{z}) + \beta(\boldsymbol{y}, \boldsymbol{z}) \quad \text{and} \quad (\boldsymbol{z}, \alpha\boldsymbol{x} + \beta\boldsymbol{y}) = \alpha(\boldsymbol{z}, \boldsymbol{x}) + \beta(\boldsymbol{z}, \boldsymbol{y})$$

22 Lemma *If $(\boldsymbol{x}, \boldsymbol{z}) = (\boldsymbol{y}, \boldsymbol{z})$ for all $\boldsymbol{z}$, then $\boldsymbol{x} = \boldsymbol{y}$.*

Proof: Bilinearity implies $((\boldsymbol{x} - \boldsymbol{y}), \boldsymbol{z}) = 0$ for all $\boldsymbol{z}$, Lemma 20 $\boldsymbol{x} - \boldsymbol{y} = \boldsymbol{0}$. ∎

Another simple consequence for real inner product spaces is the following identity that we shall use often.

$$(\boldsymbol{x} + \boldsymbol{y}, \boldsymbol{x} + \boldsymbol{y}) = (\boldsymbol{x}, \boldsymbol{x}) + 2(\boldsymbol{x}, \boldsymbol{y}) + (\boldsymbol{y}, \boldsymbol{y})$$

For complex inner product spaces, this becomes

$$(\boldsymbol{x} + \boldsymbol{y}, \boldsymbol{x} + \boldsymbol{y}) = (\boldsymbol{x}, \boldsymbol{x}) + (\boldsymbol{x}, \boldsymbol{y}) + (\boldsymbol{y}, \boldsymbol{x}) + (\boldsymbol{y}, \boldsymbol{y}) = (\boldsymbol{x}, \boldsymbol{x}) + (\boldsymbol{x}, \boldsymbol{y}) + \overline{(\boldsymbol{x}, \boldsymbol{y})} + (\boldsymbol{y}, \boldsymbol{y})$$

23 Example The **dot product** of two vectors $\boldsymbol{x} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m)$ and $\boldsymbol{y} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$ in $\boldsymbol{R}^{\mathrm{m}}$ is defined by

$$\boldsymbol{x} \cdot \boldsymbol{y} = \sum_{i=1}^{m} x_i y_i.$$

The dot product is an inner product, and **Euclidean $\boldsymbol{m}$-space** is $\boldsymbol{R}^{\mathrm{m}}$ equipped with this inner product. The dot product of two vectors is zero if they meet at a right angle. □

24 Cauchy–Schwartz Inequality *In a real inner product space,*

$$(\boldsymbol{x}, \boldsymbol{y})^2 \leqslant (\boldsymbol{x}, \boldsymbol{x})(\boldsymbol{y}, \boldsymbol{y}) \tag{1}$$

with $=$ if and only if $\boldsymbol{x}$ and $\boldsymbol{y}$ are dependent.

Proof: (Cf. MacLane and Birkhoff [17, p. 353] or van der Waerden [22, p. 161]) If $\boldsymbol{x}$ or $\boldsymbol{y}$ is zero, then we have equality, so assume $\boldsymbol{x}, \boldsymbol{y}$ are nonzero. Define the quadratic $Q \colon \boldsymbol{R} \to \boldsymbol{R}$ by

$$Q(\lambda) = (\lambda\boldsymbol{x} + \boldsymbol{y}, \lambda\boldsymbol{x} + \boldsymbol{y}) = (\boldsymbol{x}, \boldsymbol{x})\lambda^2 + 2(\boldsymbol{x}, \boldsymbol{y})\lambda + (\boldsymbol{y}, \boldsymbol{y}).$$

By Property IP.4 of inner products (Definition 19), $Q(\lambda) \geqslant 0$ for each $\lambda \in \boldsymbol{R}$. Therefore the discriminant of Q is nonpositive, [2] that is, $4(\boldsymbol{x},\boldsymbol{y})^2 - 4(\boldsymbol{x},\boldsymbol{x})(\boldsymbol{y},\boldsymbol{y}) \leqslant 0$, or $(\boldsymbol{x},\boldsymbol{y})^2 \leqslant (\boldsymbol{x},\boldsymbol{x})(\boldsymbol{y},\boldsymbol{y})$. Equality in (1) can occur only if the discriminant is zero, in which case Q has a real root. That is, there is some λ for which $Q(\lambda) = (\lambda\boldsymbol{x}+\boldsymbol{y}, \lambda\boldsymbol{x}+\boldsymbol{y}) = 0$. But this implies that $\lambda\boldsymbol{x}+\boldsymbol{y} = \boldsymbol{0}$, which means the vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ are linearly dependent. ∎

25 Proposition *If $(\cdot,\cdot)$ is an inner product, then $\|\boldsymbol{x}\| = (\boldsymbol{x},\boldsymbol{x})^{\frac{1}{2}}$ is a norm.*

Proof: The only nontrivial part is showing Property N.4: $\|\boldsymbol{x}+\boldsymbol{y}\| \leqslant \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$ with equality if and only if $\boldsymbol{x} = 0$ or $\boldsymbol{y} = 0$ or $\boldsymbol{y} = \alpha\boldsymbol{x}$, $\alpha > 0$.

So observe that the Cauchy–Schwartz Inequality 24, $(\boldsymbol{x},\boldsymbol{y})^2 \leqslant (\boldsymbol{x},\boldsymbol{x})(\boldsymbol{y},\boldsymbol{y})$, is equivalent to

$$(\boldsymbol{x},\boldsymbol{y}) \leqslant \sqrt{(\boldsymbol{x},\boldsymbol{x})(\boldsymbol{y},\boldsymbol{y})}.$$

Multiply by 2 and add $(\boldsymbol{x},\boldsymbol{x}) + (\boldsymbol{y},\boldsymbol{y})$ to both sides to get

$$\underbrace{(\boldsymbol{x},\boldsymbol{x}) + 2(\boldsymbol{x},\boldsymbol{y}) + (\boldsymbol{y},\boldsymbol{y})}_{=(\boldsymbol{x}+\boldsymbol{y},\boldsymbol{x}+\boldsymbol{y})=\|\boldsymbol{x}+\boldsymbol{y}\|^2} \leqslant \underbrace{(\boldsymbol{x},\boldsymbol{x}) + 2\sqrt{(\boldsymbol{x},\boldsymbol{x})(\boldsymbol{y},\boldsymbol{y})} + (\boldsymbol{y},\boldsymbol{y})}_{=\left(\|\boldsymbol{x}\|+\|\boldsymbol{y}\|\right)^2}$$

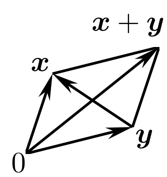
Taking square roots of both sides gives

$$\|\boldsymbol{x}+\boldsymbol{y}\| \leqslant \|\boldsymbol{x}\| + \|\boldsymbol{y}\|.$$

Now equality holds in Cauchy–Schwartz if and only $\boldsymbol{x}$ and $\boldsymbol{y}$ are linearly dependent. So to finish the proof of N.4, we still have to show that if $\boldsymbol{y}$ and $\boldsymbol{x}$ are both nonzero, $\boldsymbol{y} = \alpha\boldsymbol{x}$ and we have equality above if and only if $\alpha > 0$. But equality reduces to $|1+\alpha| = 1 + |\alpha|$, which reduces to $\alpha \geqslant 0$, and the case $\alpha = 0$ is ruled out by $\boldsymbol{y} \neq 0$. ∎

If the norm induced by the inner product gives rise to a complete metric space,[3] then the inner product space is called a **Hilbert space** or **complete inner product space**.

5.1 The Parallelogram Law



The next result asserts that in an inner product space, the sum of the squares of the lengths of the diagonals of a parallelogram is equal to the sum of the squares of the lengths of the sides. Consider the parallelogram with vertices $\boldsymbol{0}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y}$. Its diagonals are the segments $[\boldsymbol{0}, \boldsymbol{x}+\boldsymbol{y}]$ and $[\boldsymbol{x}, \boldsymbol{y}]$, and their lengths are $\|\boldsymbol{x}+\boldsymbol{y}\|$ and $\|\boldsymbol{x}-\boldsymbol{y}\|$. It has two sides of length $\|\boldsymbol{x}\|$ and two of length $\|\boldsymbol{y}\|$. So the claim is:

[2] In case you have forgotten how you derived the quadratic formula in Algebra I, rewrite the polynomial as

$$f(z) = \alpha z^2 + \beta z + \gamma = \tfrac{1}{\alpha}\left(\alpha z + \tfrac{\beta}{2}\right)^2 - (\beta^2 - 4\alpha\gamma)/4\alpha,$$

and note that the only way to guarantee that $f(z) \geqslant 0$ for all z is to have $\alpha > 0$ and $\beta^2 - 4\alpha\gamma \leqslant 0$.

[3] A metric space is **complete** if every Cauchy sequence has a limit point in the space. A sequence $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots$ is a **Cauchy sequence** if $\lim \|x_m - x_n\| = 0$ as $n, m \to \infty$.

26 The Parallelogram Law *In an inner product space,*

$$\|\boldsymbol{x}+\boldsymbol{y}\|^2 + \|\boldsymbol{x}-\boldsymbol{y}\|^2 = 2\,\|\boldsymbol{x}\|^2 + 2\,\|\boldsymbol{y}\|^2 .$$

Proof: Note that

$$\begin{aligned}\big((\boldsymbol{x}+\boldsymbol{y}),(\boldsymbol{x}+\boldsymbol{y})\big) &= (\boldsymbol{x},\boldsymbol{x}) + 2(\boldsymbol{x},\boldsymbol{y}) + (\boldsymbol{y},\boldsymbol{y})\\ \big((\boldsymbol{x}-\boldsymbol{y}),(\boldsymbol{x}-\boldsymbol{y})\big) &= (\boldsymbol{x},\boldsymbol{x}) - 2(\boldsymbol{x},\boldsymbol{y}) + (\boldsymbol{y},\boldsymbol{y}).\end{aligned}$$

Add these two to get

$$\big((\boldsymbol{x}+\boldsymbol{y}),(\boldsymbol{x}+\boldsymbol{y})\big) + \big((\boldsymbol{x}-\boldsymbol{y}),(\boldsymbol{x}-\boldsymbol{y})\big) = 2(\boldsymbol{x},\boldsymbol{x}) + 2(\boldsymbol{y},\boldsymbol{y}),$$

and the desired result is restated in terms of norms. ∎

On a related note, we have the following.

27 Proposition *In an inner product space.*

$$\|\boldsymbol{x}+\boldsymbol{y}\|^2 - \|\boldsymbol{x}-\boldsymbol{y}\|^2 = 4(\boldsymbol{x},\boldsymbol{y}).$$

Proof: In the proof above, instead of adding the two equations, subtract them.

$$\begin{aligned}\|\boldsymbol{x}+\boldsymbol{y}\|^2 - \|\boldsymbol{x}-\boldsymbol{y}\|^2 &= \big((\boldsymbol{x}+\boldsymbol{y}),(\boldsymbol{x}+\boldsymbol{y})\big) - \big((\boldsymbol{x}-\boldsymbol{y}),(\boldsymbol{x}-\boldsymbol{y})\big)\\ &= (\boldsymbol{x},\boldsymbol{x}) + 2(\boldsymbol{x},\boldsymbol{y}) + (\boldsymbol{y},\boldsymbol{y}) - \big((\boldsymbol{x},\boldsymbol{x}) - 2(\boldsymbol{x},\boldsymbol{y}) + (\boldsymbol{y},\boldsymbol{y})\big)\\ &= 4(\boldsymbol{x},\boldsymbol{y}).\end{aligned}$$

∎

As an aside, a norm on a vector space is induced by an inner product if and only if it satisfies the Parallelogram Law; see for instance [3, Problem 32.10, p. 303].

5.2 Orthogonality

28 Definition *Vectors* $\boldsymbol{x}$ *and* $\boldsymbol{y}$ *are* ***orthogonal*** *if* $(\boldsymbol{x},\boldsymbol{y}) = 0$*, written*

$$\boldsymbol{x} \perp \boldsymbol{y}.$$

A set of vectors $E \subset V$ *is* ***orthogonal*** *if it is pairwise orthogonal. That is, for all* $\boldsymbol{x},\boldsymbol{y} \in E$ *with* $\boldsymbol{x} \neq \boldsymbol{y}$ *we have* $(\boldsymbol{x},\boldsymbol{y}) = 0$*. A set* E *is* ***orthonormal*** *if* E *is orthogonal and* $(\boldsymbol{x},\boldsymbol{x}) = 1$ *for all* $\boldsymbol{x} \in E$*.*

29 Lemma *If a set of nonzero vectors is pairwise orthogonal, then the set is independent.*

Proof: Suppose $\sum_{i=1}^m \alpha_i \boldsymbol{x}_i = 0$, where the $\boldsymbol{x}_i$'s are pairwise orthogonal. Then for each k,

$$0 = (\boldsymbol{x}_k, \boldsymbol{0}) = \Big(\boldsymbol{x}_k, \sum_{i=1}^m \alpha_i \boldsymbol{x}_i\Big) = \sum_{i=1}^m \alpha_i (\boldsymbol{x}_k, \boldsymbol{x}_i) = \alpha_k (\boldsymbol{x}_k, \boldsymbol{x}_k).$$

But $\boldsymbol{x}_k \neq 0$, so $(\boldsymbol{x}_k, \boldsymbol{x}_k) > 0$, so $\alpha_k = 0$. That is, the vectors $\boldsymbol{x}_i$ are linearly independent. ∎

5.3 The Pythagorean Theorem and the geometry of the Euclidean inner product

The Pythagorean Theorem is usually stated in terms of right triangles in the plane. Two vectors meet at a right angle if they are orthogonal in the Euclidean inner product. See Figure 1. The theorem has a generalization to arbitrary inner product spaces.

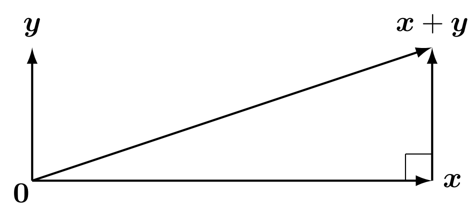


Figure 1. Pythagorean Theorem: $\boldsymbol{x} \perp \boldsymbol{y}$ if and only the triangle with vertices $\mathbf{0}$, $\boldsymbol{x}$, and $\boldsymbol{y}+\boldsymbol{x}$ is a right triangle with hypotenuse $\boldsymbol{x}+\boldsymbol{y}$, in which case, $\|\boldsymbol{x}+\boldsymbol{y}\|^2 = \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2$.

30 Pythagorean Theorem *In an inner product space*

$$\|\boldsymbol{x}+\boldsymbol{y}\|^2 = \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 \quad \textit{if and only if} \quad \boldsymbol{x} \perp \boldsymbol{y}.$$

Proof: Bilinearity implies

$$\|\boldsymbol{x}+\boldsymbol{y}\|^2 = (\boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y}) = (\boldsymbol{x}, \boldsymbol{x}) + 2(x,\boldsymbol{y}) + (\boldsymbol{y}, \boldsymbol{y}) = \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 + 2(\boldsymbol{x}, \boldsymbol{y}),$$

and the conclusion follows. ∎

The triangle with vertices $\mathbf{0}$, $\boldsymbol{x}$, and $\boldsymbol{z}$ is a right triangle with hypotenuse $\boldsymbol{z}$ if $\boldsymbol{x} \perp \boldsymbol{y} = \boldsymbol{z} - \boldsymbol{x}$. But even if $\boldsymbol{x}$ and $\boldsymbol{z} - \boldsymbol{x}$ are not orthogonal, as long as $\boldsymbol{x}$ and $\boldsymbol{z}$ are not collinear and nonzero, then there is a scalar multiple of $\boldsymbol{x}$ that will make a right triangle. To see this, write $\boldsymbol{z} = \alpha\boldsymbol{x} + \boldsymbol{y}$ and find α to make $\boldsymbol{y} = \boldsymbol{z} - \alpha\boldsymbol{x}$ satisfy $\boldsymbol{y} \cdot \boldsymbol{x} = 0$. In other words we want the following lemma.

31 Lemma *In an inner product space,*

$$(\boldsymbol{z} - \alpha\boldsymbol{x}) \perp \boldsymbol{x}, \quad \textit{where} \quad \alpha = \frac{(\boldsymbol{x}, \boldsymbol{z})}{(\boldsymbol{x}, \boldsymbol{x})}.$$

Proof: We have

$$\Big((\boldsymbol{z} - \alpha\boldsymbol{x}), \boldsymbol{x}\Big) = (\boldsymbol{z}, \boldsymbol{x}) - (\alpha\boldsymbol{x}, \boldsymbol{x}) = 0 \quad \Longrightarrow \quad \alpha = \frac{(\boldsymbol{x}, \boldsymbol{z})}{(\boldsymbol{x}, \boldsymbol{x})}.$$

∎

This leads to the following geometric interpretation of the Euclidean inner product.

32 Proposition *For nonzero vectors $\boldsymbol{x}$ and $\boldsymbol{z}$ in a Euclidean space,*

$$\boldsymbol{x} \cdot \boldsymbol{z} = \|\boldsymbol{x}\| \, \|\boldsymbol{z}\| \, \cos\theta,$$

where θ is the angle between $\boldsymbol{x}$ and $\boldsymbol{z}$.

Proof: Let $\alpha = \frac{(\boldsymbol{x},\boldsymbol{z})}{(\boldsymbol{x},\boldsymbol{x})}$. Referring to Figure 2 we see that

$$\cos\theta = \alpha \frac{\|\boldsymbol{x}\|}{\|\boldsymbol{y}\|} = \frac{\boldsymbol{x} \cdot \boldsymbol{y}}{\|\boldsymbol{x}\| \, \|\boldsymbol{y}\|},$$

This works even when $\alpha < 0$, which means θ is an obtuse angle. ∎

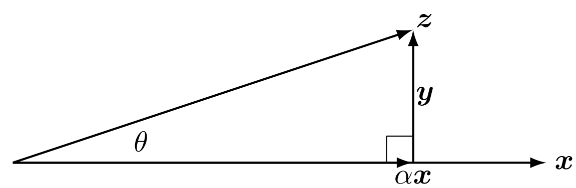


Figure 2. Dot product and angles: $\cos\theta = \dfrac{\alpha \, \|\boldsymbol{x}\|}{\|\boldsymbol{z}\|} = \dfrac{\boldsymbol{x} \cdot \boldsymbol{z}}{\|\boldsymbol{x}\| \, \|\boldsymbol{z}\|}$.

33 Definition *In a real inner product space, the* **angle** $\angle \boldsymbol{xy}$ *between two nonzero vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ is defined to be*

$$\angle \boldsymbol{xy} = \arccos \frac{(\boldsymbol{x},\boldsymbol{y})}{\sqrt{(\boldsymbol{x},\boldsymbol{x})\,(\boldsymbol{y},\boldsymbol{y})}}.$$

5.4 Orthogonal projection and orthogonal complements

34 Definition *The* ***orthogonal complement*** *of M in V is the set*

$$\{\boldsymbol{x} \in V : (\forall \boldsymbol{y} \in M)\ [\,\boldsymbol{x} \perp \boldsymbol{y}\,]\},$$

denoted $M_\perp$.

35 Lemma *If $\boldsymbol{x} \perp \boldsymbol{y}$ and $\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{0}$, then $\boldsymbol{x} = \boldsymbol{y} = \boldsymbol{0}$.*

Proof: Now $(\boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y}) = (\boldsymbol{x},\boldsymbol{x}) + 2(\boldsymbol{x},\boldsymbol{y}) + (\boldsymbol{y},\boldsymbol{y})$, so $(\boldsymbol{x},\boldsymbol{y}) = 0$ implies $(\boldsymbol{x},\boldsymbol{x}) + (\boldsymbol{y},\boldsymbol{y}) = 0$. Since $(\boldsymbol{x},\boldsymbol{x}) \geqslant 0$ and $(\boldsymbol{y},\boldsymbol{y}) \geqslant 0$ we have $\boldsymbol{x} = \boldsymbol{y} = \boldsymbol{0}$. ∎

The next lemma is left as an exercise.

36 Lemma *For any set M, the set $M_\perp$ is a linear subspace. If M is a subspace, then*

$$M \cap M_\perp = \{\boldsymbol{0}\}.$$

The fact that $M_\perp$ is a subspace is not by itself very useful. It might be the trivial subspace $\{\mathbf{0}\}$. We shall see below in Corollary 41 that for finite dimensional spaces, the dimensions of M and $M_\perp$ add up to the dimension of the entire space.

The next result may be found, for instance, in Apostol [6, Theorem 1.14, p. 24], and the proof is known as the **Gram–Schmidt procedure**. It can be viewed as a generalization of Lemma 31.

37 Proposition *Let $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots$ be a sequence (finite or infinite) of vectors in an inner product space. Then there exists a sequence $\boldsymbol{y}_1, \boldsymbol{y}_2, \dots$ such that for each m, the span of $\boldsymbol{y}_1, \dots, \boldsymbol{y}_m$ is the same as the span of $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$, and the $\boldsymbol{y}_i$'s are orthogonal.*

Proof: Set $\boldsymbol{y}_1 = \boldsymbol{x}_1$. For $m > 1$ recursively define

$$\boldsymbol{y}_m = \boldsymbol{x}_m - \frac{(\boldsymbol{x}_m, \boldsymbol{y}_{m-1})}{(\boldsymbol{y}_{m-1}, \boldsymbol{y}_{m-1})}\boldsymbol{y}_{m-1} - \frac{(\boldsymbol{x}_m, \boldsymbol{y}_{m-2})}{(\boldsymbol{y}_{m-2}, \boldsymbol{y}_{m-2})}\boldsymbol{y}_{m-2} - \cdots - \frac{(\boldsymbol{x}_m, \boldsymbol{y}_1)}{(\boldsymbol{y}_1, \boldsymbol{y}_1)}\boldsymbol{y}_1.$$

Use induction on m to prove that the vectors $\boldsymbol{y}_1, \dots, \boldsymbol{y}_m$ are orthogonal and span the same space as the $\boldsymbol{x}_i$'s. Observe that $\boldsymbol{y}_2$ is orthogonal to $\boldsymbol{y}_1 = \boldsymbol{x}_1$:

$$(\boldsymbol{y}_2, \boldsymbol{y}_1) = (\boldsymbol{y}_2, \boldsymbol{x}_1) = (\boldsymbol{x}_2, \boldsymbol{x}_1) - \frac{(\boldsymbol{x}_2, \boldsymbol{x}_1)}{(\boldsymbol{x}_1, \boldsymbol{x}_1)}(\boldsymbol{x}_2, \boldsymbol{x}_1) = 0.$$

Furthermore any linear combination of $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ can be replicated with $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$.

For $m > 2$, let $\boldsymbol{y}_1, \dots, \boldsymbol{y}_{m-1}$ be orthogonal and span the same space as $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{m-1}$. Now compute $(\boldsymbol{y}_m, \boldsymbol{y}_k)$ for $k \leqslant m$:

$$\begin{aligned}(\boldsymbol{y}_m, \boldsymbol{y}_k) &= (\boldsymbol{x}_m, \boldsymbol{y}_k) - \sum_{i=1}^{m-1} \left(\frac{(\boldsymbol{x}_m, \boldsymbol{y}_i)}{(\boldsymbol{y}_i, \boldsymbol{y}_i)}\boldsymbol{y}_i, \boldsymbol{y}_k \right) \\ &= (\boldsymbol{x}_m, \boldsymbol{y}_k) - \sum_{i=1}^{m-1} \frac{(\boldsymbol{x}_m, \boldsymbol{y}_i)}{(\boldsymbol{y}_i, \boldsymbol{y}_i)}(\boldsymbol{y}_i, \boldsymbol{y}_k) \\ &= (\boldsymbol{x}_m, \boldsymbol{y}_k) - \frac{(\boldsymbol{x}_m, \boldsymbol{y}_k)}{(\boldsymbol{y}_k, \boldsymbol{y}_k)}(\boldsymbol{y}_k, \boldsymbol{y}_k) \\ &= 0,\end{aligned}$$

so $\boldsymbol{y}_m$ is orthogonal to each $\boldsymbol{y}_1, \dots, \boldsymbol{y}_{m-1}$. As an exercise verify that the span of $\boldsymbol{y}_1, \dots, \boldsymbol{y}_m$ is the same as the span of $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$. ∎

38 Corollary *Every nontrivial finite-dimensional subspace of an inner product space has an orthonormal basis.*

Proof: Apply the Gram–Schmidt procedure to a basis. To obtain an orthonormal basis, simply normalize each $\boldsymbol{y}_k$ by dividing it by its norm $(\boldsymbol{y}_k, \boldsymbol{y}_k)^{1/2}$. ∎

39 Orthogonal Projection Theorem *Let M be a linear subspace of the finite-dimensional real inner product space V. For each $\boldsymbol{x} \in V$ we can write $\boldsymbol{x}$ in a unique way as $\boldsymbol{x} = \boldsymbol{x}_M + \boldsymbol{x}_\perp$, where $\boldsymbol{x}_M \in M$ and $\boldsymbol{x}_\perp \in M_\perp$.*

Proof: Let $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$ be an orthonormal basis for M. Put $\boldsymbol{z}_i = (\boldsymbol{x}, \boldsymbol{y}_i)\boldsymbol{y}_i$ for $i = 1, \ldots, m$. Put $\boldsymbol{x}_M = \sum_{i=1}^m \boldsymbol{z}_i$, and $\boldsymbol{x}_\perp = \boldsymbol{x} - \boldsymbol{x}_M$. Let $\boldsymbol{y} \in M$, $\boldsymbol{y} = \sum_{i=1}^m \alpha_i \boldsymbol{y}_i$. Then

$$\begin{aligned}
(\boldsymbol{y}, \boldsymbol{x}_\perp) &= \Big(\sum_{i=1}^m \alpha_i \boldsymbol{y}_i, \boldsymbol{x} - \sum_{j=1}^m (\boldsymbol{x}, \boldsymbol{y}_j)\boldsymbol{y}_j\Big) \\
&= \sum_{i=1}^m \alpha_i (\boldsymbol{y}_i, \boldsymbol{x} - \sum_{j=1}^m (\boldsymbol{x}, \boldsymbol{y}_j)\boldsymbol{y}_j) \\
&= \sum_{i=1}^m \alpha_i \Big\{(\boldsymbol{y}_i, \boldsymbol{x}) - (\boldsymbol{y}_i, \sum_{j=1}^m (\boldsymbol{x}, \boldsymbol{y}_j)\boldsymbol{y}_j)\Big\} \\
&= \sum_{i=1}^m \alpha_i \Big\{(\boldsymbol{y}_i, \boldsymbol{x}) - \sum_{j=1}^m (\boldsymbol{x}, \boldsymbol{y}_j)(\boldsymbol{y}_i, \boldsymbol{y}_j)\Big\} \\
&= \sum_{i=1}^m \alpha_i \{(\boldsymbol{y}_i, \boldsymbol{x}) - (\boldsymbol{x}, \boldsymbol{y}_i)\} \\
&= 0.
\end{aligned}$$

Uniqueness: Let $\boldsymbol{x} = \boldsymbol{x}_M + \boldsymbol{x}_\perp = \boldsymbol{z}_M + \boldsymbol{z}_\perp$. Then $\boldsymbol{0} = \underbrace{(\boldsymbol{x}_M - \boldsymbol{z}_M)}_{\in M} + \underbrace{(\boldsymbol{x}_\perp - \boldsymbol{z}_\perp)}_{\in M_\perp}$. Rewriting this yields $\boldsymbol{x}_M - \boldsymbol{z}_M = \boldsymbol{0} - (\boldsymbol{x}_\perp - \boldsymbol{z}_\perp)$, so $\boldsymbol{x}_M - \boldsymbol{z}_M$ also lies in $M_\perp$. Similarly $\boldsymbol{x}_\perp - \boldsymbol{z}_\perp$ also lies in M. Thus $\boldsymbol{x}_M - \boldsymbol{z}_M \in M \cap M_\perp = \{\boldsymbol{0}\}$ and $\boldsymbol{x}_\perp - \boldsymbol{z}_\perp \in M \cap M_\perp = \{\boldsymbol{0}\}$. ∎

40 Definition *The vector $\boldsymbol{x}_M$ given by the theorem above is called the* ***orthogonal projection*** *of $\boldsymbol{x}$ onto M.*

41 Corollary *For a finite-dimensional space V and any subspace M of V,* $\dim M + \dim M_\perp = \dim V$.

There is another important characterization of orthogonal projection.

42 Proposition (Orthogonal projection minimizes the norm of the "residual") *Let M be a linear subspace of the real inner product space V. Let $\boldsymbol{x} \in V$. Then*

$$\|\boldsymbol{x} - \boldsymbol{x}_M\| \leqslant \|x - z\| \quad \textit{for all } \boldsymbol{z} \in M.$$

Proof: This is really just the Pythagorean Theorem: Note that if $\boldsymbol{z} \in M$, then the points $\boldsymbol{x}$, $\boldsymbol{x}_M$, and $\boldsymbol{z}$ are the vertexes of a right triangle, where the sides $\overline{\boldsymbol{z}\boldsymbol{x}_M}$ and $\overline{\boldsymbol{x}_M\boldsymbol{x}}$ meet at a right angle, and $\overline{\boldsymbol{x}\boldsymbol{z}}$ is the hypotenuse. See Figure 3. (To prove that $\overline{\boldsymbol{z}\boldsymbol{x}_M}$ and $\overline{\boldsymbol{x}_M\boldsymbol{x}}$ meet at a right angle, note that $\boldsymbol{z} - \boldsymbol{x}_M$ also belongs to M, so it is orthogonal to $\boldsymbol{x}_\perp = \boldsymbol{x} - \boldsymbol{x}_M$.) So by Pythagoras

$$\begin{aligned}
\|\boldsymbol{x} - \boldsymbol{z}\|^2 &= \|\boldsymbol{x} - \boldsymbol{x}_M\|^2 + \|\boldsymbol{z} - \boldsymbol{x}_M\|^2 \\
&\geqslant \|\boldsymbol{x} - \boldsymbol{x}_M\|^2 .
\end{aligned}$$

That is, $\boldsymbol{z} = \boldsymbol{x}_M$ minimizes $\|\boldsymbol{x} - \boldsymbol{z}\|$ over M. ∎

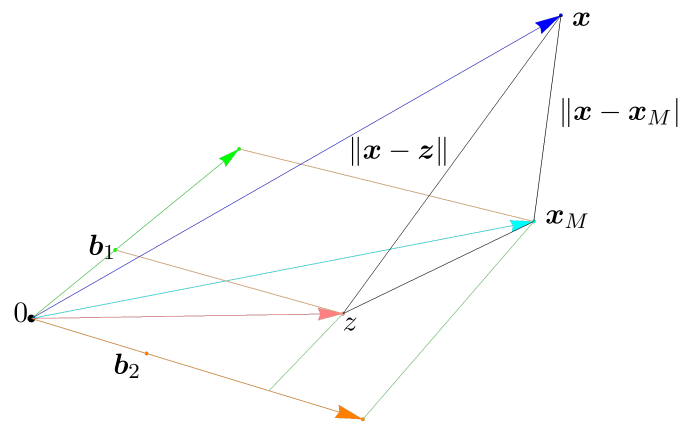


Figure 3. Orthogonal projection onto $M = \operatorname{span}\{\boldsymbol{b}_1, \boldsymbol{b}_2\}$ minimizes $\|\boldsymbol{x} - \boldsymbol{z}\|$ for $\boldsymbol{z} \in M$.

43 Proposition (Linearity of Projection) *Orthogonal projection satisfies*

$$(\boldsymbol{x} + \boldsymbol{z})_M = \boldsymbol{x}_M + \boldsymbol{z}_M \quad \textit{and} \quad (\alpha \boldsymbol{x})_M = \alpha \boldsymbol{x}_M.$$

Proof: Let $\boldsymbol{b}_1, \dots, \boldsymbol{b}_k$ be an orthonormal basis for M. Use $\boldsymbol{x}_M = \sum_{j=1}^k (\boldsymbol{x}, \boldsymbol{b}_j)\boldsymbol{b}_j$ and $\boldsymbol{z}_M = \sum_{j=1}^k (\boldsymbol{z}, \boldsymbol{b}_j)\boldsymbol{b}_j$. Then

$$(\boldsymbol{x} + \boldsymbol{z})_M = \sum_{j=1}^k (\boldsymbol{x} + \boldsymbol{z}, \boldsymbol{b}_j)\boldsymbol{b}_j.$$

Use linearity of $(\cdot, \cdot)$. ∎

5.5 Orthogonality and alternatives

We now present a lemma about linear functions that is true in quite general linear spaces, see the *Hitchhiker's Guide* [2, Theorem 5.91, p. 212], but we will prove it using some of the special properties of inner products.

44 Lemma *Let V be an inner product space. Then $\boldsymbol{y}$ is a linear combination of $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$ if and only if*

$$\bigcap_{i=1}^m \{\boldsymbol{x}_i\}_\perp \subset \{\boldsymbol{y}\}_\perp. \tag{2}$$

Proof: If $\boldsymbol{y}$ is a linear combination of $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$, say $\boldsymbol{y} = \sum_{i=1}^m \alpha_i \boldsymbol{x}_i$, then

$$(\boldsymbol{z}, \boldsymbol{y}) = \sum_{i=1}^m \alpha_i (\boldsymbol{z}, \boldsymbol{x}_i),$$

so (2) holds.

For the converse, suppose (2) holds. Let $M = \operatorname{span}\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_m\}$ and orthogonally project $\boldsymbol{y}$ onto M to get $\boldsymbol{y} = \boldsymbol{y}_M + \boldsymbol{y}_\perp$, where $\boldsymbol{y}_M \in M$ and $\boldsymbol{y}_\perp \perp M$. In particular, $(\boldsymbol{x}_i, \boldsymbol{y}_\perp) = 0$, $i = 1, \dots, m$. Consequently, by hypothesis, $(\boldsymbol{y}, \boldsymbol{y}_\perp) = 0$ too. But

$$0 = (\boldsymbol{y}, \boldsymbol{y}_\perp) = (\boldsymbol{y}_M, \boldsymbol{y}_\perp) + (\boldsymbol{y}_\perp, \boldsymbol{y}_\perp) = 0 + (\boldsymbol{y}_\perp, \boldsymbol{y}_\perp).$$

Thus $\boldsymbol{y}_\perp = \boldsymbol{0}$, so $\boldsymbol{y} = \boldsymbol{y}_M \in M$. That is, $\boldsymbol{y}$ is a linear combination of $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$. ∎

We can rephrase the above result as an alternative.

45 Corollary (Fredholm alternative) *Either there exist real numbers $\alpha_1, \dots, \alpha_m$ such that*

$$\boldsymbol{y} = \sum_{i=1}^{m} \alpha_i \boldsymbol{x}_i$$

or else there exists a vector $\boldsymbol{z}$ satisfying

$$(\boldsymbol{z}, \boldsymbol{x}_i) = 0, \ i = 1, \dots, m \quad \text{and} \quad (\boldsymbol{z}, \boldsymbol{y}) = 1.$$

6 The dual of an inner product space

Recall that the topological dual V^* of a vector space V is the vector subspace of $\mathsf{L}(V, \boldsymbol{R}) = V'$ consisting of continuous real linear functionals on V. When V is an inner product space, V^* has a particularly nice structure. It is clear from the bilinearity of the inner product (Proposition 21) that for every $\boldsymbol{y}$ in the real inner product space V, the function ℓ on V defined by

$$\ell(\boldsymbol{x}) = (\boldsymbol{y}, \boldsymbol{x})$$

is linear. Moreover, it is continuous with respect to the norm induced by the inner product.

46 Proposition *The inner product is jointly norm-continuous. That is, if $\|\boldsymbol{y}_n - \boldsymbol{y}\| \to 0$ and $\|\boldsymbol{x}_n - \boldsymbol{x}\| \to 0$, then $(\boldsymbol{y}_n, \boldsymbol{x}_n) \to (\boldsymbol{y}, \boldsymbol{x})$.*

Proof: By bilinearity and the Cauchy–Schwartz Inequality 24,

$$\begin{aligned}
|(\boldsymbol{y}_n, \boldsymbol{x}_n) - (\boldsymbol{y}, \boldsymbol{x})| &= |(\boldsymbol{y}_n \underbrace{- \boldsymbol{y} + \boldsymbol{y}}, \boldsymbol{x}_n \underbrace{- \boldsymbol{x} + \boldsymbol{x}}) - (\boldsymbol{y}, \boldsymbol{x})| \\
&= |(\boldsymbol{y}_n - \boldsymbol{y}, \boldsymbol{x}_n - \boldsymbol{x}) + (\boldsymbol{y}_n - \boldsymbol{y}, \boldsymbol{x}) + (\boldsymbol{y}, \boldsymbol{x}_n - \boldsymbol{x}) + (\boldsymbol{y}, \boldsymbol{x}) - (\boldsymbol{y}, \boldsymbol{x})| \\
&\leqslant \sqrt{\|\boldsymbol{y}_n - \boldsymbol{y}\| \, \|\boldsymbol{x}_n - \boldsymbol{x}\|} + \sqrt{\|\boldsymbol{y}_n - \boldsymbol{y}\| \, \|\boldsymbol{x}\|} + \sqrt{\|\boldsymbol{y}\| \, \|\boldsymbol{x}_n - \boldsymbol{x}\|} \\
&\xrightarrow[n \to \infty]{} 0.
\end{aligned}$$

∎

The converse is true if the inner product space is complete as a metric space, that is, if it is a Hilbert space. Every continuous linear functional on a real Hilbert space has the form of an inner product with some vector. The question is, which vector? If $\ell(\boldsymbol{x}) = (\boldsymbol{y}, \boldsymbol{x})$, then Section 5.3 suggests that ℓ is maximized on the unit sphere when the angle between $\boldsymbol{x}$ and $\boldsymbol{y}$ maximizes the cosine. The maximum value of the cosine is one, which occurs when the angle is zero, that is, when $\boldsymbol{x}$ is a positive multiple of $\boldsymbol{y}$. Thus to find y given ℓ, we need to find the maximizer of ℓ on the unit ball. But first we need to know that such a maximizer exists.

47 Theorem *Let V be a Hilbert space, and let U be its unit ball:*

$$U = \{\boldsymbol{x} \in V : (\boldsymbol{x}, \boldsymbol{x}) \leqslant 1\}.$$

Let ℓ be a continuous linear functional on V. Then ℓ has a maximizer in U. If ℓ is nonzero, the maximizer is unique and has norm 1.

Note that if V is finite dimensional, then U is compact, and the result follows from the Weierstrass Theorem. When V is infinite dimensional, the unit ball is not compact, so another technique is needed.

Proof: (Cf. Murray [19, pp. 12–13]) The case where ℓ is the zero functional is obvious, so restrict attention to the case where ℓ is not identically zero.

First observe that if ℓ is continuous, then it is bounded on U. To see this, consider the standard ε-δ definition of continuity at 0, where $\varepsilon = 1$. Then there is some $\delta > 0$ such that if $\|\boldsymbol{x}\| = \|\boldsymbol{x} - \boldsymbol{0}\| < \delta$, then $|\ell(x)| = |\ell(x) - \ell(0)| < 1$. Thus ℓ is bounded by $|1/\delta|$ on U.

So let $\mu = \sup_{\boldsymbol{x} \in U} \ell(\boldsymbol{x})$, and note that $0 < \mu < \infty$. Since $\boldsymbol{x} \in U$ implies $-\boldsymbol{x} \in U$ we also have that $-\mu =\in f_{\boldsymbol{x} \in U} \ell(\boldsymbol{x})$. The scalar μ is called the **operator norm** of ℓ. It has the property that for any $\boldsymbol{x} \in V$,

$$|\ell(\boldsymbol{x})| \leqslant \mu \|\boldsymbol{x}\|. \tag{3}$$

To see this for nonzero $\boldsymbol{x}$, observe that $\boldsymbol{x}/\|\boldsymbol{x}\| \in U$ so $|\ell(\boldsymbol{x}/\|\boldsymbol{x}\|)| \leqslant \mu$, and the result follows by multiplying by both sides by $\|\boldsymbol{x}\|$.

Pick a sequence $\boldsymbol{x}_n$ in U with $\ell(\boldsymbol{x}_n)$ approaching the supremum μ that satisfies

$$\ell(\boldsymbol{x}_n) \geqslant \tfrac{n-1}{n}\mu. \tag{4}$$

We shall show that the sequence $\boldsymbol{x}_n$ is a Cauchy sequence, and so has a limit. This limit is the maximizer. To see that we have a Cauchy sequence, we use the Parallelogram Law 26 to write

$$\|\boldsymbol{x}_n - \boldsymbol{x}_m\|^2 = 2\|\boldsymbol{x}_n\|^2 + 2\|\boldsymbol{x}_m\|^2 - \|\boldsymbol{x}_n + \boldsymbol{x}_m\|^2. \tag{5}$$

Now observe that by (3) and (4),

$$\mu \|\boldsymbol{x}_n\| \geqslant |\ell(\boldsymbol{x}_n)| = \ell(\boldsymbol{x}_n) \geqslant \tfrac{n-1}{n}\mu.$$

Dividing by $\mu > 0$ and recalling that $1 \geqslant \|\boldsymbol{x}_n\|$ we see that $\|\boldsymbol{x}_n\| \to 1$ as $n \to \infty$. (This makes sense. If a nonzero linear functional is going to achieve a maximum over the unit ball, it should happen on the boundary.)

Similarly we have

$$\mu \|\boldsymbol{x}_n + \boldsymbol{x}_m\| \geqslant |\ell(\boldsymbol{x}_n + \boldsymbol{x}_m)| = \ell(\boldsymbol{x}_n) + \ell(\boldsymbol{x}_m) \geqslant \left(\tfrac{n-1}{n} + \tfrac{m-1}{m}\right)\mu.$$

Dividing by $\mu > 0$ gives

$$\|\boldsymbol{x}_n + \boldsymbol{x}_m\| \geqslant \tfrac{n-1}{n} + \tfrac{m-1}{m}.$$

Square both sides and substitute in (5) to get

$$\|\boldsymbol{x}_n - \boldsymbol{x}_m\|^2 \leqslant 2\|\boldsymbol{x}_n\|^2 + 2\|\boldsymbol{x}_m\|^2 - \left(\tfrac{n-1}{n} + \tfrac{m-1}{m}\right)^2.$$

Since $\|\boldsymbol{x}_n\|, \|\boldsymbol{x}_m\| \to 1$, the right-hand side tends to $2 + 2 - (1+1)^2 = 0$ as $n, m \to \infty$, so the sequence is indeed a Cauchy sequence.

Thus there is a limit point $\boldsymbol{x} \in U$, with $\|\boldsymbol{x}\| = 1$, and which by continuity satisfies

$$\ell(\boldsymbol{x}) = \mu = \max_{\boldsymbol{x} \in U} \ell(\boldsymbol{x}).$$

To see that the maximizer is unique, suppose $\ell(\boldsymbol{x}) = \ell(\boldsymbol{y}) = \mu > 0$. (Note that this rules out $\boldsymbol{y} = -\boldsymbol{x}$.) Then by the Cauchy–Schwartz Inequality $\|(\boldsymbol{x}+\boldsymbol{y})/2\| < 1$ (unless $\boldsymbol{y}$ and $\boldsymbol{x}$ are dependent, which in this case means $\boldsymbol{y} = \boldsymbol{x}$), so $\ell\big((\boldsymbol{x}+\boldsymbol{y})/\|(x+y)\|\big) > \mu$, a contradiction. ∎

48 Theorem *Let V be a Hilbert space. For every continuous linear functional ℓ on V, there is a vector $\boldsymbol{y}$ in V such that for every $\boldsymbol{x} \in V$,*

$$\ell(\boldsymbol{x}) = (\boldsymbol{y}, \boldsymbol{x}).$$

The correspondence $\ell \leftrightarrow \boldsymbol{y}$ is a homomorphism between V^* and V.

Proof: (Cf. Murray [19, p. 13]) If ℓ is the zero functional, let $\boldsymbol{y} = 0$. Otherwise, let $\hat{\boldsymbol{y}}$ be the unique maximizer of ℓ over the unit ball (so $\|\hat{\boldsymbol{y}}\| = 1$), and let $\mu = \ell(\hat{\boldsymbol{y}})$. Set

$$\boldsymbol{y} = \mu\hat{\boldsymbol{y}}.$$

Then

$$(\boldsymbol{y}, \hat{\boldsymbol{y}}) = (\mu\hat{\boldsymbol{y}}, \hat{\boldsymbol{y}}) = \mu(\hat{\boldsymbol{y}}, \hat{\boldsymbol{y}}) = \mu = \ell(\hat{\boldsymbol{y}}),$$

so we are off to a good start. We need to show that for every $\boldsymbol{x}$, we have $(\boldsymbol{y}, \boldsymbol{x}) = \ell(\boldsymbol{x})$.

We start by showing that if $\ell(\boldsymbol{x}) = 0$, then $(\boldsymbol{y}, \boldsymbol{x}) = 0$. So assume that $\ell(x) = 0$. Then $\ell(\hat{\boldsymbol{y}} \pm \lambda\boldsymbol{x}) = \ell(\hat{\boldsymbol{y}}) = \mu$ for every λ. But by (3) above,

$$\mu = \ell(\hat{\boldsymbol{y}} \pm \lambda\boldsymbol{x}) \leqslant \mu\|\hat{\boldsymbol{y}} \pm \lambda\boldsymbol{x}\|,$$

so

$$\|\hat{\boldsymbol{y}} \pm \lambda\boldsymbol{x}\| \geqslant 1 = \|\hat{\boldsymbol{y}}\|.$$

Squaring both sides gives

$$\|\hat{\boldsymbol{y}}\|^2 \pm 2\lambda(\hat{\boldsymbol{y}}, \boldsymbol{x}) + \lambda^2\|\boldsymbol{x}\|^2 \geqslant \|\hat{\boldsymbol{y}}\|^2$$

or

$$\lambda\|\boldsymbol{x}\|^2 \geqslant \mp 2(\hat{\boldsymbol{y}}, \boldsymbol{x})$$

for all $\lambda > 0$. Letting $\lambda \to 0$ implies $(\hat{\boldsymbol{y}}, \boldsymbol{x}) = 0$, so $(\boldsymbol{y}, \boldsymbol{x}) = 0$.

For an arbitrary $\boldsymbol{x}$, let

$$\boldsymbol{x}' = \boldsymbol{x} - \ell(\boldsymbol{x})(\hat{\boldsymbol{y}}/\mu).$$

Then

$$\ell(\boldsymbol{x}') = \ell(\boldsymbol{x}) - \ell(\boldsymbol{x})\ell(\hat{\boldsymbol{y}}/\mu) = 0.$$

So $(\boldsymbol{y}, \boldsymbol{x}') = 0$. Now observe that

$$\begin{aligned}
(\boldsymbol{y}, \boldsymbol{x}) &= (\boldsymbol{y}, \boldsymbol{x}' + \ell(\boldsymbol{x})(\hat{\boldsymbol{y}}/\mu)) \\
&= (\boldsymbol{y}, \boldsymbol{x}') + \ell(\boldsymbol{x})(\boldsymbol{y}, \hat{\boldsymbol{y}}/\mu) \\
&= 0 + \ell(\boldsymbol{x})(\mu\hat{\boldsymbol{y}}, \hat{\boldsymbol{y}}/\mu) \\
&= \ell(\boldsymbol{x}).
\end{aligned}$$

This completes the proof. ∎

7 ⋆ Linear functionals on infinite dimensional spaces

If ℓ is a linear functional on the finite dimensional vector space $\boldsymbol{R}^{\mathrm{m}}$, then by Theorem 48, there is a vector $\boldsymbol{y} = (y_1, \dots, y_m)$ such that for any $\boldsymbol{x} = (x_1, \dots, x_m)$ we have

$$\ell(\boldsymbol{x}) = \sum_{i=1}^{n} y_i x_i,$$

so that ℓ is a continuous function. However, for infinite dimensional normed spaces there are always linear functionals that are discontinuous! Lots of them in fact.

49 Proposition *Every infinite dimensional normed space has a discontinuous linear functional.*

Proof: If X is an infinite dimensional normed space, then it has an infinite Hamel basis B. We may normalize each basis vector to have norm one. Let $S = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \dots\}$ be a countable subset of the basis B. Define the function ℓ on the basis B by $\ell(\boldsymbol{x}_n) = n$ for $\boldsymbol{x}_n \in S$, and $\ell(\boldsymbol{v}) = 0$ for $\boldsymbol{v} \in B \setminus S$. Every $\boldsymbol{x} \in X$ has a unique representation as

$$\boldsymbol{x} = \sum_{\boldsymbol{v} \in B} \alpha_v \boldsymbol{v},$$

where only finitely many α_v are nonzero. Extend ℓ from B to X by

$$\ell(\boldsymbol{x}) = \sum_{\boldsymbol{v} \in B} \alpha_v \ell(\boldsymbol{v}).$$

Then ℓ is a linear functional, but it is not bounded on the unit ball (as $\ell(\boldsymbol{x}_n) = n$). The same argument used in the proof of Theorem 47 shows that in order for ℓ to be continuous, it must be bounded on the unit ball, so it is not continuous. ∎

8 Linear transformations

Recall (Definition 11) that a linear transformation is a function $T\colon V \to W$ between vector spaces satisfying

$$T(\alpha \boldsymbol{x} + \beta \boldsymbol{y}) = \alpha T\boldsymbol{x} + \beta T\boldsymbol{y}.$$

There are three special classes of linear transformations from a space into itself.

- The first is just a rescaling along various dimensions. The identity function is of this class, where the scale factor is one in each dimension. These transformations are symmetric, see Definition 70 and Theorem 78 below.
- Another important class is orthogonal projection onto a linear subspace, see Proposition 43.
- And another important class is rotation about an axis. Rotations are a kind of orthogonal transformation, see Definition 67 below.

These classes do not include all the linear transformation, since, for instance, the composition of two of these kinds of transformations need not belong to any of these groups.

50 Definition *For a linear transformation $T\colon V \to W$, the **null space** or **kernel** of T is the inverse image of 0, that is, $\{\boldsymbol{x} \in V : T\boldsymbol{x} = 0\}$.*

51 Proposition *The null space of T, $\{\boldsymbol{x} : T\boldsymbol{x} = 0\}$, is a linear subspace of V, and the range of T, $\{T\boldsymbol{x} : \boldsymbol{x} \in V\}$, is a linear subspace of W.*

52 Proposition *A linear transformation T is one-to-one if and only if its null space is $\{\mathbf{0}\}$. In other words, T is one-to-one if and only if $T\boldsymbol{x} = \mathbf{0}$ implies $\boldsymbol{x} = \mathbf{0}$.*

The dimension of the range of T is called the **rank** of T. The dimension of the null space of T is called the **nullity** of T. The next result may be found in [6, Theorem 2.3, p. 34]. You can prove it using Corollary 41 applied to the null space of T.

53 Nullity Plus Rank Theorem *Let $T\colon V \to W$, where V and W are finite-dimensional inner product spaces. Then*

$$\operatorname{rank} T + \operatorname{nullity} T = \dim V.$$

Proof: Let N denote the null space of T. For $\boldsymbol{x}$ in V, decompose it orthogonally as $\boldsymbol{x} = \boldsymbol{x}_N + \boldsymbol{x}_\perp$, where $\boldsymbol{x}_N \in N$ and $\boldsymbol{x}_\perp \in N_\perp$. Then $T\boldsymbol{x} = T\boldsymbol{x}_\perp$, so the range of T is just $T(N_\perp)$. Now let $'x_1, \dots, 'x_k$ be a basis for $N_\perp$. I claim that $T\boldsymbol{x}_1, \dots, T\boldsymbol{x}_k$ are independent and therefore constitute a basis for the range of T. For suppose some linear combination $\sum_{i=1}^k \alpha_i T\boldsymbol{x}_i$ is zero. By linearity of T we have $T\left(\sum_{i=1}^k \alpha_i \boldsymbol{x}_i\right) = \mathbf{0}$. Which implies $\sum_{i=1}^k \alpha_i \boldsymbol{x}_i$ belongs to the null space N. But this combination also lies in $N_\perp$, so it must be zero. But since the $\boldsymbol{x}_i$'s are independent, it follows that $\alpha_1 = \cdots = \alpha_k = 0$. ∎

54 Corollary *Let $T\colon V \to W$ be a linear transformation between m-dimensional spaces. Then T is one-to-one if and only if T is onto.*

Proof: ($\Longrightarrow$) Assume T is one-to-one. If $T\boldsymbol{x} = \mathbf{0} = T\mathbf{0}$, $\boldsymbol{x} = \mathbf{0}$ by one-to-oneness. In other words, the null space of T is just $\{\mathbf{0}\}$. Then by the Nullity Plus Rank Theorem 53 the rank of T is m, but this mean the image under T of V is all of W.

($\Longleftarrow$) Assume T maps V onto W. Then the rank of T is m, so by the Nullity Plus Rank Theorem 53 its null space of T contains only 0. Suppose $T\boldsymbol{x} = T\boldsymbol{y}$. Then $T(\boldsymbol{x} - \boldsymbol{y}) = \mathbf{0}$, so $\boldsymbol{x} - \boldsymbol{y} = \mathbf{0}$, which implies T is one-to-one. ∎

8.1 Inverse of a linear transformation

Let $T\colon V \to W$ be a linear transformation between two vector spaces. A **left inverse** for T is a function $L\colon \operatorname{range} T \to V$ such that for all $\boldsymbol{x} \in V$, we have $LT\boldsymbol{x} = \boldsymbol{x}$. Observe that this implies that $\operatorname{range} L = V$. It also implies that T must be one-to-one. For suppose $T\boldsymbol{x} = T\boldsymbol{y}$. Then $\boldsymbol{x} = LT\boldsymbol{x} = LT\boldsymbol{y} = \boldsymbol{y}$. A **right inverse** for T is a function $R\colon \operatorname{range} T \to V$ such that for all $\boldsymbol{y} \in \operatorname{range} T$, we have $TR\boldsymbol{y} = \boldsymbol{y}$.

55 Lemma (Left vs. right inverses) *Let $T\colon V \to W$ be a linear transformation. If T has a left inverse, then it is unique, and also a right inverse.*

Proof: (Cf. Apostol [6, Theorem 2.8, pp. 39–40].) Let L and M be left inverses for T. Let $\boldsymbol{y} \in \operatorname{range} T$, say $\boldsymbol{y} = T\boldsymbol{x}$. Then

$$L\boldsymbol{y} = LT\boldsymbol{x} = \boldsymbol{x} = MT\boldsymbol{x} = M\boldsymbol{y}.$$

That is $L = M$ on $\operatorname{range} T$.

Now we show that L is also a right inverse. Let

$$\boldsymbol{y} = T\boldsymbol{x}$$

belong to $\operatorname{range} T$. Then applying TL to both sides gives

$$TL\boldsymbol{y} = TLT\boldsymbol{x} = T(LT)\boldsymbol{x} = T\boldsymbol{x} = \boldsymbol{y}.$$

That is, L is a right inverse. ∎

Is it the case that if T has a right inverse, then it also has left inverse? The answer is no. Here is an example.

56 Example (A right inverse need not be a left inverse) Define $T\colon \boldsymbol{R}^2 \to \boldsymbol{R}^2$ via

$$T(x, y) = (x, 0).$$

(That is, T is the projection onto the x-axis.) Define $R\colon \operatorname{range} T \to \boldsymbol{R}^2$ via

$$R(x, 0) = (x, 0).$$

Then

$$TR(x, 0) = T(x, 0) = (x, 0),$$

so R is a right inverse of T. But it is clear that T has no left inverse since T is not one-to-one. □

57 Proposition *Let $T: V \to W$ be linear, one-to-one, and onto, where V and W are finite-dimensional vector spaces. Then $\dim V = \dim W$, and T^{-1} is linear.*

Proof: First we show that T^{-1} is linear: Let $\boldsymbol{x}_i = T^{-1}(\boldsymbol{u}_i)$, $i = 1, 2$. Now

$$T(\alpha \boldsymbol{x}_1 + \beta \boldsymbol{x}_2) = \alpha T \boldsymbol{x}_1 + \beta T \boldsymbol{x}_2 = \alpha \boldsymbol{u}_1 + \beta \boldsymbol{u}_2.$$

So taking T^{-1} of both sides gives

$$\alpha \underbrace{T^{-1}(\boldsymbol{u}_1)}_{\boldsymbol{x}_1} + \beta \underbrace{T^{-1}(\boldsymbol{u}_2)}_{\boldsymbol{x}_2} = T^{-1}(\alpha \boldsymbol{u}_1 + \beta \boldsymbol{u}_2)$$

Next we show that $\dim W \leqslant \dim V$: Let $\boldsymbol{y}_1, \dots, \boldsymbol{y}_n$ be a basis for V. Then $T\boldsymbol{y}_1, \dots, T\boldsymbol{y}_n$ span W since T is linear and onto. Therefore $\dim W \leqslant n = \dim V$.

On the other hand, $T\boldsymbol{y}_1, \dots, T\boldsymbol{y}_n$ are linearly independent, so $\dim W \geqslant \dim V$. To see this, suppose

$$\mathbf{0} = \sum_{i=1}^{n} \alpha_i T \boldsymbol{y}_i = T\left(\sum_{i=1}^{n} \alpha_i \boldsymbol{y}_i\right)$$

But T is one-to-one and $T\mathbf{0} = \mathbf{0}$, so $\sum_{i=1}^{n} \alpha_i \boldsymbol{y}_i = \mathbf{0}$. But this implies $\alpha_1 = \cdots = \alpha_n = 0$.

This shows that $\dim V = \dim W$. ∎

8.2 Adjoint of a transformation

58 Definition *Let $T: V \to W$ be linear where V and W are Hilbert spaces. The* ***transpose****, or* ***adjoint****,[4] of T, denoted T', is the linear transformation $T': W \to V$ such that for every $\boldsymbol{x}$ in V and every $\boldsymbol{y}$ in W.*

$$(T'\boldsymbol{y}, \boldsymbol{x}) = (\boldsymbol{y}, T\boldsymbol{x}). \tag{6}$$

The first question is, does such a linear transformation T' exist?

59 Proposition *The adjoint of T exists, and is uniquely determined by (6).*

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[dr, "\ell_{T'\boldsymbol{y}}"'] & W \arrow[d, "\ell_y"] \\ & \boldsymbol{R} \end{tikzcd}$$

Proof: By bilinearity of the inner product (Proposition 21) on W, for each $\boldsymbol{y} \in W$, the mapping $\ell_y: \boldsymbol{z} \mapsto (\boldsymbol{y}, \boldsymbol{z})$ from W to $\boldsymbol{R}$ is linear, so the composition $\ell_y \circ T: V \to \boldsymbol{R}$ is linear. By Theorem 48 on the representation of linear functionals on Hilbert spaces, there is a unique vector, call it $T'\boldsymbol{y}$, in V so that $(\boldsymbol{y}, T\boldsymbol{x}) = (\ell_y \circ T)(\boldsymbol{x}) = (T'\boldsymbol{y}, \boldsymbol{x})$, holds for each $\boldsymbol{x} \in V$. The correspondence $\boldsymbol{y} \mapsto T'\boldsymbol{y}$ defines the transformation $T': W \to V$.

Let $\boldsymbol{y}$ and $\boldsymbol{z}$ belong to W. Then again by bilinearity,

$$\ell_{\alpha y + \beta z} \circ T = \alpha \ell_y \circ T + \beta \ell_z \circ T.$$

That is, the mapping T' is linear.

Finally, Lemma 22 implies that $T'\boldsymbol{y}$ is uniquely determined by (6). ∎

Elaborate this.

60 Proposition *Let $S, T \colon V \to W$ and $U \colon W \to X$. Then*

$$(UT)' = T'U'$$

$$(\alpha S + \beta T)' = \alpha S' + \beta T'$$

$$(T')' = T$$

61 Theorem *Let $T \colon V \to W$, where V and W are inner product spaces, so $T' \colon W \to V$. Then $T'\boldsymbol{y} = \boldsymbol{0}$ iff $\boldsymbol{y} \perp \operatorname{range} T$. In other words,*

$$\text{null space}\, T' = (\operatorname{range} T)_\perp.$$

Proof: ($\Longrightarrow$) If $T'\boldsymbol{y} = \boldsymbol{0}$, then $(T'\boldsymbol{y}, \boldsymbol{x}) = (\boldsymbol{0}, \boldsymbol{x}) = 0$ for all $\boldsymbol{x}$ in V. But $(T'\boldsymbol{y}, \boldsymbol{x}) = (\boldsymbol{y}, T\boldsymbol{x})$, so $(\boldsymbol{y}, T\boldsymbol{x}) = 0$ for all $\boldsymbol{x}$ in V. That is, $\boldsymbol{y} \perp \operatorname{range} T$.

($\Longleftarrow$) If $\boldsymbol{y} \perp \operatorname{range} T$, then $(\boldsymbol{y}, T\boldsymbol{x}) = 0$ for all $\boldsymbol{x}$ in V. Therefore $(T'\boldsymbol{y}, \boldsymbol{x}) = 0$ for all $\boldsymbol{x}$ in V, so $T'\boldsymbol{y} = \boldsymbol{0}$. ∎

62 Corollary *Let $T \colon V \to W$, where V and W are inner product spaces. Then $\operatorname{range} T'T = \operatorname{range} T'$. Consequently, $\operatorname{rank} T' = \operatorname{rank} T'T$.*

Proof: Clearly $\operatorname{range} T'T \subset \operatorname{range} T'$.

Let $\boldsymbol{x}$ belong to the range of T', so $\boldsymbol{x} = T'\boldsymbol{y}$ for some $\boldsymbol{y}$ in W. Let M denote the range of T and consider the orthogonal decomposition $\boldsymbol{y} = \boldsymbol{y}_M + \boldsymbol{y}_\perp$. Then $T'\boldsymbol{y} = T'\boldsymbol{y}_M + T'\boldsymbol{y}_\perp$, but $T'\boldsymbol{y}_\perp = 0$ by Theorem 61. Now $\boldsymbol{y}_M = T\boldsymbol{z}$ some $\boldsymbol{z} \in W$. Then $\boldsymbol{x} = T'T\boldsymbol{z}$, so $\boldsymbol{x}$ belongs to the range of $T'T$. ∎

63 Corollary *Let $T \colon V \to W$, where V and W are finite-dimensional inner product spaces. Then $\operatorname{rank} T' = \operatorname{rank} T$*

Proof: By Theorem 61, $\text{null space}\, T' = (\operatorname{range} T)_\perp \subset W$. Therefore

$$\dim W - \operatorname{rank} T' = \operatorname{nullity} T' = \dim(\operatorname{range} T)_\perp = \dim W - \operatorname{rank} T,$$

where the first equality follows from the Nullity Plus Rank Theorem 53, the second from Theorem 61, and the third from Corollary 41. Therefore, $\operatorname{rank} T = \operatorname{rank} T'$. ∎

64 Corollary *Let $T \colon \boldsymbol{R}^{\mathrm{n}} \to \boldsymbol{R}^{\mathrm{m}}$. Then $\text{null space}\, T = \text{null space}\, T'T$.*

Proof: Clearly $\text{null space}\, T \subset \text{null space}\, T'T$, since $T\boldsymbol{x} = \boldsymbol{0} \implies T'T\boldsymbol{x} = T'\boldsymbol{0} = \boldsymbol{0}$.

Now suppose $T'T\boldsymbol{x} = \boldsymbol{0}$. Then $(\boldsymbol{x}, T'T\boldsymbol{x}) = (\boldsymbol{x}, \boldsymbol{0}) = 0$. But

$$(\boldsymbol{x}, T'T\boldsymbol{x}) = (T'T\boldsymbol{x}, \boldsymbol{x}) = (T\boldsymbol{x}, T\boldsymbol{x}),$$

where the first equality is IP.1 and the second is the definition of T', so $T\boldsymbol{x} = \boldsymbol{0}$. ∎

[4] When dealing with complex vector spaces, the definition of the adjoint is modified to $(\boldsymbol{y}, T\boldsymbol{x}) = \overline{(T'\boldsymbol{y}, \boldsymbol{x})}$.

We can even get a version of the Fredholm Alternative 45 as a corollary. I leave it to you to unravel why I think this a version of the Fredholm Alternative.

65 Corollary (Fredholm Alternative II) *Let $T \colon V \to W$, where V and W are inner product spaces, and let $\boldsymbol{z}$ belong to W. Then either*

$$\text{there exists } \boldsymbol{x} \in V \text{ with } \boldsymbol{z} = T\boldsymbol{x},$$

or else

$$\text{there exists } \boldsymbol{y} \in W \text{ with } (\boldsymbol{y}, \boldsymbol{z}) \neq 0 \ \&\ T'\boldsymbol{y} = \boldsymbol{0}.$$

Proof: The first alternative states that $\boldsymbol{z} \in \operatorname{range} T$, or equivalently (by Theorem 61), that $\boldsymbol{z} \in (\text{null space}\, T')_{\perp}$. If this is not the case, that is, if $\boldsymbol{z} \notin (\text{null space}\, T')_{\perp}$, then there must be some $\boldsymbol{y}$ in null space T' that is not orthogonal to $\boldsymbol{z}$. Such a $\boldsymbol{y}$ satisfies $T'\boldsymbol{y} = 0$ and $(\boldsymbol{y}, \boldsymbol{z}) \neq 0$, which is the second alternative.

To see that the two alternatives are inconsistent, suppose that $\boldsymbol{x}$ and $\boldsymbol{y}$ satisfy the alternatives. Then $0 \neq (\boldsymbol{y}, \boldsymbol{z}) = (\boldsymbol{y}, T\boldsymbol{x}) = (T'\boldsymbol{y}, \boldsymbol{x}) = (\boldsymbol{0}, \boldsymbol{x}) = 0$, a contradiction. (The middle equality is just the definition of the transpose.) ∎

66 Proposition (Summary) *For a linear transformation T between finite-dimensional spaces, $\operatorname{range} T'T = \operatorname{range} T'$ and $\operatorname{range} TT' = \operatorname{range} T$, so*

$$\operatorname{rank} T = \operatorname{rank} T' = \operatorname{rank} T'T = \operatorname{rank} TT'.$$

8.3 Orthogonal transformations

67 Definition *Let V be a real inner product space, and let $T \colon V \to V$ be a linear transformation of V into itself. We say that T is an **orthogonal transformation** if its adjoint is its inverse,*

$$T' = T^{-1}.$$

68 Proposition *For a linear transformation $T \colon V \to V$ on an inner product space, the following are equivalent.*

1. *T is orthogonal. That is, $T' = T^{-1}$.*
2. *T preserves norms. That is, for all x,*
$$(T\boldsymbol{x}, T\boldsymbol{x}) = (\boldsymbol{x}, \boldsymbol{x}). \tag{7}$$
3. *T preserves inner products, that is, for every $\boldsymbol{x}, \boldsymbol{y} \in V$,*
$$(T\boldsymbol{x}, T\boldsymbol{y}) = (\boldsymbol{x}, \boldsymbol{y}).$$

Proof: (1) $\implies$ (2) Assume T is orthogonal. Fix $\boldsymbol{x}$ and let $\boldsymbol{y} = T\boldsymbol{x}$. By the definition of T' we have

$$(T'\boldsymbol{y}, \boldsymbol{x}) = (\boldsymbol{y}, T\boldsymbol{x}),$$

so

$$(\boldsymbol{x}, \boldsymbol{x}) = (T'T\boldsymbol{x}, \boldsymbol{x}) = (T'\boldsymbol{y}, \boldsymbol{x}) = (\boldsymbol{y}, T\boldsymbol{x}) = (T\boldsymbol{x}, T\boldsymbol{x}).$$

(2) $\implies$ (3) Assume T preserves norms. By Proposition 27,

$$\begin{aligned}(T\boldsymbol{x}, T\boldsymbol{y}) &= \frac{\|T\boldsymbol{x} + T\boldsymbol{y}\| - \|T\boldsymbol{x} - T\boldsymbol{y}\|}{4} \\ &= \frac{\|T(\boldsymbol{x} + \boldsymbol{y})\| - \|T(\boldsymbol{x} - \boldsymbol{y})\|}{4} \\ &= \frac{\|\boldsymbol{x} + \boldsymbol{y}\| - \|\boldsymbol{x} - \boldsymbol{y}\|}{4} \\ &= (\boldsymbol{x}, \boldsymbol{y}).\end{aligned}$$

(3) $\implies$ (1) Assume T preserves inner products. By the definition of T', for all $\boldsymbol{x}, \boldsymbol{y}$,

$$(T'\boldsymbol{y}, x) = (\boldsymbol{y}, T\boldsymbol{x}).$$

Taking $\boldsymbol{y} = T\boldsymbol{z}$, we have

$$(T'T\boldsymbol{z}, \boldsymbol{x}) = (T'\boldsymbol{y}, \boldsymbol{x}) = (\boldsymbol{y}, T\boldsymbol{x}) = (T\boldsymbol{z}, T\boldsymbol{x}) = (\boldsymbol{z}, \boldsymbol{x}),$$

so by Lemma 22, $T'T\boldsymbol{z} - \boldsymbol{z} = 0$ for every $\boldsymbol{z}$, which is equivalent to $T' = T^{-1}$. ∎

A norm preserving mapping is also called an **isometry**. Since the composition of norm-preserving mappings preserves norms we have the following.

69 Corollary *The composition of orthogonal transformations is an orthogonal transformation.*

An orthogonal transformation preserves angles (since it preserves inner products) and distances between vectors. Reflection and rotation are the basic orthogonal transformations in a finite-dimensional Euclidean space.

8.4 Symmetric transformations

70 Definition *A transformation $T\colon V \to V$ is* ***symmetric*** *or* ***self-adjoint*** *if $T' = T$. A transformation T is* ***skew-symmetric*** *if $T' = -T$.*

71 Proposition *Let $\pi_M\colon V \to V$ be the orthogonal projection onto the linear subspace M. Then π_M is symmetric.*

Proof: To show $(\boldsymbol{x}, \pi_M\boldsymbol{z}) = (\pi_M\boldsymbol{x}, \boldsymbol{z})$. Observe that

$$(\boldsymbol{x}, \boldsymbol{z}_M) = (\boldsymbol{x}_M + \boldsymbol{x}_\perp, \boldsymbol{z}_M) = (\boldsymbol{x}_M, \boldsymbol{z}_M) + (\boldsymbol{x}_\perp, \boldsymbol{z}_M) = (\boldsymbol{x}_M, \boldsymbol{z}_M) + 0.$$

Similarly,

$$(\boldsymbol{x}_M, \boldsymbol{z}) = (\boldsymbol{x}_M, \boldsymbol{z}_M + \boldsymbol{z}_\perp) = (\boldsymbol{x}_M, \boldsymbol{z}_M) + (\boldsymbol{x}_M, \boldsymbol{z}_\perp) = (\boldsymbol{x}_M, \boldsymbol{z}_M) + 0.$$

Therefore $(\boldsymbol{x}, \boldsymbol{z}_M) = (\boldsymbol{x}_M, \boldsymbol{z}) = (\boldsymbol{x}_M, \boldsymbol{z}_M)$. ∎

In light of the following exercise, a linear transformation is an orthogonal projection if and only if it is symmetric and idempotent. A transformation T is **idempotent** if $T^2\boldsymbol{x} = TT\boldsymbol{x} = T\boldsymbol{x}$ for all $\boldsymbol{x}$.

72 Exercise Let V be an inner product space, and let $P\colon V \to V$ be a linear transformation satisfying

$$P' = P \quad \text{and} \quad P^2\boldsymbol{x} = P\boldsymbol{x} \text{ for all } \boldsymbol{x} \in \boldsymbol{R}^{\mathrm{m}}.$$

That is, P is idempotent and symmetric. Set $M = I - P$ (where I is the identity on V). Prove the following.

1. For any $\boldsymbol{x}$, $\boldsymbol{x} = M\boldsymbol{x} + P\boldsymbol{x}$.
2. $M^2\boldsymbol{x} = M\boldsymbol{x}$ for all $\boldsymbol{x}$ and $M' = M$.
3. null space $P = (\operatorname{range} P)_\perp = \operatorname{range} M$ and null space $M = (\operatorname{range} M)_\perp = \operatorname{range} P$
4. P is the orthogonal projection onto its range. Likewise for M.

□

9 Eigenvalues and eigenvectors

73 Definition *Let V be a real vector space, and let T be a linear transformation of V into itself, $T\colon V \to V$. A real number λ is an* ***eigenvalue*** *of T if there is a nonzero vector $\boldsymbol{x}$ in V such that $T\boldsymbol{x} = \lambda\boldsymbol{x}$. The vector $\boldsymbol{x}$ is called an* ***eigenvector*** *of T associated with λ. Note that the vector $\mathbf{0}$ is by definition* not *an eigenvector of T.*[5]

If T has an eigenvalue λ with eigenvector $\boldsymbol{x}$, the transformation "stretches" the space by a factor λ in the direction $\boldsymbol{x}$.

While the vector $\mathbf{0}$ is never an eigenvector, the scalar 0 may be an eigenvalue. Indeed 0 is the eigenvalue associated with any nonzero vector in the null space of T.

There are linear transformations with no (real) eigenvalues. For instance, consider the rotation of $\boldsymbol{R}^2$ by ninety degrees. This is given by the transformation $(\boldsymbol{x}, y) \mapsto (-y, \boldsymbol{x})$. In order to satisfy $T\boldsymbol{x} = \lambda\boldsymbol{x}$ we must have $\lambda\boldsymbol{x} = -y$ and $\lambda y = \boldsymbol{x}$. This cannot happen for any nonzero real vector $(\boldsymbol{x}, y)$ and real λ.

On the other hand, the identity transformation has an eigenvalue 1, associated with every nonzero vector.

Observe that there is a unique eigenvalue associated with each eigenvector: If $T\boldsymbol{x} = \lambda\boldsymbol{x}$ and $T\boldsymbol{x} = \alpha\boldsymbol{x}$, then $\alpha\boldsymbol{x} = \lambda\boldsymbol{x}$, so $\alpha = \lambda$, since by definition $\boldsymbol{x}$ is nonzero.

On the other hand, one eigenvalue must be associated with many eigenvectors, for if $\boldsymbol{x}$ is an eigenvector associated with λ, so is any nonzero scalar multiple of $\boldsymbol{x}$. More generally, a linear combination of eigenvectors corresponding to an eigenvalue is also an eigenvector corresponding to the same eigenvalue (provided the linear combination does not equal the zero vector). The span of the set of eigenvectors associated with the eigenvalue λ is called the **eigenspace** of T

[5]For a linear transformation of a complex vector space, eigenvalues may be complex, but I shall only deal with real vector spaces here.

corresponding to λ. Every nonzero vector in the eigenspace is an eigenvector associated with λ. The dimension of the eigenspace is called the **multiplicity** of λ.

74 Proposition *If $T\colon V \to V$ is idempotent, then each of its eigenvalues is either 0 or 1.*

Proof: Suppose $T\boldsymbol{x} = \lambda \boldsymbol{x}$ with $\boldsymbol{x} \neq \boldsymbol{0}$. Since T is idempotent, we have $\lambda \boldsymbol{x} = T\boldsymbol{x} = T^2\boldsymbol{x} = \lambda^2\boldsymbol{x}$. Since $\boldsymbol{x} \neq \boldsymbol{0}$, this implies $\lambda = \lambda^2$, so $\lambda = 0$ or $\lambda = 1$. ∎

For distinct eigenvalues we have the following, taken from [6, Theorem 4.1, p. 100].

75 Theorem *Let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ be eigenvectors associated with distinct eigenvalues $\lambda_1, \ldots, \lambda_n$. Then the vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ are independent.*

Proof: The proof is by induction n. The case $n = 1$ is trivial, since by definition eigenvectors are nonzero. Now consider $n > 1$ and suppose that the result is true for $n - 1$. Now let

$$\sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i = \boldsymbol{0}. \tag{8}$$

Applying the transformation T to both sides gives

$$\sum_{i=1}^{n} \alpha_i \lambda_i \boldsymbol{x}_i = \boldsymbol{0}. \tag{9}$$

Let us eliminate $\boldsymbol{x}_n$ from (9) by multiplying (8) by λ_n and subtracting to get

$$\sum_{i=1}^{n} \alpha_i(\lambda_i - \lambda_n)\boldsymbol{x}_i = \sum_{i=1}^{n-1} \alpha_i(\lambda_i - \lambda_n)\boldsymbol{x}_i = \boldsymbol{0}.$$

But $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-1}$ are linearly independent, so by the induction hypothesis $\alpha_i(\lambda_i - \lambda_n) = 0$ for each $i = 1, \ldots, n-1$. Since the eigenvalues are distinct, this implies each $\alpha_i = 0$, $i = 1, \ldots, n-1$. So (8) reduces to $\alpha_n \boldsymbol{x}_n = \boldsymbol{0}$, which implies $\alpha_n = 0$. Thus $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ are independent. ∎

76 Corollary *A linear transformation on an n-dimensional space has at most n distinct eigenvalues. If it has n, then the space has a basis made up of eigenvectors.*

When T is a symmetric transformation of an inner product space into itself, not only are eigenvectors associated with distinct eigenvalues independent, they are orthogonal.

77 Proposition *Let V be a real inner product space, and let T be a symmetric linear transformation of V into itself. Let $\boldsymbol{x}$ and y be eigenvectors of T corresponding to eigenvalues α and λ with $\alpha \neq \lambda$. Then $\boldsymbol{x} \perp y$.*

Proof: We are given $T\boldsymbol{x} = \alpha\boldsymbol{x}$ and $T\boldsymbol{y} = \lambda y$. Thus $(T\boldsymbol{x}, y) = (\lambda\boldsymbol{x}, y) = \lambda(\boldsymbol{x}, y)$ and $(\boldsymbol{x}, T\boldsymbol{y}) = (\boldsymbol{x}, \alpha y) = \alpha(\boldsymbol{x}, y)$. Since T is symmetric, $(T\boldsymbol{x}, y) = (\boldsymbol{x}, T\boldsymbol{y})$, so $\alpha(\boldsymbol{x}, y) = \lambda(\boldsymbol{x}, y)$. Since $\lambda \neq \alpha$ we must then have $(\boldsymbol{x}, y) = 0$. ∎

Also if T is symmetric, we are guaranteed that it has plenty of eigenvectors.

78 Theorem *Let $T : V \to V$ be symmetric, where V is an n-dimensional inner product space. Then V has an orthonormal basis consisting of eigenvectors of T.*

Proof: This proof uses some well known results from topology and calculus that are beyond the scope of these notes. Cf. Anderson [4, pp. 273–275], Carathéodory [10, § 195], Franklin [12, Section 6.2, pp. 141–145], Rao [20, 1f.2.iii, p. 62].

Let $S = \{\boldsymbol{x} \in V : (\boldsymbol{x}, \boldsymbol{x}) = 1\}$ denote the unit sphere in V. Set $M_0 = \{\boldsymbol{0}\}$ and define $S_0 = S \cap M_{0\perp}$. Define the *quadratic form* $Q : V \to \boldsymbol{R}$ by

$$Q(\boldsymbol{x}) = (\boldsymbol{x}, T\boldsymbol{x}).$$

It is easy to see that Q is continuous, so it has a maximizer on S_0, which is compact. (This maximizer cannot be unique, since $Q(-\boldsymbol{x}) = Q(\boldsymbol{x})$, and indeed if T is the identity, then Q is constant on S.) Fix a maximizer $\boldsymbol{x}_1$ of Q over S_0.

Proceed recursively for $k = 1, \dots, n-1$. Let M_k denote the span of $\boldsymbol{x}_1, \dots, \boldsymbol{x}_k$, and set $S_k = S \cap M_{k\perp}$. Let $\boldsymbol{x}_{k+1}$ maximize Q over S_k. By construction, $\boldsymbol{x}_{k+1} \in M_{k\perp}$, so the $\boldsymbol{x}_k$'s are orthogonal, indeed orthonormal.

Since $\boldsymbol{x}_1$ maximizes Q on $S = S_0$, it maximizes Q subject to the constraint $1 - (\boldsymbol{x}, \boldsymbol{x}) = 0$. Now $Q(\boldsymbol{x}) = (\boldsymbol{x}, T\boldsymbol{x})$ is continuously differentiable and $Q'(\boldsymbol{x}) = 2T\boldsymbol{x}$, and the gradient of the constraint function is $-2\boldsymbol{x}$, which is clearly nonzero (hence linearly independent) on S. It is a nuisance to have these 2s popping up, so let us agree to maximize $\frac{1}{2}(\boldsymbol{x}, T\boldsymbol{x})$ subject $\frac{1}{2}(1 - (\boldsymbol{x}, \boldsymbol{x})) = 0$ instead. Therefore by the well known Lagrange Multiplier Theorem, there exists λ_1 satisfying

$$T\boldsymbol{x}_1 - \lambda_1 \boldsymbol{x}_1 = \boldsymbol{0}.$$

This obviously implies that the Lagrange multiplier λ_1 is an eigenvalue of T and $\boldsymbol{x}_1$ is a corresponding eigenvector. Further, it is the value of the maximum:

$$Q(\boldsymbol{x}_1) = (\boldsymbol{x}_1, T\boldsymbol{x}_1) = (\boldsymbol{x}_1, \lambda_1 \boldsymbol{x}_1) = \lambda_1,$$

since $(\boldsymbol{x}_1, \boldsymbol{x}_1) = 1$.

Let $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ be defined as above and assume that for $i = 1, \dots, k < n$, each $\boldsymbol{x}_i$ is an eigenvector of T and that $\lambda_i = Q(\boldsymbol{x}_i)$ is its corresponding eigenvalue. We wish to show that $\boldsymbol{x}_{k+1}$ is an eigenvector of T and $\lambda_{k+1} = Q(\boldsymbol{x}_{k+1})$ is its corresponding eigenvalue.

By construction, $\boldsymbol{x}_{k+1}$ maximizes $\frac{1}{2}Q(\boldsymbol{x})$ subject to the $k+1$ constraints

$$\tfrac{1}{2}(1 - (\boldsymbol{x}, \boldsymbol{x})) = 0, \quad (\boldsymbol{x}, \boldsymbol{x}_1) = 0, \quad \dots \quad (\boldsymbol{x}, \boldsymbol{x}_k) = 0.$$

The gradients of these constraint functions are $-\boldsymbol{x}$ and $\boldsymbol{x}_1, \dots, \boldsymbol{x}_k$ respectively. By construction, $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{k+1}$ are orthonormal, so at $\boldsymbol{x} = \boldsymbol{x}_{k+1}$ the gradients of the constraint are linearly independent. Therefore there exist Lagrange multipliers λ_{k+1} and $\mu_1, \dots, \mu_k$ satisfying

$$T\boldsymbol{x}_{k+1} - \lambda_{k+1}\boldsymbol{x}_{k+1} + \mu_1 \boldsymbol{x}_1 + \dots + \mu_k \boldsymbol{x}_k = 0. \tag{10}$$

Therefore

$$Q(\boldsymbol{x}_{k+1}) = (\boldsymbol{x}_{k+1}, T\boldsymbol{x}_{k+1}) = \lambda_{k+1}(\boldsymbol{x}_{k+1}, \boldsymbol{x}_{k+1}) - \mu_1(\boldsymbol{x}_{k+1}, \boldsymbol{x}_1) - \dots - \mu_k(\boldsymbol{x}_{k+1}, \boldsymbol{x}_k) = \lambda_{k+1},$$

since $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{k+1}$ are orthonormal. That is, the multiplier λ_{k+1} is the maximum value of Q over S_k.

By hypothesis, $T\boldsymbol{x}_i = \lambda_i \boldsymbol{x}_i$ for $i = 1, \ldots, k$. Then since T is symmetric,

$$(\boldsymbol{x}_i, T\boldsymbol{x}_{k+1}) = (\boldsymbol{x}_{k+1}, T\boldsymbol{x}_i) = (\boldsymbol{x}_{k+1}, \lambda_i \boldsymbol{x}_i) = 0, \quad i = 1, \ldots, k.$$

That is, $T\boldsymbol{x}_{k+1} \in M_{k\perp}$, so $T\boldsymbol{x}_{k+1} - \lambda_{k+1}\boldsymbol{x}_{k+1} \in M_{k\perp}$, so by Lemma 35 equation (10) implies

$$\underbrace{T\boldsymbol{x}_{k+1} - \lambda_{k+1}\boldsymbol{x}_{k+1}}_{\in M_{k\perp}} = 0 \quad \text{and} \quad \underbrace{\mu_1 \boldsymbol{x}_1 + \cdots + \mu_k \boldsymbol{x}_k}_{\in M_k} = 0.$$

We conclude therefore that $T\boldsymbol{x}_{k+1} = \lambda_{k+1}\boldsymbol{x}_{k+1}$, so that $\boldsymbol{x}_{k+1}$ is an eigenvector of T and λ_{k+1} is the corresponding eigenvalue.

Since V is n-dimensional, $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ is an orthonormal basis of eigenvectors. ∎

10 Matrices

A **matrix** is merely a rectangular array of numbers, or equivalently, a doubly indexed ordered list of real numbers. An $m \times n$ matrix has m rows and n columns. The entries in a matrix are doubly indexed, with the first index denoting its row and the second its column. Here is a generic matrix:

$$\boldsymbol{A} = \begin{bmatrix} \alpha_{1,1} & \ldots & \alpha_{1,n} \\ \vdots & & \vdots \\ \alpha_{m,1} & \ldots & \alpha_{m,n} \end{bmatrix}$$

The plural of *matrix* is *matrices*. Matrices are of interest for two separate but hopelessly intertwined reasons. One is their relation to systems of linear equations and inequalities, and the other is their connection to linear transformations between finite-dimensional vector spaces.

The set of $m \times n$ matrices is denoted

$$\mathbf{M}(m, n).$$

Given a matrix $\boldsymbol{A}$, let $\boldsymbol{A}_i$ denote the i^{th} row of $\boldsymbol{A}$ and let $\boldsymbol{A}^j$ denote the j^{th} column. The i^{th} row and j^{th} column entry is generally denoted by a lower case Greek letter, e.g., $\alpha_{i,j}$. We can identify the rows or columns of a matrix with singly indexed lists of real numbers, that is, elements of some $\boldsymbol{R}^{\text{k}}$. If $\boldsymbol{A}$ is $m \times n$, the **column space** of $\boldsymbol{A}$ is the subset of $\boldsymbol{R}^{\text{m}}$ spanned by the n columns of $\boldsymbol{A}$. Its **row space** is the subspace of $\boldsymbol{R}^{\text{n}}$ spanned by its m rows.

10.1 Matrix operations

If both $\boldsymbol{A}$ and $\boldsymbol{B}$ are $m \times n$ matrices, the **sum** $\boldsymbol{A} + \boldsymbol{B}$ is the $m \times n$ matrix $\boldsymbol{C}$ defined by

$$\gamma_{i,j} = \alpha_{i,j} + \beta_{i,j}.$$

The **scalar multiple** $\alpha\boldsymbol{A}$ of a matrix $\boldsymbol{A}$ by a scalar α is the matrix M defined by $m_{i,j} = \alpha\alpha_{i,j}$. Under these operations the set of $m \times n$ matrices becomes an mn-dimensional vector space.

79 Proposition *The set $\mathbf{M}(m,n)$ is a vector space under the operations of matrix addition and scalar multiplication. It has dimension mn.*

If $\boldsymbol{A}$ is $m \times p$ and $\boldsymbol{B}$ is $p \times n$, the **product** of $\boldsymbol{A}$ and $\boldsymbol{B}$ is the $m \times n$ matrix whose i^{th} row, j^{th} column entry is the dot product $\boldsymbol{A}_i \cdot \boldsymbol{B}^j$ of the i^{th} row of $\boldsymbol{A}$ with the j^{th} column of $\boldsymbol{B}$.

$$(\boldsymbol{AB})_{i,j} = \boldsymbol{A}_i \cdot \boldsymbol{B}^j$$

The reason for this peculiar definition is explained in the next section.

Vectors in $\boldsymbol{R}^{\mathrm{m}}$ may also be considered to be one-dimensional matrices. Let $\boldsymbol{x}'$ be an m-vector (a $1 \times m$ row matrix), $\boldsymbol{y}$ be an n-vector (an $n \times 1$ column matrix), and let $\boldsymbol{A}$ be an $m \times n$ matrix. Then the matrix product $\boldsymbol{x}'\boldsymbol{A}$ considered as a vector in $\boldsymbol{R}^{\mathrm{n}}$ belongs to the row space of $\boldsymbol{A}$, and $\boldsymbol{Ay}$ as a vector in $\boldsymbol{R}^{\mathrm{m}}$ belongs to the column space of $\boldsymbol{A}$.

$$\boldsymbol{x}'\boldsymbol{A} = \sum_{i=1}^{m} x_i \boldsymbol{A}_i \quad \text{and} \quad \boldsymbol{Ay} = \sum_{j=1}^{n} y_j \boldsymbol{A}^j$$

Note that the i^{th} row of $\boldsymbol{AB}$ is given by

$$(\boldsymbol{AB})_i = (\boldsymbol{A}_i)\boldsymbol{B}$$

and the j^{th} column of $\boldsymbol{AB}$ is given by

$$(\boldsymbol{AB})^j = \boldsymbol{A}(\boldsymbol{B}^j).$$

The **main diagonal** of a square matrix $\boldsymbol{A} = [\alpha_{i,j}]$ is the set of $\alpha_{i,j}$ with $i = j$. A matrix is called a **diagonal matrix** if it is square and all its nonzero entries are on the main diagonal. A square matrix is **upper triangular** if the only nonzero elements are on or above the main diagonal, that is, if $i > j$ implies $\alpha_{i,j} = 0$. A square matrix is **lower triangular** if $i < j$ implies $\alpha_{i,j} = 0$.

The $n \times n$ diagonal matrix $\boldsymbol{I}$ whose diagonal entries are all 1 and off-diagonal entries are all 0 has the property that

$$\boldsymbol{AI} = \boldsymbol{IA} = \boldsymbol{A}$$

for any $n \times n$ matrix $\boldsymbol{A}$. The matrix $\boldsymbol{I}$ is called the **$\boldsymbol{n \times n}$ identity matrix**. The **zero matrix** $\mathbf{0}$ has all its entries zero, and satisfies $\boldsymbol{A} + \mathbf{0} = \boldsymbol{A}$.

80 Fact (Summary) *Direct computation reveals the following facts.*

$$\begin{aligned}
(\boldsymbol{AB})\boldsymbol{C} &= \boldsymbol{A}(\boldsymbol{BC}) \\
\boldsymbol{AB} &\neq \boldsymbol{BA} \quad \textit{(in general)} \\
\boldsymbol{A}(\boldsymbol{B}+\boldsymbol{C}) &= (\boldsymbol{AB}) + (\boldsymbol{AC}) \\
(\boldsymbol{A}+\boldsymbol{B})\boldsymbol{C} &= \boldsymbol{AC} + \boldsymbol{BC}
\end{aligned}$$

81 Exercise Verify the following.

1. The product of upper triangular matrices is upper triangular.

2. The product of lower triangular matrices is lower triangular.

3. The product of diagonal matrices is diagonal.

4. The inverse of an upper triangular matrix is upper triangular (if it exists).

5. The inverse of a lower triangular matrix is lower triangular (if it exists).

6. The inverse of a diagonal matrix is diagonal (if it exists).

□

10.2 Systems of linear equations

One of the main uses of matrices is the simplification of representing a system of linear equations. For instance, consider the following system of equations.

$$\begin{aligned} 3x_1 + 2x_2 &= 8 \\ 2x_1 + 3x_2 &= 7 \end{aligned}$$

It has align unique solution $x_1 = 2$ and $x_2 = 1$. One way to solve this is to take the second equation and solve for $x_1 = \frac{7}{2} - \frac{3}{2}x_2$ and substitute this into the first equation to get $3(\frac{7}{2} - \frac{3}{2}x_2) + 2x_2 = 8$, so $x_2 = 1$ and $x_1 = \frac{7}{2} - \frac{3}{2} = 2$. However, there is a computationally efficient way to attack these problems using **elementary row operations**. The first step is to write down the so-called augmented coefficient matrix of the system, which is the 2×3 matrix of just the numbers above:

$$\begin{bmatrix} 3 & 2 & 8 \\ 2 & 3 & 7 \end{bmatrix}.$$

There are three elementary row operations, and they correspond to steps used to solve a system of equations. One of these operations is to interchange two rows. We won't use that here. Another is to multiply a row by a nonzero scalar. This does not change the solution. The third operation is to add one row to another. These last two operations can be combined, and we can think of adding a scalar multiple of one row to another as an elementary row operation. We apply these operations until we get a matrix of the form

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \end{bmatrix}$$

which is the augmented matrix of the system

$$\begin{aligned} x_1 &= a \\ x_2 &= b \end{aligned}$$

and the system is solved. There is a simple algorithm for deciding which elementary row operations to apply, namely, the **Gaussian elimination algorithm**. In a section below, we shall go into this algorithm in detail, but let me just give you a hint here. First we multiply the first row by $\frac{1}{3}$, to get a leading 1:

$$\begin{bmatrix} 1 & \frac{2}{3} & \frac{8}{3} \\ 2 & 3 & 7 \end{bmatrix}$$

We want to eliminate x_1 from the second equation, so we add an appropriate multiple of the first row to the second. In this case the multiple is -2, the result is:

$$\begin{bmatrix} 1 & \frac{2}{3} & \frac{8}{3} \\ 2-2\cdot 1 & 3-2\cdot\frac{2}{3} & 7-2\cdot\frac{8}{3} \end{bmatrix} = \begin{bmatrix} 1 & \frac{2}{3} & \frac{8}{3} \\ 0 & \frac{5}{3} & \frac{5}{3} \end{bmatrix}.$$

Now multiply the second row by $\frac{3}{5}$ to get

$$\begin{bmatrix} 1 & \frac{2}{3} & \frac{8}{3} \\ 0 & 1 & 1 \end{bmatrix}.$$

Finally to eliminate x_2 from the first row we add $-\frac{2}{3}$ times the second row to the first and get

$$\begin{bmatrix} 1-\frac{2}{3}\cdot 0 & \frac{2}{3}-\frac{2}{3}\cdot 1 & \frac{8}{3}-\frac{2}{3}\cdot 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{bmatrix},$$

which accords with our earlier result.

10.3 Matrix representation of a linear transformation

Let T be a linear transformation from the n-dimensional space V into the m-dimensional space W. Let $\boldsymbol{x}_1,\dots,\boldsymbol{x}_n$ be an ordered basis for V and $\boldsymbol{y}_1,\dots,\boldsymbol{y}_m$ be an ordered basis for W. Then there are scalars $\tau_{i,j}$, $i=1,\dots,m$, $j=1,\dots,n$ satisfying

$$\begin{aligned} T\boldsymbol{x}_1 &= \sum_{i=1}^m \tau_{i,1}\boldsymbol{y}_i \\ T\boldsymbol{x}_2 &= \sum_{i=1}^m \tau_{i,2}\boldsymbol{y}_i \\ &\vdots \\ T\boldsymbol{x}_n &= \sum_{i=1}^m \tau_{i,n}\boldsymbol{y}_i. \end{aligned}$$

The $m\times n$ array of numbers

$$\mathbf{M}(T) = \begin{bmatrix} \tau_{1,1} & \dots & \tau_{1,n} \\ \vdots & & \vdots \\ \tau_{m,1} & \dots & \alpha_{m,n} \end{bmatrix}$$

is the **matrix representation of $\boldsymbol{T}$ with respect to the ordered bases $(\boldsymbol{x}_j), (\boldsymbol{y}_i)$**. Note that the j^{th} column of this matrix is the coordinate vector of $T\boldsymbol{x}_j$ with respect to the ordered basis $\boldsymbol{y}_1,\dots,\boldsymbol{y}_m$.

This representation provides an isomorphism between matrices and linear transformations. The proof is left as an exercise.

82 Proposition *Let V be an n-dimensional vector space, and let W be an m-dimensional vector space. Fix an ordered basis for each, and let $\mathbf{M}(T) = \left[\tau_{i,j}\right]$ be the matrix representation a linear transformation $T \colon V \to W$. Then the mapping*

$$T \to \mathbf{M}(T)$$

is a linear isomorphism from $\mathsf{L}(V, W)$ to $\mathbf{M}(m, n)$.

Let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ be an ordered basis for V and let $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$ be an ordered basis for W. Let $\boldsymbol{z}$ belong to V and let $\zeta_1, \ldots, \zeta_n$ be the coordinates of $\boldsymbol{z}$ with respect to the basis $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$,. That is,

$$\boldsymbol{z} = \sum_{i=1}^{n} \zeta_i \boldsymbol{x}_i.$$

We can use matrix multiplication to compute the coordinates of $T\boldsymbol{z}$ with respect to the basis $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$. We have

$$\begin{aligned} T\boldsymbol{z} &= \sum_{j=1}^{n} \zeta_j T\boldsymbol{x}_j \\ &= \sum_{j=1}^{n} \zeta_j \sum_{i=1}^{m} \tau_{i,j} \boldsymbol{y}_i \\ &= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \tau_{i,j} \zeta_j \right) \boldsymbol{y}_i \end{aligned}$$

The coordinates of $T\boldsymbol{z}$ with respect to $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$ are given by Need better notation.

$$(T\boldsymbol{z})_i = \sum_{j=1}^{n} \tau_{i,j} \zeta_j.$$

That is, the coordinate vector of $T\boldsymbol{z}$ is $\mathbf{M}(T)$ times the column vector $\boldsymbol{\zeta} = [\zeta_1, \ldots, \zeta_n]$ of coordinates of $\boldsymbol{z}$.

The matrix representation can be thought of in the following terms. Let X denote the coordinate mapping of V onto $\boldsymbol{R}^{\mathrm{n}}$ with respect to the ordered basis $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$. Similarly Y denotes the coordinate mapping from W onto $\boldsymbol{R}^{\mathrm{m}}$. In order to compute the coordinates of $T\boldsymbol{z}$, we first find the coordinate vector of $X\boldsymbol{z}$, and then multiply by the matrix $\mathbf{M}(T)$, as the following "commutative diagram" shows.

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "X"] & W \arrow[d, "Y"] \\ \boldsymbol{R}^{\mathrm{n}} \arrow[r, "\mathbf{M}(T)"] & \boldsymbol{R}^{\mathrm{m}} \end{tikzcd}$$

83 Example (The matrix of the coordinate mapping) Consider the case $V = \boldsymbol{R}^{\mathrm{n}}$. That is, elements of V are already thought of as ordered lists of real numbers. Let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ be an ordered basis, and let X denote the coordinate mapping from $\boldsymbol{R}^{\mathrm{n}}$ with this basis to $\boldsymbol{R}^{\mathrm{n}}$ with the standard basis. Then $\mathbf{M}(X)$ is simply the matrix whose j^{th} column is $\boldsymbol{x}_j$. □

84 Example (Matrices as linear transformations from $\boldsymbol{R}^{\mathrm{n}}$ to $\boldsymbol{R}^{\mathrm{m}}$) Let $\boldsymbol{A} = [\alpha_{i,j}]$ be an $m \times n$ matrix and

$$\boldsymbol{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \boldsymbol{R}^{\mathrm{n}},$$

an $n \times 1$ matrix. The matrix product $\boldsymbol{Ax}$ is an $m \times 1$ matrix whose i^{th} row is

$$\sum_{j=1}^{n} \alpha_{i,j} x_j \quad i = 1, \ldots, m.$$

Then $T \colon \boldsymbol{x} \mapsto \boldsymbol{Ax}$ defines a linear transformation from $\boldsymbol{R}^{\mathrm{n}}$ to $\boldsymbol{R}^{\mathrm{m}}$. The matrix $\mathbf{M}(T)$ of this transformation with respect to the standard ordered bases (the bases of unit coordinate vectors) is just $\boldsymbol{A}$. □

85 Definition *The rank of a matrix is the largest number of linearly independent columns.*

It follows from Proposition 57 that:

86 Proposition *An $m \times m$ matrix has an inverse if and only if it has rank m.*

87 Example (The identity matrix) What is the matrix representation for the identity mapping $I \colon \boldsymbol{R}^{\mathrm{m}} \to \boldsymbol{R}^{\mathrm{m}}$?

$$\mathbf{M}(I) = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$$

is the $m \times m$ identity matrix $\boldsymbol{I}$. If the transformation T is invertible, so that $TT^{-1} = I$, then $\mathbf{M}(T)\mathbf{M}(T^{-1}) = \boldsymbol{I}$. The matrix $\mathbf{M}(T^{-1})$ is naturally referred to as the **inverse of the matrix $\mathbf{M}(T)$**. In general, if $\boldsymbol{A}$ defines an invertible transformation from $\boldsymbol{R}^{\mathrm{m}}$ onto $\boldsymbol{R}^{\mathrm{m}}$, the matrix $\boldsymbol{A}^{-1}$ satisfies

$$\boldsymbol{A}\boldsymbol{A}^{-1} = \boldsymbol{A}^{-1}\boldsymbol{A} = \boldsymbol{I}.$$

□

88 Example (The zero matrix) The matrix for the zero transformation $\mathbf{0} \colon \boldsymbol{R}^{\mathrm{n}} \to \boldsymbol{R}^{\mathrm{m}}$, is

$$\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix},$$

the $m \times n$ zero matrix. □

The **transpose of a matrix** is the matrix formed by interchanging rows and columns. The transpose of a matrix is also sometimes called the **adjoint** matrix. This definition is justified by the following lemma.

89 Lemma $\mathbf{M}(T)_{i,j} = \mathbf{M}(T')_{j,i}$.

Proof:

$$\mathbf{M}(T)_{i,j} = (\boldsymbol{e}_i, T\boldsymbol{e}_j) = (T'\boldsymbol{e}_i, \boldsymbol{e}_j) = (\boldsymbol{e}_j, T'\boldsymbol{e}_i) = \mathbf{M}(T')_{j,i}$$

∎

10.4 Gershgorin's Theorem

For a diagonal matrix, the diagonal elements of the matrix are the eigenvalues of the corresponding linear transformation. Even if the matrix is not diagonal, its eigenvalues are "close" to the diagonal elements.

90 Gershgorin's Theorem *Let* $\boldsymbol{A} = \begin{bmatrix}\alpha_{i,j}\end{bmatrix}$ *be an* $m \times m$ *real matrix. If* λ *is an eigenvalue of* $\boldsymbol{A}$*, that is, if* $\boldsymbol{A}\boldsymbol{x} = \lambda\boldsymbol{x}$ *for some nonzero* $\boldsymbol{x}$*, then for some* i*,*

$$|\lambda - \alpha_{i,i}| \leqslant \sum_{j:j\neq i} |\alpha_{i,j}|\,.$$

Proof: (Cf. Franklin [12, p. 162].) Let $\boldsymbol{x} = (\xi_1, \dots, \xi_m)$ be an eigenvector of $\boldsymbol{A}$ belonging to the eigenvalue λ. Choose the index i so that

$$|\xi_i| = \max\{|\xi_1|, \dots, |\xi_m|\},$$

and note that since $\boldsymbol{x} \neq \mathbf{0}$, we have $|\xi_i| > 0$. Then by the definition of eigenvalue and eigenvector,

$$(\lambda\boldsymbol{I} - \boldsymbol{A})\boldsymbol{x} = \mathbf{0}.$$

Now the i^{th} component of the vector $(\lambda\boldsymbol{I} - \boldsymbol{A})\boldsymbol{x}$ is just $(\lambda - \alpha_{i,i})\xi_i - \sum_{j:j\neq i} \alpha_{i,j}\xi_j = 0$, so

$$(\lambda - \alpha_{i,i})\xi_i = \sum_{j:j\neq i} \alpha_{i,j}\xi_j$$

so taking absolute values,

$$\begin{aligned}|\lambda - \alpha_{i,i}|\ |\xi_i| &= |\sum_{j:j\neq i} \alpha_{i,j}\xi_j| \\ &\leqslant \sum_{j:j\neq i} |\alpha_{i,j}|\ |\xi_j|\end{aligned}$$

so dividing by $|\xi_i| > 0$,

$$\begin{aligned}|\lambda - \alpha_{i,i}| &\leqslant \sum_{j:j\neq i} |\alpha_{i,j}|\,\frac{|\xi_j|}{|\xi_i|} \\ &\leqslant \sum_{j:j\neq i} |\alpha_{i,j}|\,.\end{aligned}$$

∎

A square matrix $\boldsymbol{A}$ has a **dominant diagonal** if for each i,

$$|a_{i,i}| > \sum_{j:j\neq i} |\alpha_{i,j}|\,.$$

Note that any diagonal matrix with nonzero diagonal elements has a dominant diagonal. This leads to the following corollary of Gershgorin's Theorem.

91 Corollary *If $\boldsymbol{A}$ is a nonnegative square matrix with a dominant diagonal, then every eigenvalue of $\boldsymbol{A}$ is strictly positive.*

Proof: Since $\boldsymbol{A}$ is nonnegative, if λ is an eigenvalue, then Gershgorin's theorem implies that for some i,

$$\alpha_{i,i} - \lambda \leqslant |\lambda - \alpha_{i,i}| \leqslant \sum_{j:j\neq i} \alpha_{i,j},$$

so

$$0 < \alpha_{i,i} - \sum_{j:j\neq i} \alpha_{i,j} \leqslant \lambda,$$

where the first inequality is the dominant diagonal property. ∎

For applications of this corollary and related results, see McKenzie [18].

10.5 Matrix representation of a composition

Let S take $\boldsymbol{R}^{\mathrm{p}} \to \boldsymbol{R}^{\mathrm{n}}$ be linear with matrix $\mathbf{M}(S) = [\beta_{j,k}]_{j=1,\ldots,n}^{k=1,\ldots,p}$. Let T take $\boldsymbol{R}^{\mathrm{n}} \to \boldsymbol{R}^{\mathrm{m}}$ be linear with matrix $\mathbf{M}(T) = [\alpha_{i,j}]_{i=1,\ldots,m}^{j=1,\ldots,n}$. Then $T \circ S\colon \boldsymbol{R}^{\mathrm{p}} \to \boldsymbol{R}^{\mathrm{m}}$ is linear. What is $\mathbf{M}(TS)$?

Let $\boldsymbol{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_p \end{bmatrix}$. Then

$$S\boldsymbol{x} = \sum_{j=1}^{n} \left(\sum_{k=1}^{p} \beta_{j,k} x_k \right) \boldsymbol{e}_j.$$

$$T(S\boldsymbol{x}) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{i,j} \left(\sum_{k=1}^{p} \beta_{j,k} x_k \right) \right) \boldsymbol{e}_i.$$

Set

$$\gamma_{i,k} = \sum_{j=1}^{n} \alpha_{i,j} \beta_{j,k}.$$

Then

$$T(S\boldsymbol{x}) = \sum_{i=1}^{m} \left(\sum_{k=1}^{p} \gamma_{i,k} x_k \right) \boldsymbol{e}_i.$$

Thus $\mathbf{M}(TS) = [\gamma_{i,k}]_{i=1,\ldots,m}^{k=1,\ldots,p}$. This proves the following theorem.

92 Theorem $\mathbf{M}(TS) = \mathbf{M}(T)\mathbf{M}(S)$.

Thus multiplication of matrices corresponds to composition of linear transformations.

Let $S, T\colon \boldsymbol{R}^{\mathrm{n}} \to \boldsymbol{R}^{\mathrm{m}}$ be linear transformations with matrices $\boldsymbol{A}, \boldsymbol{B}$. Then $S + T$ is linear. The matrix for $S + T$ is $\boldsymbol{A} + \boldsymbol{B}$ where $(\boldsymbol{A} + \boldsymbol{B})_{i,j} = \alpha_{i,j} + \beta_{i,j}$.

10.6 Change of basis

A linear transformation may have different matrix representations for different bases. Is there some way to tell if two matrices represent the same transformation?

We shall answer this question for the important case where T maps an m-dimensional vector space V into itself, and we use the same basis for V as both the domain and the range. Let $\boldsymbol{A} = [\alpha_{i,j}]$ represent T with respect to the ordered basis $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$, and let $\boldsymbol{B} = [\beta_{i,j}]$ represent T with respect to the ordered basis $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$.

That is,

$$T\boldsymbol{x}_i = \sum_{k=1}^{m} \alpha_{k,i}\boldsymbol{x}_k \quad \text{and} \quad T\boldsymbol{y}_i = \sum_{k=1}^{m} \beta_{k,i}\boldsymbol{y}_k.$$

Let X be the coordinate map from V into $\boldsymbol{R}^{\mathrm{m}}$ with respect to the ordered basis $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$, and let Y be the coordinate map for the ordered basis $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$. Then X and Y have full rank and so have inverses.

Consider the following commutative diagram.

$$\begin{tikzcd}
\boldsymbol{R}^{\mathrm{m}} \arrow[r, "\boldsymbol{B}"] & \boldsymbol{R}^{\mathrm{m}} \\
V \arrow[r, "T"] \arrow[u, "Y"] \arrow[d, "X"] & V \arrow[u, "Y"] \arrow[d, "X"] \\
\boldsymbol{R}^{\mathrm{m}} \arrow[r, "\boldsymbol{A}"] & \boldsymbol{R}^{\mathrm{m}}
\end{tikzcd}$$

The mapping XY^{-1} from $\boldsymbol{R}^{\mathrm{m}}$ onto $\boldsymbol{R}^{\mathrm{m}}$ followed by $\boldsymbol{A}$ from $\boldsymbol{R}^{\mathrm{m}}$ into $\boldsymbol{R}^{\mathrm{m}}$, which maps the upper left $\boldsymbol{R}^{\mathrm{m}}$ into the lower right $\boldsymbol{R}^{\mathrm{m}}$, is the same as $\boldsymbol{B}$ followed by XY^{-1}. Let $\boldsymbol{C}$ be the matrix representation of XY^{-1} with respect to the standard ordered basis of unit coordinate vectors. Then

$$\boldsymbol{A} = \boldsymbol{C}\boldsymbol{B}\boldsymbol{C}^{-1} \quad \text{and} \quad \boldsymbol{B} = \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C}. \tag{$\star$}$$

93 Definition *Two $m \times m$ matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ are called **similar** if there is some nonsingular matrix $\boldsymbol{C}$ such that ($\star$) holds.*

So we have already proved half of the following. The second half is left for you. (See Apostol [6, Theorem 4.7, p. 110] if you get stuck.)

94 Theorem *Two matrices are similar if and only if they represent the same linear transformation.*

The following are corollaries, but have simple direct proofs.

95 Proposition *If $\boldsymbol{A}, \boldsymbol{B}$ are similar with $\boldsymbol{A} = \boldsymbol{C}\boldsymbol{B}\boldsymbol{C}^{-1}$, then λ is an eigenvalue of $\boldsymbol{A}$ if it is an eigenvalue of $\boldsymbol{B}$. If $\boldsymbol{x}$ is an eigenvector of $\boldsymbol{A}$, $\boldsymbol{C}^{-1}\boldsymbol{x}$ is an eigenvector of $\boldsymbol{B}$.*

Proof: Suppose $\boldsymbol{x}$ is an eigenvector of $\boldsymbol{A}$, $\boldsymbol{A}\boldsymbol{x} = \lambda\boldsymbol{x}$. Let $\boldsymbol{y} = \boldsymbol{C}^{-1}\boldsymbol{x}$. Since $\boldsymbol{A} = \boldsymbol{C}\boldsymbol{B}\boldsymbol{C}^{-1}$,

$$\lambda\boldsymbol{x} = \boldsymbol{A}\boldsymbol{x} = \boldsymbol{C}\boldsymbol{B}\boldsymbol{C}^{-1}\boldsymbol{x} = \boldsymbol{C}\boldsymbol{B}\boldsymbol{y}.$$

Premultiplying by $\boldsymbol{C}^{-1}$,

$$\lambda\boldsymbol{y} = \lambda\boldsymbol{C}^{-1}\boldsymbol{x} = \boldsymbol{C}^{-1}\boldsymbol{C}\boldsymbol{B}\boldsymbol{y} = \boldsymbol{B}\boldsymbol{y}.$$

∎

96 Proposition *If $\boldsymbol{A}$ and $\boldsymbol{B}$ are similar, then* $\operatorname{rank}\boldsymbol{A} = \operatorname{rank}\boldsymbol{B}$.

Proof: We prove $\operatorname{rank}\boldsymbol{B} \geqslant \operatorname{rank}\boldsymbol{A}$. Symmetry completes the argument. Let $\boldsymbol{z}_1, \dots, \boldsymbol{z}_k$ be a basis for $\operatorname{range}\boldsymbol{A}$, and let $\boldsymbol{y}_i$ satisfy $\boldsymbol{z}_i = \boldsymbol{A}\boldsymbol{y}_i$. Put $\boldsymbol{w}_i = \boldsymbol{C}^{-1}\boldsymbol{y}_i$. Then the $\boldsymbol{B}\boldsymbol{w}_i$'s are independent. To see this suppose

$$0 = \sum_{i=1}^{k} \alpha_i(\boldsymbol{B}\boldsymbol{w}_i) = \sum_{i=1}^{k} \alpha_i\boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C}\boldsymbol{C}^{-1}\boldsymbol{y}_i = \sum_{i=1}^{k} \alpha_i\boldsymbol{C}^{-1}\boldsymbol{z}_i = \boldsymbol{C}^{-1}\Big(\sum_{i=1}^{k} \alpha_i\boldsymbol{z}_i\Big).$$

Since $\boldsymbol{C}^{-1}$ is nonsingular, this implies $\sum_{i=1}^{k} \alpha_i z_i = 0$, which in turn implies $\alpha_i = 0$, $i = 1, \dots, k$.

∎

10.7 The Principal Axis Theorem

The next result describes the diagonalization of a symmetric matrix.

97 Definition *A square matrix $\boldsymbol{X}$ is* **orthogonal** *if $\boldsymbol{X}'\boldsymbol{X} = \boldsymbol{I}$, or equivalently $\boldsymbol{X}' = \boldsymbol{X}^{-1}$.*

98 Principal Axis Theorem *Let $\boldsymbol{A}\colon \boldsymbol{R}^{\mathrm{m}} \to \boldsymbol{R}^{\mathrm{m}}$ be a symmetric matrix. Let $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$ be an orthonormal basis for $\boldsymbol{R}^{\mathrm{m}}$ made up of eigenvectors of $\boldsymbol{A}$, with corresponding eigenvalues $\lambda_1, \dots, \lambda_m$. Set*

$$\boldsymbol{\Lambda} = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_m \end{bmatrix},$$

and set $\boldsymbol{X} = [\boldsymbol{x}_1, \dots, \boldsymbol{x}_m]$.

Then

$$\boldsymbol{A} = \boldsymbol{X}\boldsymbol{\Lambda}\boldsymbol{X}^{-1},$$
$$\boldsymbol{\Lambda} = \boldsymbol{X}^{-1}\boldsymbol{A}\boldsymbol{X},$$

and $\boldsymbol{X}$ is orthogonal, that is,

$$\boldsymbol{X}^{-1} = \boldsymbol{X}'.$$

Proof: Now $\boldsymbol{X}'\boldsymbol{X} = \boldsymbol{I}$ by orthonormality, so $\boldsymbol{X}^{-1} = \boldsymbol{X}'$. Pick any $\boldsymbol{z}$ and set $\boldsymbol{y} = \boldsymbol{X}^{-1}\boldsymbol{z}$, so $\boldsymbol{z} = \boldsymbol{X}\boldsymbol{y} = \sum_{j=1}^{m} y_j \boldsymbol{x}_j$. Then

$$\begin{aligned}\boldsymbol{A}\boldsymbol{z} = \sum_{j=1}^{m} y_j \boldsymbol{A}\boldsymbol{x}_i &= \sum_{j=1}^{m} y_j(\lambda_j \boldsymbol{x}_j)\\ &= \boldsymbol{X}\boldsymbol{\Lambda}\boldsymbol{y}\\ &= \boldsymbol{X}\boldsymbol{\Lambda}\boldsymbol{X}^{-1}\boldsymbol{z}.\end{aligned}$$

Since $\boldsymbol{z}$ is arbitrary $\boldsymbol{A} = \boldsymbol{X}\boldsymbol{\Lambda}\boldsymbol{X}^{-1}$. ∎

This result is called the principal axis theorem because in the case where $\boldsymbol{A}$ is positive definite (see Definition 109 below), the columns of $\boldsymbol{X}$ are the principal axes of the ellipsoid $\{\boldsymbol{x} : \boldsymbol{x}'\boldsymbol{A}\boldsymbol{x} = 1\}$. See Franklin [12, § 4.6, pp. 80–83].

10.8 Simultaneous diagonalization

99 Theorem (Simultaneous Diagonalization) *Let $\boldsymbol{A}$, $\boldsymbol{B}$ be symmetric $m \times m$ matrices.*

Then $\boldsymbol{A}\boldsymbol{B} = \boldsymbol{B}\boldsymbol{A}$ if and only if there exists an orthonormal basis consisting of vectors that are eigenvectors of both $\boldsymbol{A}$ and $\boldsymbol{B}$. Then letting $\boldsymbol{X}$ be the orthogonal matrix whose columns are the basis we have

$$\begin{aligned}\boldsymbol{A} &= \boldsymbol{X}\boldsymbol{\Lambda}_A\boldsymbol{X}^{-1}\\ \boldsymbol{B} &= \boldsymbol{X}\boldsymbol{\Lambda}_B\boldsymbol{X}^{-1},\end{aligned}$$

where $\boldsymbol{\Lambda}_A$ and $\boldsymbol{\Lambda}_B$ are diagonal matrices of eigenvalues of $\boldsymbol{A}$ and $\boldsymbol{B}$ respectively.

Partial proof: ($\Longleftarrow$)

$$\boldsymbol{A}\boldsymbol{B} = \boldsymbol{X}\boldsymbol{\Lambda}_A\boldsymbol{X}^{-1}\boldsymbol{X}\boldsymbol{\Lambda}_B\boldsymbol{X}^{-1} = \boldsymbol{X}\boldsymbol{\Lambda}_A\boldsymbol{\Lambda}_B\boldsymbol{X}^{-1} = \boldsymbol{X}\boldsymbol{\Lambda}_B\boldsymbol{\Lambda}_A\boldsymbol{X}^{-1} = \boldsymbol{X}\boldsymbol{\Lambda}_B\boldsymbol{X}^{-1}\boldsymbol{X}\boldsymbol{\Lambda}_A\boldsymbol{X} = \boldsymbol{B}\boldsymbol{A},$$

since diagonal matrices commute.

($\Longrightarrow$) We shall prove the result for the special case where $\boldsymbol{A}$ has distinct eigenvalues. In this case, the eigenvectors associated with any eigenvalue are distinct up to scalar multiplication.

Let $\boldsymbol{x}$ be an eigenvector of $\boldsymbol{A}$ corresponding to eigenvalue λ. Suppose $\boldsymbol{A}$ and $\boldsymbol{B}$ commute. Then

$$\boldsymbol{A}(\boldsymbol{B}\boldsymbol{x}) = \boldsymbol{B}\boldsymbol{A}\boldsymbol{x} = \boldsymbol{B}(\lambda\boldsymbol{x}) = \lambda(\boldsymbol{B}\boldsymbol{x}).$$

This means that $\boldsymbol{B}\boldsymbol{x}$ too is an eigenvector of $\boldsymbol{A}$ corresponding to λ, provided $\boldsymbol{B}\boldsymbol{x} \neq 0$. But as remarked above, this implies that $\boldsymbol{B}\boldsymbol{x}$ is a scalar multiple of $\boldsymbol{x}$, so $\boldsymbol{x}$ is an eigenvector of $\boldsymbol{B}$ too. So let $\boldsymbol{X}$ be a matrix whose columns are a basis of orthonormal eigenvectors for both $\boldsymbol{A}$ and $\boldsymbol{B}$. Then it follows that $\boldsymbol{A} = \boldsymbol{X}\boldsymbol{\Lambda}_A\boldsymbol{X}^{-1}$, where $\boldsymbol{\Lambda}_A$ is the diagonal matrix of eigenvalues, and similarly $\boldsymbol{B} = \boldsymbol{X}\boldsymbol{\Lambda}_B\boldsymbol{X}^{-1}$.

We now present a sketch of the proof for the general case. The crux of the proof is that in general, the eigenspace M associated with λ may be more than one-dimensional, so it is harder to conclude that the eigenvectors of $\boldsymbol{A}$ and $\boldsymbol{B}$ are the same. To get around this problem observe that $\boldsymbol{B}^2\boldsymbol{A} = \boldsymbol{B}\boldsymbol{B}\boldsymbol{A} = \boldsymbol{B}\boldsymbol{A}\boldsymbol{B} = \boldsymbol{A}\boldsymbol{B}\boldsymbol{B} = \boldsymbol{A}\boldsymbol{B}^2$, and in general, $\boldsymbol{B}^n\boldsymbol{A} = \boldsymbol{A}\boldsymbol{B}^n$, so that if $\boldsymbol{Ax} = \lambda\boldsymbol{x}$, then $\boldsymbol{A}(\boldsymbol{B}^n\boldsymbol{x}) = \boldsymbol{B}^n\boldsymbol{Ax} = \boldsymbol{B}^n\lambda\boldsymbol{x} = \lambda(\boldsymbol{B}^n\boldsymbol{x})$. That is, for every n, the vector $\boldsymbol{B}^n\boldsymbol{x}$ is also an eigenvector of $\boldsymbol{A}$ corresponding to λ. Since the eigenspace M associated with λ is finite-dimensional, for some minimal k, the vectors $\boldsymbol{x}, \boldsymbol{Bx}, \dots, \boldsymbol{B}^k\boldsymbol{x}$ are dependent. That is, there are $\alpha_0, \dots, \alpha_k$, not all zero, with

$$\alpha_0\boldsymbol{x} + \alpha_1\boldsymbol{Bx} + \alpha_2\boldsymbol{B}^2\boldsymbol{x} + \cdots + \alpha_k\boldsymbol{B}^k\boldsymbol{x} = \boldsymbol{0}.$$

Let $\mu_1, \dots, \mu_k$ be the roots of the polynomial $\alpha_0 + \alpha_1 y + \alpha_2 y^2 + \cdots + \alpha_k y^k$. Then

$$[(\boldsymbol{B} - \mu_1\boldsymbol{I})(\boldsymbol{B} - \mu_2\boldsymbol{I}) \cdots (\boldsymbol{B} - \mu_k\boldsymbol{I})]\boldsymbol{x} = 0.$$

Set $\boldsymbol{z} = [(\boldsymbol{B} - \mu_2\boldsymbol{I})(\boldsymbol{B} - \mu_3\boldsymbol{I}) \cdots (\boldsymbol{B} - \mu_k\boldsymbol{I})]\boldsymbol{x}$

If k is minimal, then $\boldsymbol{z} \neq \boldsymbol{0}$. (Even if coefficients are complex. Independence over the real field implies independence over complex field. Just look at real and imaginary parts.) Therefore $(\boldsymbol{B} - \mu_1\boldsymbol{I})\boldsymbol{z} = \boldsymbol{0}$

Claim: μ_1 and z are *real.*

Proof of claim: Let $\mu_1 = \alpha + i\beta$ and $\boldsymbol{z} = \boldsymbol{x} + i\boldsymbol{y}$

$$\boldsymbol{B}(\boldsymbol{x} + i\boldsymbol{y}) = (\alpha + i\beta)(\boldsymbol{x} + i\boldsymbol{y})$$

Therefore $\boldsymbol{Bx} = \alpha\boldsymbol{x} - \beta\boldsymbol{y}$ and $\boldsymbol{By} = \beta\boldsymbol{x} + \alpha\boldsymbol{y}$ (equate real and imaginary parts). Thus $\boldsymbol{y}'\boldsymbol{Bx} = \alpha\boldsymbol{y}'\boldsymbol{x} - \beta\boldsymbol{y}'\boldsymbol{y}$ and by symmetry $\boldsymbol{y}'\boldsymbol{Bx} = \boldsymbol{x}'\boldsymbol{By} = \beta\boldsymbol{x}'\boldsymbol{x} + \alpha\boldsymbol{x}'\boldsymbol{y}$.

Now,

$$\alpha(\boldsymbol{y}'\boldsymbol{x}) - \beta(\boldsymbol{y}'\boldsymbol{y}) = \beta(\boldsymbol{x}'\boldsymbol{x}) + \alpha(\boldsymbol{x}'\boldsymbol{y}),$$

so $\beta = 0$ or $\boldsymbol{z} = \boldsymbol{0}$, i.e., $\boldsymbol{x} = 0$ and $\boldsymbol{y} = 0$. But $\boldsymbol{z} \neq \boldsymbol{0}$, so $\beta = 0$ and μ_1 is real. Similarly *each* μ_i is real. □

Therefore $\boldsymbol{z}$ is a real linear combination of $\boldsymbol{B}^n\boldsymbol{x}$ (all eigenvectors of $\boldsymbol{A}$) satisfying $(\boldsymbol{B} - \mu_1\boldsymbol{I})\boldsymbol{z} = \boldsymbol{0}$. In other words, $\boldsymbol{Bz} = \mu_1\boldsymbol{z}$, so $\boldsymbol{z}$ is an eigenvector of both $\boldsymbol{B}$ and $\boldsymbol{A}$!

We now consider the orthogonal complement of z in the eigenspace M to recursively construct a basis for M composed of eigenvectors for both $\boldsymbol{A}$ and $\boldsymbol{B}$.

We must do this for each eigenvalue λ of $\boldsymbol{A}$. More details are in Rao [20, Result (iii), pp. 41–42]. ■

10.9 Trace

100 Definition *Let $\boldsymbol{A}$ be an $m \times m$ matrix. The **trace** of $\boldsymbol{A}$, denoted $\operatorname{tr}\boldsymbol{A}$, is defined by*

$$\operatorname{tr}\boldsymbol{A} = \sum_{i=1}^{m} \alpha_{ii}.$$

The trace is a linear functional on the set of $m \times m$ matrices.

101 Lemma *Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be $m \times m$ matrices. Then*

$$\operatorname{tr}(\alpha\boldsymbol{A} + \beta\boldsymbol{B}) = \alpha\operatorname{tr}\boldsymbol{A} + \beta\operatorname{tr}\boldsymbol{B} \tag{11}$$

$$\operatorname{tr}(\boldsymbol{AB}) = \operatorname{tr}(\boldsymbol{BA}). \tag{12}$$

Proof: The proof of linearity (11) is straightforward. For the proof of (12), observe that

$$\operatorname{tr} \boldsymbol{AB} = \sum_{i=1}^{m} \left(\sum_{j=1}^{m} \alpha_{i,j}\beta_{j,i} \right) = \sum_{j=1}^{m} \left(\sum_{i=1}^{m} \beta_{j,i}\alpha_{i,j} \right) = \operatorname{tr} \boldsymbol{BA}.$$

∎

Equation (11) says that the trace is a linear functional on the vector space $\mathbf{M}(m, m)$ of $m \times m$ matrices. The next result says that up to a scale multiple it is the only linear functional to satisfy (12).

102 Proposition *If ℓ is a linear functional on $\mathbf{M}(m, m)$ satisfying*

$$\ell(\boldsymbol{AB}) = \ell(\boldsymbol{BA}) \quad \textit{for all } \boldsymbol{A}, \boldsymbol{B} \in \mathbf{M}(m, m),$$

then there is a constant α such that for all $\boldsymbol{A} \in \mathbf{M}(m, m)$,

$$\ell(\boldsymbol{A}) = \alpha \operatorname{tr} \boldsymbol{A}.$$

Proof: To show uniqueness, let $\ell\colon \mathbf{M}(m, m) \to \boldsymbol{R}$ be a linear functional satisfying

$$\ell(\boldsymbol{AB}) = \ell(\boldsymbol{BA}) \quad \text{for all } \boldsymbol{A}, \boldsymbol{B} \in \mathbf{M}(m, m).$$

Now ℓ belongs to the space $\mathsf{L}(\mathbf{M}(m, m), \boldsymbol{R})$. The ordered basis on V induces a matrix representation for ℓ as an $mm \times 1$ matrix, call it $\boldsymbol{L}$ so that

$$\ell(\boldsymbol{A}) = \sum_{i=1}^{m} \sum_{j=1}^{m} \boldsymbol{L}_{ij} \boldsymbol{A}_{ij}.$$

We also know that $\ell(\boldsymbol{AB} - \boldsymbol{BA}) = 0$ for every $\boldsymbol{A}, \boldsymbol{B} \in \mathbf{M}(m, m)$. That is,

$$\sum_{i=1}^{m} \sum_{j=1}^{m} \boldsymbol{L}_{ij} (\boldsymbol{AB} - \boldsymbol{BA})_{ij} = \sum_{i=1}^{m} \sum_{j=1}^{m} \sum_{k=1}^{m} \boldsymbol{L}_{ij} \left\{ \boldsymbol{A}_{ik}\boldsymbol{B}_{kj} - \boldsymbol{B}_{ik}\boldsymbol{A}_{kj} \right\} = 0. \tag{13}$$

Now consider the matrix $\boldsymbol{A}$ with all its entries zero except for the i^{th} row, which is all ones, and $\boldsymbol{B}$, which has all its entries zero, except for the j^{th} column, which is all ones. If $i \neq j$, then the i, j entry of $\boldsymbol{AB}$ is m and the rest are zero, whereas all the entries of $\boldsymbol{BA}$ are zero. In this case, (13) implies $\boldsymbol{L}_{ij} = 0$.

Next consider the matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ where the nonzero entries of $\boldsymbol{A}$ are rows i and j, which consist of ones; and the nonzero entries of $\boldsymbol{B}$ are column i, which consists of ones, and column j, which is column of minus ones. Then $\boldsymbol{BA} = 0$ and $\boldsymbol{AB}$ is zero except for $(\boldsymbol{AB})_{ij} = (\boldsymbol{AB})_{ji} = m$ and $(\boldsymbol{AB})_{ij} = (\boldsymbol{AB})_{jj} = -m$. Since $\boldsymbol{L}_{ij} = 0$ whenever $i \neq j$, equation (13) reduces to $\boldsymbol{L}_{ii}m + \boldsymbol{L}_{jj}(-m) = 0$, which implies $\boldsymbol{L}_{ii} = \boldsymbol{L}_{jj}$.

Let α be the common value of the elements of the diagonal matrix $\boldsymbol{L}$. We have just shown that $\ell(\boldsymbol{A}) = \alpha \operatorname{tr} \boldsymbol{A}$. ∎

Add: The trace is also equal to the sum of the characteristic roots (eigenvalues).

103 Proposition *The trace of a matrix depends only on the linear transformation of* $\boldsymbol{R}^{\mathrm{m}}$ *into* $\boldsymbol{R}^{\mathrm{m}}$ *that it represents. In other words, if* $\boldsymbol{A}$ *and* $\boldsymbol{B}$ *are similar matrices, that is, if* $\boldsymbol{B} = \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C}$, *then* $\operatorname{tr} \boldsymbol{B} = \operatorname{tr} \boldsymbol{A}$.

Proof: Theorem 94 asserts that two matrices represent the same transformation if and only if they are similar. By Lemma 101, equation (12),

$$\operatorname{tr} \boldsymbol{B} = \operatorname{tr} \boldsymbol{C}^{-1}\boldsymbol{A}\boldsymbol{C} = \operatorname{tr} \boldsymbol{A}\boldsymbol{C}\boldsymbol{C}^{-1} = \operatorname{tr} \boldsymbol{A}.$$

∎

104 Corollary *Let* V *be an* m*-dimensional inner product space. There is a unique linear functional* tr *on* $\mathsf{L}(V, V)$ *satisfying*

$$\operatorname{tr} ST = \operatorname{tr} TS \quad \text{for all } S, T \in \mathsf{L}(V, V),$$

and

$$\operatorname{tr} I = m.$$

105 Theorem *If* $\boldsymbol{A}$ *is symmetric and idempotent, then* $\operatorname{tr} \boldsymbol{A} = \operatorname{rank} \boldsymbol{A}$.

Proof: Since $\boldsymbol{A}$ is symmetric, $\boldsymbol{A} = \boldsymbol{X}\boldsymbol{B}\boldsymbol{X}^{-1}$ where $\boldsymbol{X} = [\boldsymbol{x}_1, \dots, \boldsymbol{x}_m]$ is an orthogonal matrix whose columns are eigenvectors of $\boldsymbol{A}$, and $\boldsymbol{B}$ is a diagonal matrix whose diagonal elements the eigenvalues of $\boldsymbol{A}$, which are either are 0 or 1.

Thus $\operatorname{tr} \boldsymbol{B}$ is the number of nonzero eigenvalues of $\boldsymbol{A}$. Also $\operatorname{rank} \boldsymbol{B}$ is the number of nonzero diagonal elements. Thus $\operatorname{tr} \boldsymbol{B} = \operatorname{rank} \boldsymbol{B}$, but since $\boldsymbol{A}$ and $\boldsymbol{B}$ are similar, $\operatorname{tr} \boldsymbol{A} = \operatorname{tr} \boldsymbol{B} = \operatorname{rank} \boldsymbol{B} = \operatorname{rank} \boldsymbol{A}$. ∎

It also follows that on the space of symmetric matrices, the trace can be used to define an inner product.

106 Proposition *The function of two matrices*

$$(\boldsymbol{A}, \boldsymbol{B}) = \operatorname{tr} \boldsymbol{A}\boldsymbol{B}$$

is an inner product on the linear space of symmetric $m \times m$ *real matrices.*

Proof: Lemma 101, equation (12) shows that $(\boldsymbol{A}, \boldsymbol{B}) = (\boldsymbol{B}, \boldsymbol{A})$ so **IP.1** is satisfied. Moreover equation (11) implies

$$\begin{aligned}
(\boldsymbol{A}, \boldsymbol{B} + \boldsymbol{C}) = \operatorname{tr} \boldsymbol{A}(\boldsymbol{B} + \boldsymbol{C}) = \operatorname{tr}(\boldsymbol{A}\boldsymbol{B} + \boldsymbol{A}\boldsymbol{C}) = \operatorname{tr} \boldsymbol{A}\boldsymbol{B} + \operatorname{tr} \boldsymbol{A}\boldsymbol{C} = (\boldsymbol{A}, \boldsymbol{B}) + (\boldsymbol{A}, \boldsymbol{C}),\\
(\alpha\boldsymbol{A}, \boldsymbol{B}) = \operatorname{tr} \alpha\boldsymbol{A}\boldsymbol{B} = \alpha \operatorname{tr} \boldsymbol{A}\boldsymbol{B} = \alpha(\boldsymbol{A}, \boldsymbol{B})\\
(\boldsymbol{A}, \alpha\boldsymbol{B}) = \operatorname{tr} \boldsymbol{A}\alpha\boldsymbol{B} = \alpha \operatorname{tr} \boldsymbol{A}\boldsymbol{B} = \alpha(\boldsymbol{A}, \boldsymbol{B})
\end{aligned}$$

so **IP.2** and **IP.3** are satisfied.

To see that **IP.4** is satisfied, observe that if $\boldsymbol{A}$ is a symmetric matrix, then $(\boldsymbol{A}\boldsymbol{A})_{ii}$ is just the inner product of the the i^{th} row of $\boldsymbol{A}$ with itself, which is $\geqslant 0$ and equals zero only if the row is zero. Thus $(\boldsymbol{A}, \boldsymbol{A}) = \operatorname{tr} \boldsymbol{A}\boldsymbol{A} = \sum_i (\boldsymbol{A}\boldsymbol{A})_{ii} \geqslant 0$ and $= 0$ only if every row of $\boldsymbol{A}$ is zero, that is, if $\boldsymbol{A}$ itself is zero. ∎

107 Exercise What does it mean for symmetric matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ to be orthogonal under this inner product? □

10.10 Matrices and orthogonal projection

Section 5.4 discussed orthogonal projection as a linear transformation. In this section we discuss matrix representations for orthogonal projection.

Let M be a k-dimensional subspace of $\boldsymbol{R}^{\mathrm{m}}$, and let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$ be a basis for M. Given a vector $\boldsymbol{y}$, the orthogonal projection $\boldsymbol{y}_M$ of $\boldsymbol{y}$ is the vector in M that minimizes the distance to $\boldsymbol{y}$ (Proposition 42). The difference $\boldsymbol{y}_\perp = \boldsymbol{y} - \boldsymbol{y}_M$ is orthogonal to M (Theorem 39).

The next result is crucial to the statistical analysis of linear regression models.

108 Least squares regression *Let $\boldsymbol{B}$ the $m \times k$ matrix with columns $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$, which constitute a basis for the k-dimensional subspace M. Given a vector $\boldsymbol{y}$ in $\boldsymbol{R}^{\mathrm{m}}$, the orthogonal projection $\boldsymbol{y}_M$ of $\boldsymbol{y}$ onto M satisfies*

$$\boldsymbol{y}_M = \boldsymbol{B}(\boldsymbol{B}'\boldsymbol{B})^{-1}\boldsymbol{B}'\boldsymbol{y}.$$

Proof: The first thing to note is that since $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k\}$ is a basis for M, the matrix $\boldsymbol{B}$ has rank k, so by Corollary 62, the $k \times k$ matrix $\boldsymbol{B}'\boldsymbol{B}$ has rank k, so by Proposition 86 it is invertible.

Next note that the $m \times 1$ column vector $\boldsymbol{B}(\boldsymbol{B}'\boldsymbol{B})^{-1}\boldsymbol{B}'\boldsymbol{y}$ belongs to M. In fact, setting

$$\boldsymbol{a} = (\boldsymbol{B}'\boldsymbol{B})^{-1}\boldsymbol{B}'\boldsymbol{y}$$

($\boldsymbol{a}$ is a $k \times 1$ column matrix), we see that it is the linear combination

$$\boldsymbol{B}\boldsymbol{a} = \sum_{j=1}^{k} \alpha_j \boldsymbol{b}_j$$

of basis vectors. Thus by the Orthogonal Projection Theorem 39, to show that $\boldsymbol{y}_M = \boldsymbol{B}\boldsymbol{a}$, it suffices to show that $\boldsymbol{y} - \boldsymbol{B}\boldsymbol{a}$ is orthogonal to M. This in turn is equivalent to $\boldsymbol{y} - \boldsymbol{B}\boldsymbol{a}$ being orthogonal to each basis vector $\boldsymbol{b}_j$. Now for any $\boldsymbol{x}$, the $k \times 1$ column matrix $\boldsymbol{B}'\boldsymbol{x}$ has as its j^{th} (row) entry the dot product $\boldsymbol{b}_j \cdot \boldsymbol{x}$. Thus all we need do is show that $\boldsymbol{B}'(\boldsymbol{y} - \boldsymbol{B}\boldsymbol{a}) = \boldsymbol{0}$. To this end, compute

$$\boldsymbol{B}'(\boldsymbol{y} - \boldsymbol{B}\boldsymbol{a}) = \boldsymbol{B}'\boldsymbol{y} - \boldsymbol{B}'\boldsymbol{B}(\boldsymbol{B}'\boldsymbol{B})^{-1}\boldsymbol{B}'\boldsymbol{y} = \boldsymbol{B}'\boldsymbol{y} - \boldsymbol{B}'\boldsymbol{y} = \boldsymbol{0}.$$

∎

A perhaps more familiar way to restate this result is that the vector $\boldsymbol{a}$ of coefficients that minimizes the sum of squared residuals, $(\boldsymbol{y} - \boldsymbol{B}\boldsymbol{a}) \cdot (\boldsymbol{y} - \boldsymbol{B}\boldsymbol{a})$, is given by $\boldsymbol{a} = (\boldsymbol{B}'\boldsymbol{B})^{-1}\boldsymbol{B}'\boldsymbol{y}$.

11 Quadratic forms

We introduced quadratic forms in the proof of Theorem 78. We go a little deeper here. If you want to know even more, I recommend my on-line notes [9].

Let $\boldsymbol{A}$ be an $n \times n$ symmetric matrix, and let $\boldsymbol{x}$ be an n-vector. Then $\boldsymbol{x} \cdot \boldsymbol{A}\boldsymbol{x}$ is a scalar, and

$$\boldsymbol{x} \cdot \boldsymbol{A}\boldsymbol{x} = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} x_i x_j. \tag{14}$$

(We may also write this as $\boldsymbol{x}'\boldsymbol{A}\boldsymbol{x}$ in matrix notation.)

The mapping $Q\colon \boldsymbol{x} \mapsto \boldsymbol{x} \cdot \boldsymbol{A}\boldsymbol{x}$ is the **quadratic form** defined by $\boldsymbol{A}$.[6]

109 Definition *A symmetric matrix $\boldsymbol{A}$ (or its associated quadratic form) is called*

- ***positive definite*** *if $\boldsymbol{x}'\boldsymbol{A}\boldsymbol{x} > 0$ for all nonzero $\boldsymbol{x}$.*
- ***negative definite*** *if $\boldsymbol{x}'\boldsymbol{A}\boldsymbol{x} < 0$ for all nonzero $\boldsymbol{x}$.*
- ***positive semidefinite*** *if $\boldsymbol{x}'\boldsymbol{A}\boldsymbol{x} \geqslant 0$ for all $\boldsymbol{x}$.*
- ***negative semidefinite*** *if $\boldsymbol{x}'\boldsymbol{A}\boldsymbol{x} \leqslant 0$ for all $\boldsymbol{x}$.*

We want all our (semi)definite matrices to be symmetric so that their eigenvectors generate an orthonormal basis for $\boldsymbol{R}^{\mathrm{n}}$. (If $\boldsymbol{A}$ is not symmetric, then $\frac{\boldsymbol{A}+\boldsymbol{A}'}{2}$ is symmetric and $\boldsymbol{x}'\boldsymbol{A}\boldsymbol{x} = \boldsymbol{x}'(\frac{\boldsymbol{A}+\boldsymbol{A}'}{2})\boldsymbol{x}$ for any $\boldsymbol{x}$.) Some authors use the term **quasi-(semi)definite** when they do not wish to impose symmetry.

11.1 Diagonalization of quadratic forms

By the Principal Axis Theorem 98 we may write

$$\boldsymbol{A} = \boldsymbol{X}\boldsymbol{\Lambda}\boldsymbol{X}',$$

where $\boldsymbol{X}$ is an orthogonal matrix with columns that are eigenvectors of $\boldsymbol{A}$, and $\boldsymbol{\Lambda}$ is a diagonal matrix of eigenvalues of $\boldsymbol{A}$. Then the quadratic form can be written in terms of the diagonal matrix $\boldsymbol{\Lambda}$:

$$\boldsymbol{x} \cdot \boldsymbol{A}\boldsymbol{x} = \boldsymbol{x}'\boldsymbol{A}\boldsymbol{x} = \boldsymbol{x}'\boldsymbol{X}\boldsymbol{\Lambda}\boldsymbol{X}'\boldsymbol{x} = \boldsymbol{y}'\boldsymbol{\Lambda}\boldsymbol{y} = \sum_{i=1}^{n} \lambda_i y_i^2,$$

where

$$\boldsymbol{y} = \boldsymbol{X}'\boldsymbol{x}.$$

110 Proposition (Eigenvalues and definiteness) *The symmetric matrix $\boldsymbol{A}$ is*

1. *positive definite if and only if all its eigenvalues are strictly positive.*
2. *negative definite if and only if all its eigenvalues are strictly negative.*
3. *positive semidefinite if and only if all its eigenvalues are nonnegative.*
4. *negative semidefinite if and only if all its eigenvalues are nonpositive.*

[6] For decades I was baffled by the term *form*. I once asked Tom Apostol at a faculty cocktail party what it meant. He professed not to know (it was a cocktail party, so that is excusable), but suggested that I should ask John Todd. He hypothesized that mathematicians don't know the difference between form and function, a clever reference to modern architectural philosophy. I was too intimidated by Todd to ask, but I subsequently learned (where, I can't recall) that *form* refers to a polynomial function in several variables where each term in the polynomial has the same degree. (The *degree* of the term is the sum of the exponents. For example, in the expression $xyz + x^2y + xz + z$, the first two terms have degree three, the third term has degree two and the last one has degree one. It is thus not a form.) This is most often encountered in the phrases *linear form* (each term has degree one) or *quadratic form* (each term has degree two).

Proof: As above, let $\boldsymbol{y} = \boldsymbol{X}'\boldsymbol{x}$ and write

$$\boldsymbol{x}'\boldsymbol{A}\boldsymbol{x} = \sum_{i=1}^{n} \lambda_i y_i^2.$$

where the λ_i's are the eigenvalues of $\boldsymbol{A}$. All the statements above follow from this equation and the fact that $y_i^2 \geqslant 0$ for all k. ∎

111 Proposition (Definiteness of the inverse) *If $\boldsymbol{A}$ is positive definite (negative definite), then $\boldsymbol{A}^{-1}$ exists and is also positive definite (negative definite).*

Proof: First off, how do we know the inverse of $\boldsymbol{A}$ exists? Suppose $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$. Then $\boldsymbol{x} \cdot \boldsymbol{A}\boldsymbol{x} = \boldsymbol{x} \cdot \boldsymbol{0} = 0$. Since $\boldsymbol{A}$ is positive definite, we see that $\boldsymbol{x} = \boldsymbol{0}$. Therefore $\boldsymbol{A}$ is invertible. Here are two proofs of the proposition.

First proof. Since $(\boldsymbol{A}\boldsymbol{x} = \lambda\boldsymbol{x}) \implies (\boldsymbol{x} = \lambda\boldsymbol{A}^{-1}\boldsymbol{x}) \implies (\boldsymbol{A}^{-1}\boldsymbol{x} = \frac{1}{\lambda}\boldsymbol{x})$, the eigenvalues of $\boldsymbol{A}$ and $\boldsymbol{A}^{-1}$ are reciprocals, so they must have the same sign. Apply Proposition 110.

Second proof.

$$\boldsymbol{x}'\boldsymbol{A}^{-1}\boldsymbol{x} = \boldsymbol{y}'\boldsymbol{A}\boldsymbol{y} \quad \text{where} \quad \boldsymbol{y} = \boldsymbol{A}^{-1}\boldsymbol{x}.$$

∎

12 Determinants

The main quick references here are Apostol [6, Chapter 3] and Dieudonné [11, Appendix A.6]. The main things to remember are:

- The determinant assigns a number to each square matrix $\boldsymbol{A}$, denoted either $\det \boldsymbol{A}$ or $\left|\boldsymbol{A}\right|$. A matrix is **singular** if its determinant is zero, otherwise it is **nonsingular**. For an $n \times n$ identity matrix, $\det \boldsymbol{I} = 1$.
- $\det(\boldsymbol{A}\boldsymbol{B}) = \det \boldsymbol{A} \cdot \det \boldsymbol{B}$.
- A square matrix has an inverse if and only if its determinant is nonzero.
- Multiplying a row or a column by a scalar multiplies the determinant by the same amount. Consequently for an $n \times n$ matrix $\boldsymbol{A}$,

$$\det(-\boldsymbol{A}) = (-1)^n \det \boldsymbol{A}.$$

- Also consequently, the determinant of a diagonal matrix is the product of its diagonal elements.
- Adding a multiple of one row to another does not change the determinant.
- Consequently, the determinant of an upper (or lower) triangular matrix is the product of its diagonal.

- Moreover if a square matrix $\boldsymbol{A}$ is block upper triangular, that is, of the form

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{B} & \boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{D} \end{bmatrix},$$

  where $\boldsymbol{B}$ and $\boldsymbol{D}$ are square, then $\det \boldsymbol{A} = \det \boldsymbol{B} \cdot \det \boldsymbol{D}$. Likewise for block lower triangular matrices.

- $\det \boldsymbol{A} = \det \boldsymbol{A}'$.

- The determinant can be defined recursively in terms of minors (determinants of submatrices).

- The inverse of a matrix can be computed in terms of these minors. The inverse of $\boldsymbol{A}$ is the transpose of its cofactor matrix divided by $\det \boldsymbol{A}$.

- **Cramer's Rule**: If $\boldsymbol{Ax} = \boldsymbol{b}$ for a nonsingular matrix $\boldsymbol{A}$, then

$$x_i = \frac{\left|\boldsymbol{A}^1, \dots, \boldsymbol{A}^{i-1}, \boldsymbol{b}, \boldsymbol{A}^{i+1}, \dots, \boldsymbol{A}^n\right|}{\left|\boldsymbol{A}\right|}.$$

- The determinant is the "oriented volume" of the n-dimensional "cube" formed by its columns.

- The determinant $\det(\lambda \boldsymbol{I} - \boldsymbol{A})$, where $\boldsymbol{A}$ and $\boldsymbol{I}$ are $n \times n$, is an n^{th} degree polynomial in λ, called the **characteristic polynomial** of $\boldsymbol{A}$.

- A root (real or complex) of the characteristic polynomial of $\boldsymbol{A}$ is called a **characteristic root** of $\boldsymbol{A}$. Characteristic roots that are real are also eigenvalues. If nonzero $\boldsymbol{x}$ belongs to the null space of $\lambda \boldsymbol{I} - \boldsymbol{A}$, then it is an eigenvector corresponding to the eigenvalue λ.

- The determinant of $\boldsymbol{A}$ is the product of its characteristic roots.

- If $\boldsymbol{A}$ is symmetric, then $\det \boldsymbol{A}$ is the product of its eigenvalues.

- If $\boldsymbol{A}$ has rank k then every minor of size greater than k has zero determinant and there is at least one minor of order k with nonzero determinant.

- The determinant of an orthogonal matrix is ± 1.

12.1 Determinants as multilinear forms

There are several ways to think about determinants. Perhaps the most useful is as an alternating multilinear n-form:

A function $\varphi \colon \underbrace{\boldsymbol{R}^{\mathrm{n}} \times \cdots \times \boldsymbol{R}^{\mathrm{n}}}_{n \text{ copies}} \to \boldsymbol{R}$ is **multilinear** if it is linear in each variable separately. That is, for each $i = 1, \dots, n$,

$$\begin{aligned}\varphi(&\boldsymbol{x}_1, \dots, \boldsymbol{x}_{i-1}, \alpha \boldsymbol{x}_i + \beta \boldsymbol{y}_i, \boldsymbol{x}_{i+1}, \dots, \boldsymbol{x}_n) \\ &= \alpha \varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{i-1}, \boldsymbol{x}_i, \boldsymbol{x}_{i+1}, \dots, \boldsymbol{x}_n) + \beta \varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{i-1}, \boldsymbol{y}_i, \boldsymbol{x}_{i+1}, \dots, \boldsymbol{x}_n).\end{aligned}$$

A consequence of this is that if any $\boldsymbol{x}_i$ is the zero vector, then so is φ. That is,

$$\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{i-1}, \boldsymbol{0}, \boldsymbol{x}_{i+1}, \dots, \boldsymbol{x}_n) = 0.$$

The multilinear function φ is **alternating** if $\boldsymbol{x}_i = \boldsymbol{x}_j = \boldsymbol{z}$ for distinct i and j, then

$$\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{z}, \dots, \boldsymbol{z}, \dots, \boldsymbol{x}_n) = 0.$$

The reason for this terminology is the following lemma.

112 Lemma *The multilinear function φ is alternating if and only if interchanging $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$ changes the sign of φ, that is,*

$$\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_n) = -\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_n).$$

Proof: Suppose first that φ is alternating. Then

$$\begin{aligned}
0 &= \varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_i + \boldsymbol{x}_j, \dots, \boldsymbol{x}_j + \boldsymbol{x}_i, \dots, \boldsymbol{x}_n) \\
&= \varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_j + \boldsymbol{x}_i, \dots, \boldsymbol{x}_n) + \varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_j + \boldsymbol{x}_i, \dots, \boldsymbol{x}_n) \\
&= \varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_n) + \underbrace{\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_n)}_{=0} \\
&\quad + \underbrace{\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_n)}_{=0} + \varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_n) \\
&= \varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_n) + \varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_n).
\end{aligned}$$

So $\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_n) = -\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{x}_j, \dots, \boldsymbol{x}_i, \dots, \boldsymbol{x}_n)$.

Now suppose interchanging $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$ changes the sign of φ. Then if $\boldsymbol{x}_i = \boldsymbol{x}_j = \boldsymbol{z}$,

$$\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{z}, \dots, \boldsymbol{z}, \dots, \boldsymbol{x}_n) = -\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{z}, \dots, \boldsymbol{z}, \dots, \boldsymbol{x}_n),$$

which implies $\varphi(\boldsymbol{x}_1, \dots, \boldsymbol{z}, \dots, \boldsymbol{z}, \dots, \boldsymbol{x}_n) = 0$, so φ is alternating. ∎

There is an obvious identification of $n \times n$ square matrices with the elements of $\boldsymbol{R}^{\mathrm{n}} \times \cdots \times \boldsymbol{R}^{\mathrm{n}}$. Namely $\boldsymbol{A} \leftrightarrow (\boldsymbol{A}^1, \dots, \boldsymbol{A}^n)$, where you will recall $\boldsymbol{A}^j$ denotes the j^{th} column of $\boldsymbol{A}$ interpreted as a vector in $\boldsymbol{R}^{\mathrm{n}}$. (We could have used rows just as well.) *Henceforth, for a multilinear form φ and $n \times n$ matrix $\boldsymbol{A}$, we write $\varphi(\boldsymbol{A})$ for $\varphi(\boldsymbol{A}^1, \dots, \boldsymbol{A}^n)$.* The next fact is rather remarkable, so pay close attention.

113 Proposition *For every $n \times n$ matrix $\boldsymbol{A}$, there is a number* $\det \boldsymbol{A}$ *with the property that for any alternating multilinear n-form φ,*

$$\varphi(\boldsymbol{A}) = \det \boldsymbol{A} \cdot \varphi(\boldsymbol{I}). \tag{$\star$}$$

Proof: Before we demonstrate the proposition in general, let us start with a special case, $n = 2$. Let

$$\boldsymbol{A} = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,1} & \alpha_{2,2} \end{bmatrix}.$$

Then

$$\begin{aligned}
\varphi(\boldsymbol{A}) &= \varphi(\boldsymbol{A}^1, \boldsymbol{A}^2) \\
&= \varphi(\alpha_{1,1}\boldsymbol{e}_1 + \alpha_{2,1}\boldsymbol{e}_2, \alpha_{1,2}\boldsymbol{e}_1 + \alpha_{2,2}\boldsymbol{e}_2) \\
&= \alpha_{1,1}\varphi(\boldsymbol{e}_1, \alpha_{1,2}\boldsymbol{e}_1 + \alpha_{2,2}\boldsymbol{e}_2) + \alpha_{2,1}\varphi(\boldsymbol{e}_2, \alpha_{1,2}\boldsymbol{e}_1 + \alpha_{2,2}\boldsymbol{e}_2) \\
&= \alpha_{1,1}\alpha_{1,2}\varphi(\boldsymbol{e}_1, \boldsymbol{e}_1) + \alpha_{1,1}\alpha_{2,2}\varphi(\boldsymbol{e}_1, \boldsymbol{e}_2) + \alpha_{2,1}\alpha_{1,2}\varphi(\boldsymbol{e}_2, \boldsymbol{e}_1) + \alpha_{2,1}\alpha_{2,2}\varphi(\boldsymbol{e}_2, \boldsymbol{e}_2) \\
&= 0 + \alpha_{1,1}\alpha_{2,2}\varphi(\boldsymbol{e}_1, \boldsymbol{e}_2) + \alpha_{2,1}\alpha_{1,2}\varphi(\boldsymbol{e}_2, \boldsymbol{e}_1) + 0 \\
&= \alpha_{1,1}\alpha_{2,2}\varphi(\boldsymbol{e}_1, \boldsymbol{e}_2) - \alpha_{2,1}\alpha_{1,2}\varphi(\boldsymbol{e}_1, \boldsymbol{e}_2) \\
&= (\alpha_{1,1}\alpha_{2,2} - \alpha_{2,1}\alpha_{1,2})\varphi(\boldsymbol{I}),
\end{aligned}$$

so we see that $\det \boldsymbol{A} = \alpha_{1,1}\alpha_{2,2} - \alpha_{2,1}\alpha_{1,2}$. Thus the whole of φ is determined by the single number $\varphi(\boldsymbol{I})$.

This is true more generally. Write

$$\varphi(\boldsymbol{A}) = \varphi\left(\sum_{i_1=1}^{n} \alpha_{i_1,1}\boldsymbol{e}_{i_1}, \sum_{i_2=1}^{n} \alpha_{i_2,2}\boldsymbol{e}_{i_2}, \dots, \sum_{i_j=1}^{n} \alpha_{i_j,j}\boldsymbol{e}_{i_j}, \dots, \sum_{i_n=1}^{n} \alpha_{i_n,n}\boldsymbol{e}_{i_n}\right).$$

Now expand this using linearity in the first component:

$$\varphi(\boldsymbol{A}) = \sum_{i_1=1}^{n} \alpha_{i_1,1}\varphi\left(\boldsymbol{e}_{i_1}, \sum_{i_2=1}^{n} \alpha_{i_2,2}\boldsymbol{e}_{i_2}, \dots, \sum_{i_j=1}^{n} \alpha_{i_j,j}\boldsymbol{e}_{i_j}, \dots, \sum_{i_n=1}^{n} \alpha_{i_n,n}\boldsymbol{e}_{i_n}\right).$$

Repeating this for the other components leads to

$$\varphi(\boldsymbol{A}) = \sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n} \alpha_{i_1,1}\alpha_{i_2,2}\cdots\alpha_{i_n,n}\varphi(\boldsymbol{e}_{i_1}, \boldsymbol{e}_{i_2}, \dots, \boldsymbol{e}_{i_n}).$$

Now consider $\varphi(\boldsymbol{e}_{i_1}, \boldsymbol{e}_{i_2}, \dots, \boldsymbol{e}_{i_n})$. Since φ is alternating, this term is zero unless $i_1, i_2, \dots, i_n$ are distinct. When these are distinct, then by switching pairs we get to $\pm\varphi(\boldsymbol{e}_1, \boldsymbol{e}_2, \dots, \boldsymbol{e}_n)$ where the sign on whether we need an odd or an even number of switches. It now pays to introduce some new terminology and notation. A **permutation** $\boldsymbol{i}$ is an ordered list $\boldsymbol{i} = (i_1, \dots, i_n)$ of the numbers $1, \dots, n$. The **signature** $\operatorname{sgn}(\boldsymbol{i})$ of $\boldsymbol{i}$ is 1 if $\boldsymbol{i}$ can be put in numerical order by switching terms an even number of times and is -1 if it requires an odd number. It follows then that defining

How do we know that $\operatorname{sgn}(\boldsymbol{i})$ is well defined?

$$\det \boldsymbol{A} = \sum_{\boldsymbol{i}} \operatorname{sgn}(\boldsymbol{i}) \cdot \alpha_{i_1,1}\alpha_{i_2,2}\cdots\alpha_{i_n,n}, \tag{15}$$

where the sum runs over all permutations $\boldsymbol{i}$, satisfies the conclusion of the proposition. ∎

This result still leaves the following question: *Are there any alternating multilinear n-forms at all?* The reason the result above does not settle this is that it would be vacuously true if there were none. Fortunately, it is not hard to verify that det itself is such an n-form.

114 Proposition *The function $\boldsymbol{A} \mapsto \det \boldsymbol{A}$ as defined in (15) is an alternating multilinear n-form.*

Proof: Observe that in each product $\operatorname{sgn}(\boldsymbol{i}) \cdot \alpha_{i_1,1}\alpha_{i_2,2}\cdots\alpha_{i_n,n}$ in the sum in (15) there is exactly one element from each row and each column of $\boldsymbol{A}$. This makes it obvious that $\det(\boldsymbol{A}^1,\dots,\alpha\boldsymbol{A}^j,\dots,\boldsymbol{A}^n) = \alpha\det\boldsymbol{A}$, and it is straightforward to verify that

$$\det(\boldsymbol{A}^1,\dots,\boldsymbol{x}+y,\dots,\boldsymbol{A}^n) = \det(\boldsymbol{A}^1,\dots,\boldsymbol{x},\dots,\boldsymbol{A}^n) + \det(\boldsymbol{A}^1,\dots,y,\dots,\boldsymbol{A}^n).$$

To see that det is alternating, suppose $\boldsymbol{A}^i = \boldsymbol{A}^j$ with $i \neq j$. Then for any permutation $\boldsymbol{i}$, $i_j \neq i_k$, and there is exactly one permutation $\boldsymbol{i}'$ satisfying $i_p = i'_p$ for $p \notin \{i,j\}$ and $i'_j = i_k$ and $i'_k = i_j$. Now observe that $\operatorname{sgn}(\boldsymbol{i}) = -\operatorname{sgn}(\boldsymbol{i}')$ as it requires an odd number of interchanges to swap two elements in a list (why?). Thus we can rewrite (15) as

$$\det\boldsymbol{A} = \sum_{\boldsymbol{i}:\operatorname{sgn}(\boldsymbol{i})=1} \alpha_{i_1,1}\alpha_{i_2,2}\cdots\alpha_{i_n,n} - \alpha_{i'_1,1}\alpha_{i'_2,2}\cdots\alpha_{i'_n,n},$$

but each $\alpha_{i_1,1}\alpha_{i_2,2}\cdots\alpha_{i_n,n} - \alpha_{i'_1,1}\alpha_{i'_2,2}\cdots\alpha_{i'_n,n} = 0$. (Why?) Therefore $\det\boldsymbol{A} = 0$, so det is alternating. ∎

To sum things up we have:

115 Corollary *An alternating multilinear n-form is identically zero if and only if $\varphi(\boldsymbol{I}) = 0$. The determinant is the unique alternating multilinear n-form φ that satisfies $\varphi(\boldsymbol{I}) = 1$. Any other alternating multilinear n-form φ is of the form $\varphi = \varphi(\boldsymbol{I}) \cdot \det$.*

12.2 Some simple consequences

116 Proposition *If $\boldsymbol{A}'$ is the transpose of $\boldsymbol{A}$, then $\det\boldsymbol{A} = \det\boldsymbol{A}'$.*

Write out a proof.

117 Proposition *Adding a scalar multiple of one column of $\boldsymbol{A}$ to a different column leaves the determinant unchanged. Likewise for rows.*

Proof: By multilinearity,

$$\begin{aligned}\det(\boldsymbol{A}^1,\dots,\boldsymbol{A}^j+\alpha\boldsymbol{A}^k,\dots,\boldsymbol{A}^k,\dots,\boldsymbol{A}^n) &= \\ \det(\boldsymbol{A}^1,\dots,\boldsymbol{A}^j,\dots,\boldsymbol{A}^k,\dots,\boldsymbol{A}^n) &+ \alpha\det(\boldsymbol{A}^1,\dots,\boldsymbol{A}^k,\dots,\boldsymbol{A}^k,\dots,\boldsymbol{A}^n),\end{aligned}$$

but

$$\det(\boldsymbol{A}^1,\dots,\boldsymbol{A}^k,\dots,\boldsymbol{A}^k,\dots,\boldsymbol{A}^n) = 0$$

since det is alternating. The conclusion for rows follows from that for columns and Proposition 116 on transposes. ∎

118 Proposition *The determinant of an upper triangular matrix is the product of the diagonal entries.*

Proof: Recall that an upper triangular matrix is one for which $i > j$ implies $\alpha_{i,j} = 0$. (Diagonal matrices are also upper triangular.) Now examine equation (15). The only summand that is nonzero comes from the permutation $(1,2,3,\dots,n)$, since for any other permutation there is some j satisfying $i_j > j$. (Why?) ∎

By the way, the result also holds for lower triangular matrices.

119 Lemma *If* $\boldsymbol{A}$ *is* $n \times n$ *and* φ *is an alternating multilinear* n*-form, so is the form* φ_A *defined by*

$$\varphi_A(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = \varphi(\boldsymbol{A}\boldsymbol{x}_1, \ldots, \boldsymbol{A}\boldsymbol{x}_n).$$

Furthermore

$$\varphi_A(\boldsymbol{I}) = \varphi(\boldsymbol{A}) = \det \boldsymbol{A} \cdot \varphi(\boldsymbol{I}). \tag{16}$$

Proof: That φ_A is an alternating multilinear n-form is straightforward. Therefore φ_A is proportional to φ. To see that the coefficient of proportionality is $\det \boldsymbol{A}$, consider $\varphi_A(\boldsymbol{I})$. Direct computation shows that $\varphi_A(\boldsymbol{I}) = \varphi(\boldsymbol{A})$. ∎

As an aside, I mention that we could have defined the determinant directly for linear transformations as follows. For a linear transformation $T \colon \boldsymbol{R}^{\mathrm{n}} \to \boldsymbol{R}^{\mathrm{n}}$ it follows that φ_T defined by $\varphi_T(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = \varphi(T\boldsymbol{x}_1, \ldots, T\boldsymbol{x}_n)$ is an alternating n-form whenever φ is. It also follows that we could use (16) to define $\det T$ to be the scalar satisfying $\varphi_T(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = \det T \cdot \varphi(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$. This is precisely Dieudonné's approach. It has the drawback that minors and cofactors are awkward to describe in his framework.

120 Theorem *Let* $\boldsymbol{A}$ *and* $\boldsymbol{B}$ *be* $n \times n$ *matrices. Then*

$$\det \boldsymbol{A}\boldsymbol{B} = \det \boldsymbol{A} \cdot \det \boldsymbol{B}.$$

Proof: Let φ be an alternating multilinear n-form. Applying (16) and ($\star$), we see

$$\varphi_{AB}(\boldsymbol{I}) = \varphi(\boldsymbol{A}\boldsymbol{B}) = \det \boldsymbol{A}\boldsymbol{B} \cdot \varphi(\boldsymbol{I}).$$

On the other hand

$$\varphi_{\boldsymbol{AB}}(\boldsymbol{I}) = \varphi_A(\boldsymbol{B}) = \det \boldsymbol{B} \cdot \varphi_A(\boldsymbol{I}) = \det \boldsymbol{B} \cdot \det \boldsymbol{A} \cdot \varphi(\boldsymbol{I}).$$

Therefore $\det \boldsymbol{A}\boldsymbol{B} = \det \boldsymbol{A} \cdot \det \boldsymbol{B}$. ∎

121 Corollary *If* $\det \boldsymbol{A} = 0$*, then* $\boldsymbol{A}$ *has no inverse.*

Proof: Observe that if $\boldsymbol{A}$ has an inverse, then

$$1 = \det \boldsymbol{I} = \det \boldsymbol{A} \cdot \det \boldsymbol{A}^{-1}$$

so $\det \boldsymbol{A} \neq 0$. ∎

122 Corollary *The determinant of an orthogonal matrix is* ± 1.

Proof: Recall that the matrix $\boldsymbol{A}$ is orthogonal if $\boldsymbol{A}'\boldsymbol{A} = \boldsymbol{I}$ (Definition 97). So by Theorem 120, $\det(\boldsymbol{A}') \det(\boldsymbol{A}) = 1$, but by Proposition 116, $\det(\boldsymbol{A}') = \det \boldsymbol{A}$, so $(\det \boldsymbol{A})^2 = 1$. ∎

12.3 Minors and cofactors

Different authors assign different meanings to the term **minor**. Given a square $n \times n$ matrix

$$\boldsymbol{A} = \begin{bmatrix} \alpha_{1,1} & \dots & \alpha_{1,n} \\ \vdots & & \vdots \\ \alpha_{n,1} & \dots & \alpha_{n,n} \end{bmatrix}$$

Apostol [6, p. 87] defines the i,j **minor** of $\boldsymbol{A}$ to be the $(n-1)\times(n-1)$ *submatrix* obtained from $\boldsymbol{A}$ by deleting the i^{th} row and j^{th} column, and denotes it $\boldsymbol{A}_{i,j}$. Gantmacher [13, p. 2] defines a **minor** of a (not necessarily square) matrix $\boldsymbol{A}$ to be the *determinant* of a square submatrix of $\boldsymbol{A}$, and uses the following notation for minors in terms of the remaining rows and columns:

$$\boldsymbol{A}\binom{i_1,\dots,i_p}{j_1,\dots,j_p} = \begin{vmatrix} \alpha_{i_1,j_1} & \dots & \alpha_{i_1,j_p} \\ \vdots & & \vdots \\ \alpha_{i_n,j_1} & \dots & \alpha_{i_p,j_p} \end{vmatrix}.$$

Here we require that $1 \leqslant i_1 < i_2 < \cdots < i_p \leqslant n$ and $1 \leqslant j_1 < j_2 < \cdots < j_p \leqslant n$. If the deleted (and hence remaining) rows and columns are the same, that is, if $i_1 = j_1$, $i_2 = j_2$, ..., $i_p = j_p$, then $\boldsymbol{A}\binom{i_1,\dots,i_p}{j_1,\dots,j_p}$ is called a **principal minor of order $\boldsymbol{p}$**. I think the following hybrid terminology is useful: a **minor submatrix** is any square submatrix of $\boldsymbol{A}$ (regardless of whether $\boldsymbol{A}$ is square) and a **minor** of $\boldsymbol{A}$ is the determinant of a minor submatrix (same as Gantmacher). To be on the safe side, I may use the redundant term **minor determinant** to mean minor.

Given a square $n \times n$ matrix

$$\boldsymbol{A} = \begin{bmatrix} \alpha_{1,1} & \dots & \alpha_{1,n} \\ \vdots & & \vdots \\ \alpha_{n,1} & \dots & \alpha_{n,n} \end{bmatrix}$$

the **cofactor** $\operatorname{cof} \alpha_{i,j}$ of $\alpha_{i,j}$ is the determinant obtained by replacing the j^{th} column of $\boldsymbol{A}$ with the i^{th} unit coordinate vector $\boldsymbol{e}_i$. That is,

$$\operatorname{cof} \alpha_{i,j} = \det(\boldsymbol{A}^1, \dots, \boldsymbol{A}^{j-1}, \boldsymbol{e}_i, \boldsymbol{A}^{j+1}, \dots, \boldsymbol{A}^n).$$

By multilinearity we have for any column j,

$$\det \boldsymbol{A} = \sum_{i=1}^{n} \alpha_{i,j} \operatorname{cof} \alpha_{i,j}.$$

123 Lemma (Cofactors and minors) *For any square matrix $\boldsymbol{A}$,*

$$\operatorname{cof} \alpha_{i,j} = (-1)^{i+j} \det \boldsymbol{A}_{i,j},$$

where $\boldsymbol{A}_{i,j}$ is the minor submatrix obtained by deleting the i^{th} row and j^{th} column from $\boldsymbol{A}$. Consequently

$$\det \boldsymbol{A} = \sum_{i=1}^{n} (-1)^{i+j} \alpha_{i,j} \det \boldsymbol{A}_{i,j}.$$

Similarly (interchanging the roles of rows and columns), for any row i,

$$\det \boldsymbol{A} = \sum_{j=1}^{n} (-1)^{i+j} \alpha_{i,j} \det \boldsymbol{A}_{i,j}.$$

Proof: Cf. Apostol [6, Theorem 3.9, p. 87]. By definition

$$\operatorname{cof} \alpha_{i,j} = \begin{vmatrix} \alpha_{1,1} & \dots & \alpha_{1,j-1} & 0 & \alpha_{1,j+1} & \dots & \alpha_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \alpha_{i-1,1} & \dots & \alpha_{i-1,j-1} & 0 & \alpha_{i-1,j+1} & \dots & \alpha_{i-1,n} \\ \alpha_{i,1} & \dots & \alpha_{i,j-1} & 1 & \alpha_{i,j+1} & \dots & \alpha_{i,n} \\ \alpha_{i+1,1} & \dots & \alpha_{i+1,j-1} & 0 & \alpha_{i+1,j+1} & \dots & \alpha_{i+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \alpha_{n,1} & \dots & \alpha_{n,j-1} & 0 & \alpha_{n,j+1} & \dots & \alpha_{n,n} \end{vmatrix}.$$

Adding $-\alpha_{i,k}\boldsymbol{e}_i$ to column k does not change the determinant. Doing this for all $k \neq j$ yields

$$\operatorname{cof} \alpha_{i,j} = \begin{vmatrix} \alpha_{1,1} & \dots & \alpha_{1,j-1} & 0 & \alpha_{1,j+1} & \dots & \alpha_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \alpha_{i-1,1} & \dots & \alpha_{i-1,j-1} & 0 & \alpha_{i-1,j+1} & \dots & \alpha_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ \alpha_{i+1,1} & \dots & \alpha_{i+1,j-1} & 0 & \alpha_{i+1,j+1} & \dots & \alpha_{i+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \alpha_{n,1} & \dots & \alpha_{n,j-1} & 0 & \alpha_{n,j+1} & \dots & \alpha_{n,n} \end{vmatrix}.$$

Now by repeatedly interchanging columns a total of $j-1$ times we obtain

$$\operatorname{cof} \alpha_{i,j} = (-1)^{j-1} \begin{vmatrix} 0 & \alpha_{1,1} & \dots & \alpha_{1,j-1} & \alpha_{1,j+1} & \dots & \alpha_{1,n} \\ \vdots & & & \vdots & & & \vdots \\ 0 & \alpha_{i-1,1} & \dots & \alpha_{i-1,j-1} & \alpha_{i-1,j+1} & \dots & \alpha_{i-1,n} \\ 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \alpha_{i+1,1} & \dots & \alpha_{i+1,j-1} & \alpha_{i+1,j+1} & \dots & \alpha_{i+1,n} \\ \vdots & & & \vdots & & & \vdots \\ 0 & \alpha_{n,1} & \dots & \alpha_{n,j-1} & \alpha_{n,j+1} & \dots & \alpha_{n,n} \end{vmatrix}.$$

Interchanging rows $i-1$ times yields

$$\operatorname{cof} \alpha_{i,j} = (-1)^{i+j} \begin{vmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \alpha_{1,1} & \dots & \alpha_{1,j-1} & \alpha_{1,j+1} & \dots & \alpha_{1,n} \\ \vdots & & & \vdots & & & \vdots \\ 0 & \alpha_{i-1,1} & \dots & \alpha_{i-1,j-1} & \alpha_{i-1,j+1} & \dots & \alpha_{i-1,n} \\ 0 & \alpha_{i+1,1} & \dots & \alpha_{i+1,j-1} & \alpha_{i+1,j+1} & \dots & \alpha_{i+1,n} \\ \vdots & & & \vdots & & & \vdots \\ 0 & \alpha_{n,1} & \dots & \alpha_{n,j-1} & \alpha_{n,j+1} & \dots & \alpha_{n,n} \end{vmatrix}.$$

(Recall that $(-1)^{j-1+i-1} = (-1)^{i+j}$.) This last determinant is block diagonal, so we see that it is just $\left|\boldsymbol{A}_{i,j}\right|$, which completes the proof.

The conclusion for rows follows from that for columns and Proposition 116 on transposes. ∎

By repeatedly applying this result, we can express $\det \boldsymbol{A}$ in terms of 1×1 determinants.

If we take the cofactors from an *alien* column or row, we have:

124 Lemma (Expansion by alien cofactors) *Let $\boldsymbol{A}$ be a square $n \times n$ matrix. For any column j and any $k \neq j$,*

$$\sum_{i=1}^{n} \alpha_{i,j} \operatorname{cof} \alpha_{i,k} = 0.$$

Likewise for any row i and any $k \neq i$,

$$\sum_{j=1}^{n} \alpha_{i,j} \operatorname{cof} \alpha_{k,j} = 0.$$

Proof: Consider the matrix $\boldsymbol{A}_1 = [\tilde{\alpha}_{i,j}]$ obtained from $\boldsymbol{A}$ by replacing the k^{th} column with another copy of column j. Then the i,k cofactors, $i = 1, \dots, n$, of $\boldsymbol{A}$ and $\boldsymbol{A}_1$ are the same. (The cofactors don't depend on the column they belong to, since it is replaced by a unit coordinate vector.) So by Lemma 123, $\left|\boldsymbol{A}_1\right| = \sum_{i=1}^{n} \tilde{\alpha}_{i,k} \operatorname{cof} \alpha_{i,k} = \sum_{i=1}^{n} \alpha_{i,j} \operatorname{cof} \alpha_{i,k}$. But $\left|\boldsymbol{A}_1\right| = 0$ since it has two identical columns.

The conclusion for rows follows from that for columns and Proposition 116 on transposes. ∎

The transpose of the cofactor matrix is also called the **adjugate** matrix of $\boldsymbol{A}$. Combining the previous two lemmas yields the following on the adjugate.

125 Theorem (Cofactors and the inverse matrix) *For a square matrix*

$$\boldsymbol{A} = \begin{bmatrix} \alpha_{1,1} & \dots & \alpha_{1,n} \\ \vdots & & \vdots \\ \alpha_{n,1} & \dots & \alpha_{n,n} \end{bmatrix},$$

we have

$$\begin{bmatrix} \alpha_{1,1} & \dots & \alpha_{1,n} \\ \vdots & & \vdots \\ \alpha_{n,1} & \dots & \alpha_{n,n} \end{bmatrix} \begin{bmatrix} \operatorname{cof} \alpha_{1,1} & \dots & \operatorname{cof} \alpha_{n,1} \\ \vdots & & \vdots \\ \operatorname{cof} \alpha_{1,n} & \dots & \operatorname{cof} \alpha_{n,n} \end{bmatrix} = \begin{bmatrix} \left|\boldsymbol{A}\right| & & 0 \\ & \ddots & \\ 0 & & \left|\boldsymbol{A}\right| \end{bmatrix}.$$

That is, the product of $\boldsymbol{A}$ and its adjugate is $(\det \boldsymbol{A})\boldsymbol{I}_n$. Consequently, if $\det \boldsymbol{A} \neq 0$, then

$$\boldsymbol{A}^{-1} = \frac{1}{\det \boldsymbol{A}} \begin{bmatrix} \operatorname{cof} \alpha_{1,1} & \dots & \operatorname{cof} \alpha_{n,1} \\ \vdots & & \vdots \\ \operatorname{cof} \alpha_{1,n} & \dots & \operatorname{cof} \alpha_{n,n} \end{bmatrix}.$$

Combining this with Corollary 121 yields the following.

126 Corollary (Determinants and invertibility) *A square matrix is invertible if and only if its determinant is nonzero.*

Similar reasoning leads to the following theorem due to Jacobi. It expresses a p^{th} order minor of the adjugate in terms of the corresponding complementary minor of $\boldsymbol{A}$. The **complement** of the p^{th}-order minor $\boldsymbol{A}\binom{i_1,\dots,i_p}{j_1,\dots,j_p}$ is the $n-p^{\text{th}}$-order minor obtained by deleting rows $i_1,\dots,i_p$ and columns $j_1,\dots,j_p$ from $\boldsymbol{A}$.

127 Theorem (Jacobi) *For a square matrix*

$$\boldsymbol{A} = \begin{bmatrix} \alpha_{1,1} & \dots & \alpha_{1,n} \\ \vdots & & \vdots \\ \alpha_{n,1} & \dots & \alpha_{n,n} \end{bmatrix},$$

we have for any $1 \leqslant p \leqslant n$,

$$\left|\boldsymbol{A}\right| \cdot \begin{vmatrix} cof\,\alpha_{1,1} & \dots & cof\,\alpha_{p,1} \\ \vdots & & \vdots \\ cof\,\alpha_{1,p} & \dots & cof\,\alpha_{p,p} \end{vmatrix} = \left|\boldsymbol{A}\right|^p \cdot \begin{vmatrix} \alpha_{p+1,p+1} & \dots & \alpha_{p+1,n} \\ \vdots & & \vdots \\ \alpha_{n,p+1} & \dots & \alpha_{n,n} \end{vmatrix}.$$

Proof: Observe, recalling Theorem 124 on alien cofactors, that

$$\left[\begin{array}{ccc|ccc} \alpha_{1,1} & \dots & \alpha_{1,p} & \alpha_{1,p+1} & \dots & \alpha_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_{p,1} & \dots & \alpha_{p,p} & \alpha_{p,p+1} & \dots & \alpha_{p,n} \\ \hline \alpha_{p+1,1} & \dots & \alpha_{p+1,p} & \alpha_{p+1,p+1} & \dots & \alpha_{p1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_{n,1} & \dots & \alpha_{n,p} & \alpha_{n,p+1} & \dots & \alpha_{n,n} \end{array}\right] \left[\begin{array}{ccc|ccc} \operatorname{cof}\alpha_{1,1} & \dots & \operatorname{cof}\alpha_{p,1} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \operatorname{cof}\alpha_{1,p} & \dots & \operatorname{cof}\alpha_{p,p} & 0 & \dots & 0 \\ \hline \operatorname{cof}\alpha_{1,p+1} & \dots & \operatorname{cof}\alpha_{p,p+1} & 1 & & 0 \\ \vdots & & \vdots & & \ddots & \\ \operatorname{cof}\alpha_{1,n} & \dots & \operatorname{cof}\alpha_{n,n} & 0 & & 1 \end{array}\right]$$

$$= \left[\begin{array}{ccc|ccc} \left|\boldsymbol{A}\right| & & 0 & \alpha_{1,p+1} & \dots & \alpha_{1,n} \\ & \ddots & & \vdots & & \vdots \\ 0 & & \left|\boldsymbol{A}\right| & \alpha_{p,p+1} & \dots & \alpha_{p,n} \\ \hline 0 & \dots & 0 & \alpha_{p+1,p+1} & \dots & \alpha_{p+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & \alpha_{n,p+1} & \dots & \alpha_{n,n} \end{array}\right]$$

and take determinants on both sides. ∎

12.4 Characteristic polynomials

The **characteristic polynomial** f of a square matrix $\boldsymbol{A}$ is defined by $f(\lambda) = \det(\lambda\boldsymbol{I} - \boldsymbol{A})$. Roots of this polynomial are called **characteristic roots** of $\boldsymbol{A}$.

128 Lemma *Every eigenvalue of a matrix is a characteristic root, and every real characteristic root is an eigenvalue.*

Proof: To see this note that if λ is an eigenvalue with eigenvector $\boldsymbol{x} \neq 0$, then $(\lambda \boldsymbol{I} - \boldsymbol{A})\boldsymbol{x} = \lambda\boldsymbol{x} - \boldsymbol{A}\boldsymbol{x} = 0$, so $(\lambda I - \boldsymbol{A})$ is singular, so $\det(\lambda\boldsymbol{I} - \boldsymbol{A}) = 0$. That is, λ is a characteristic root of $\boldsymbol{A}$.

Conversely, if $\det(\lambda\boldsymbol{I} - \boldsymbol{A}) = 0$, then there is some nonzero $\boldsymbol{x}$ with $(\lambda\boldsymbol{I} - \boldsymbol{A})\boldsymbol{x} = 0$, or $\boldsymbol{A}\boldsymbol{x} = \lambda\boldsymbol{x}$. ∎

129 Lemma *The determinant of a square matrix is the product of its characteristic roots.*

Proof: (Cf. [6, p. 106]) Let $\boldsymbol{A}$ be an $n \times n$ square matrix and let f be its characteristic polynomial. Then $f(0) = \det(-\boldsymbol{A}) = (-1)^n \det \boldsymbol{A}$. On the other hand, we can factor f as

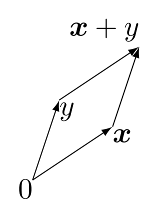
$$f(\lambda) = (\lambda - \lambda_1) \cdots (\lambda - \lambda_n)$$

where $\lambda_1, \dots, \lambda_n$ are its characteristic roots. Thus $f(0) = (-1)^n \lambda_1 \cdots \lambda_n$. ∎

130 Corollary *The determinant of a symmetric matrix is the product of its eigenvalues.*

12.5 The determinant as an "oriented volume"

There is another interpretation of the determinant of an $n \times n$ matrix $\boldsymbol{A}$. The unit coordinate vectors $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ determine a hypercube $[0,1]^n$ in $\boldsymbol{R}^{\mathrm{n}}$ of n-dimensional volume 1. The matrix $\boldsymbol{A}$ maps the j^{th} unit coordinate vector to the j^{th} column $\boldsymbol{A}^j$ of $\boldsymbol{A}$. These columns define a parallelotope and $\det \boldsymbol{A}$ is the volume of the parallelotope, perhaps multiplied by -1, depending on the *orientation* of the columns. In any event, the area of the parallelotope is equal to $|\det \boldsymbol{A}|$. So $|\det \boldsymbol{A}|$ measures the effect that $\boldsymbol{A}$ has on volumes. (That is why the absolute value of Jacobian determinants show up in change of variables formulas for integrals.) I don't want to go into detail on the notion of orientation, but I shall present enough so that you can get a glimmer of what the assertion is.



First, what is a parallelotope? It is a polytope with parallel faces, for example, a cube. The parallelotope generated by the vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ is the convex hull of zero and the vectors of the form $\boldsymbol{x}_{i_1} + \boldsymbol{x}_{i_2} + \cdots + \boldsymbol{x}_{i_k}$, where $1 \leqslant k \leqslant n$ and $i_1, \dots, i_n$ are distinct. For instance, in R^2 the parallelotope generated by $\boldsymbol{x}$ and $\boldsymbol{y}$ is the plane parallelogram with vertexes 0, $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{x} + \boldsymbol{y}$.

The notion of n-dimensional volume is straightforward. For $n = 1$, it is length, for $n = 2$, it is area, etc. Oriented volume is more complicated. It distinguishes parallelotopes based on the order that the vectors are presented. For instance, in the boxedfigure above the angle swept out from $\boldsymbol{x}$ to $\boldsymbol{y}$ counterclockwise is positive, while from $\boldsymbol{y}$ to $\boldsymbol{x}$ is clockwise. The oriented volume is positive in the first case and negative in the second.

Let's start with a simple case, with vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\boldsymbol{R}^2$. To simply further, assume that $\boldsymbol{x}$ lies on the horizontal axis, that is, $\boldsymbol{x} = (x_1, 0)$. Then $\det(\boldsymbol{x}, \boldsymbol{y}) = \det \begin{bmatrix} x_1 & y_1 \\ 0 & y_2 \end{bmatrix} = x_1 y_2$. Now consider the parallelogram generated by $\boldsymbol{x}$ and $\boldsymbol{y}$. See Figure 4. As drawn, the base of the

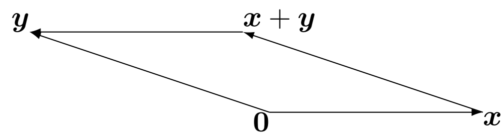


Figure 4. The area of the parallelogram determined by $\boldsymbol{x}$ and $\boldsymbol{y}$.

parallelogram has length x_1 and its altitude is y_2, so the area is $x_1 y_2$. More generally, depending on the quadrant that y lies in, the area is $|x_1 y_2|$. If $y_2 > 0$, then the area is equal to $\det \boldsymbol{A}$, and if $y_2 < 0$, then the area is $-\det \boldsymbol{A}$. The first case is where $\boldsymbol{y}$ lies counterclockwise from $\boldsymbol{x}$, and the second case is where $\boldsymbol{y}$ lies clockwise from $\boldsymbol{x}$. So the oriented area in $\boldsymbol{R}^2$ depends on the clockwise-counterclockwise notion of orientation. Higher dimensional orientation is more complicated.

For more general vectors $\boldsymbol{x}$ in $\boldsymbol{R}^2$, we make us of the linear transformation of rotation. There is an orthogonal matrix $\boldsymbol{C}$ such that $\boldsymbol{C}\boldsymbol{x}$ lies on the positive horizontal axis. Since orthogonal matrices preserve distance and angles the area of the parallelogram generated by $\boldsymbol{x}$ and $\boldsymbol{y}$ is the same as the area of the parallelogram generated by $\boldsymbol{C}\boldsymbol{x}$ and $\boldsymbol{C}$. But the latter is $\det(\boldsymbol{C}\boldsymbol{x}, \boldsymbol{C}\boldsymbol{y}) = \det \boldsymbol{C}\boldsymbol{A}$. But $\det \boldsymbol{C}\boldsymbol{A} = \det \boldsymbol{C} \cdot \det \boldsymbol{A}$, and since $\boldsymbol{C}$ is orthogonal its determinant is ± 1. Thus the area of the parallelogram generated by $\boldsymbol{x}$ and $\boldsymbol{y}$ is $|\det(\boldsymbol{x}, \boldsymbol{y})|$.

12.6 Computing inverses and determinants by Gauss' method

This section describes how to use the method of Gaussian elimination to find the inverse of a matrix and to compute its determinant. Let $\boldsymbol{A}$ be an $n \times n$ invertible matrix, so that

$$\boldsymbol{A}\boldsymbol{A}^{-1} = \boldsymbol{I}.$$

To find the j^{th} column $\boldsymbol{x} = \boldsymbol{A}^{-1j}$ of $\boldsymbol{A}^{-1}$, recall from the definition of matrix multiplication that $\boldsymbol{x}$ satisfies $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{I}^j$, where $\boldsymbol{I}^j$ is the j^{th} column of the identity matrix. Indeed if $\boldsymbol{A}$ is invertible, then $\boldsymbol{x}$ is the unique vector with this property. Thus we can form the $n \times (n+1)$ augmented coefficient matrix $(\boldsymbol{A}|\boldsymbol{I}^j)$ and use elementary row operations of Gaussian elimination to transform it to $(\boldsymbol{I}|\boldsymbol{x}) = (\boldsymbol{I}|\boldsymbol{A}^{-1j})$. The same sequence of row operations is employed to transform $\boldsymbol{A}$ into $\boldsymbol{I}$ regardless of which column $\boldsymbol{I}^j$ we use to augment with. So we can solve for *all* the columns simultaneously by augmenting with all the columns of $\boldsymbol{I}$. That is, form the $n \times 2n$ augmented matrix $(\boldsymbol{A}|\boldsymbol{I}^1, \boldsymbol{I}^2, \dots, \boldsymbol{I}^n) = (\boldsymbol{A}|\boldsymbol{I})$. If we can transform this by elementary row operations into $(\boldsymbol{I}|\boldsymbol{X})$, it must be that $\boldsymbol{X} = \boldsymbol{A}^{-1}$. Furthermore, if we cannot make the transformation, then $\boldsymbol{A}$ is not invertible.

You may ask, how can we tell if we cannot transform $\boldsymbol{A}$ into $\boldsymbol{I}$? Perhaps it is possible, but we are not clever enough. To attack this question we must write down a specific algorithm. So here is one version of an algorithm for inverting a matrix by Gaussian elimination, or else showing that it is not invertible.

> Let $\boldsymbol{A}^0 = \boldsymbol{A}$. At each stage t we apply an elementary operation to transform $\boldsymbol{A}^{t-1}$ into $\boldsymbol{A}^t$ in such a way that
>
> $$\det \boldsymbol{A}^t \neq 0 \iff \det \boldsymbol{A} \neq 0.$$

The rules for selecting the elementary row operation are described below. By stage $t = n$, either $\boldsymbol{A}^t = \boldsymbol{I}$ or else we shall have shown that $\det \boldsymbol{A} = 0$, so $\boldsymbol{A}$ is not invertible.

Stage t: At stage t, assume that all the columns $j = 1, \dots, t-1$ of $\boldsymbol{A}^{t-1}$ have been transformed into the corresponding columns of $\boldsymbol{I}$, and that $\det \boldsymbol{A} \neq 0 \iff \det \boldsymbol{A}^{t-1} \neq 0$.

Step 1: Normalize the diagonal to 1.

Case 1: $a^{t-1}_{t,t}$ is nonzero. Divide row 1 by $a^{t-1}_{t,t}$ to set $a^t_{t,t} = 1$. This has the side effect of setting $\det \boldsymbol{A}^t = a^{t-1}_{t,t} \det \boldsymbol{A}^{t-1}$.

Case 2: $a^{t-1}_{t,t} = 0$, but there is row i with $i > t$ for which $a^{t-1}_{i,t} \neq 0$. Divide row i by $a^{t-1}_{i,t}$ and add it to row 1. This sets $a^t_{t,t} = 1$, and leaves $\det \boldsymbol{A}^t = \det \boldsymbol{A}^{t-1}$.

Case 3: If $a^{t-1}_{t,t} = 0$, but there is no row i with $i > t$ for which $a^{t-1}_{i,t} \neq 0$. In this case, the first t columns of $\boldsymbol{A}^{t-1}$ must be dependent. This is because there are t column vectors whose only nonzero components are in the first $t-1$ rows. This implies $\det \boldsymbol{A}^{t-1} = 0$, and hence $\det \boldsymbol{A} = 0$. This shows that $\boldsymbol{A}$ is not invertible.

If Case 3 occurs stop. We already know that $\boldsymbol{A}$ is not invertible. In cases 1 and 2 proceed to:

Step 2: Eliminate the off diagonal elements. Since $a^t_{t,t} = 1$, for $i \neq t$ multiply row 1 by $a^{t-1}_{i,t}$ and subtract it from row i. This sets $a^t_{i,t} = 0$, for $i \neq t$, and does not change $\det \boldsymbol{A}^t$.

This completes the construction of $\boldsymbol{A}^t$ from $\boldsymbol{A}^{t-1}$. Proceed to stage $t+1$, and note that all the columns $j = 1, \dots, t$ of $\boldsymbol{A}^t$ have been transformed into the corresponding columns of $\boldsymbol{I}$, and that $\det \boldsymbol{A} \neq 0 \iff \det \boldsymbol{A}^t \neq 0$.

Now observe how this also can be used to calculate the determinant. Suppose the process runs to completion so that $\boldsymbol{A}^n = \boldsymbol{I}$. Every time a row was divided by its diagonal element $a^{t-1}_{t,t}$ to normalize it, we had $\det \boldsymbol{A}^t = \frac{1}{a^{t-1}_{t,t}} \det \boldsymbol{A}^{t-1}$. Thus we have

$$1 = \det \boldsymbol{I} = \det \boldsymbol{A}^n = \prod_{t : a^{t-1}_{t,t} \neq 0} \frac{1}{a^{t-1}_{t,t}} \det \boldsymbol{A}$$

or

$$\det \boldsymbol{A} = \prod_{t : a^{t-1}_{t,t} \neq 0} a^{t-1}_{t,t}.$$

One of the virtues of this approach is that it is extremely easy to program, and reasonably efficient. Each elementary row operation has at most $2n$ multiplications and $2n$ additions, and at most n^2 elementary row operations are required, so the number of steps grows no faster than $4n^3$.

Here are two illustrative examples, which, by the way, were produced (text and all) by a 475-line program written in `perl` of all things.

131 Example (Matrix inversion by Gaussian elimination) Invert the following 3×3

matrix using Gaussian elimination and compute its determinant as a byproduct.

$$\boldsymbol{A} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

We use only two elementary row operations: dividing a row by a scalar, which also divides the determinant, and adding a multiple of one row to a different row, which leaves the determinant unchanged. Thus the determinant of $\boldsymbol{A}$ is just the product of all the scalars used to divide the rows of $\boldsymbol{A}$ to normalize its diagonal elements to ones. We shall keep track of this product in the variable μ as we go along. At any given stage, μ times the determinant of the left hand block is equal to the determinant of $\boldsymbol{A}$. Before each step, we put a box around the target entry to be transformed.

$\alpha_{1,1}$ is zero,

$$\mu = 1 \qquad \left(\begin{array}{ccc|ccc} \boxed{0} & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

so add row 3 to row 1. To eliminate $\alpha_{3,1} = 1$,

$$\mu = 1 \qquad \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ \boxed{1} & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

subtract row 1 from row 3. To normalize $\alpha_{3,3} = -1$,

$$\mu = 1 \qquad \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & \boxed{-1} & -1 & 0 & 0 \end{array}\right)$$

divide row 3 (and multiply μ) by -1. To eliminate $\alpha_{1,3} = 1$,

$$\mu = -1 \qquad \left(\begin{array}{ccc|ccc} 1 & 0 & \boxed{1} & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right)$$

subtract row 3 from row 1. This gives us

$$\mu = -1 \qquad \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right)$$

To summarize:

$$\boldsymbol{A} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad \boldsymbol{A}^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

And the determinant of $\boldsymbol{A}$ is -1. We could have gotten this result faster by interchanging rows 1 and 3, but it is hard (for me) to program an algorithm to recognize when to do this. □

132 Example (Gaussian elimination on a singular matrix) Consider the following 3×3 matrix.

$$\boldsymbol{A} = \begin{pmatrix} 1 & 1 & 2 \\ 2 & 4 & 4 \\ 3 & 6 & 6 \end{pmatrix}$$

We shall use the method of Gaussian elimination to attempt transform the augmented block matrix $(\boldsymbol{A}|\boldsymbol{I})$ into $(\boldsymbol{I}|\boldsymbol{A}^{-1})$. To eliminate $\alpha_{2,1} = 2$,

$$\mu = 1 \qquad \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ \boxed{2} & 4 & 4 & 0 & 1 & 0 \\ 3 & 6 & 6 & 0 & 0 & 1 \end{array}\right)$$

multiply row 1 by 2 and subtract it from row 2. To eliminate $\alpha_{3,1} = 3$,

$$\mu = 1 \qquad \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & -2 & 1 & 0 \\ \boxed{3} & 6 & 6 & 0 & 0 & 1 \end{array}\right)$$

multiply row 1 by 3 and subtract it from row 3. To normalize $\alpha_{2,2} = 2$,

$$\mu = 1 \qquad \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & \boxed{2} & 0 & -2 & 1 & 0 \\ 0 & 3 & 0 & -3 & 0 & 1 \end{array}\right)$$

divide row 2 (and multiply μ) by 2. To eliminate $\alpha_{1,2} = 1$,

$$\mu = 2 \qquad \left(\begin{array}{ccc|ccc} 1 & \boxed{1} & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & \frac{1}{2} & 0 \\ 0 & 3 & 0 & -3 & 0 & 1 \end{array}\right)$$

subtract row 2 from row 1. To eliminate $\alpha_{3,2} = 3$,

$$\mu = 2 \qquad \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 2 & -\frac{1}{2} & 0 \\ 0 & 1 & 0 & -1 & \frac{1}{2} & 0 \\ 0 & \boxed{3} & 0 & -3 & 0 & 1 \end{array}\right)$$

multiply row 2 by 3 and subtract it from row 3. Now notice that the first 3 columns of $\boldsymbol{A}$ are dependent, as each column has at most its first 2 entries nonzero, and any 3 vectors in a 2-dimensional space are dependent.

$$\mu = 2 \qquad \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 2 & -\frac{1}{2} & 0 \\ 0 & 1 & 0 & -1 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & -1\frac{1}{2} & 1 \end{array}\right)$$

Therefore $\boldsymbol{A}$ has no inverse, and the determinant of $\boldsymbol{A}$ is zero. (If we had interchanged columns 1 and 3, we would have arrived at this result sooner, but hindsight is hard to program.) $\square$

133 Exercise Using the language of your choice, write a program to accept a square matrix and invert it by Gaussian elimination, or stop when you find it is not invertible. $\square$

References

[1] A. C. Aitken. 1954. *Determinants and matrices*, 8th. ed. New York: Interscience.

[2] C. D. Aliprantis and K. C. Border. 2006. *Infinite dimensional analysis: A hitchhiker's guide*, 3d. ed. Berlin: Springer–Verlag.

[3] C. D. Aliprantis and O. Burkinshaw. 1999. *Problems in real analysis*, 2d. ed. San Diego: Academic Press. Date of publication, 1998. Copyright 1999.

[4] T. W. Anderson. 1958. *An introduction to multivariate statistical analysis*. A Wiley Publication in Mathematical Statistics. New York: Wiley.

[5] T. M. Apostol. 1967. *Calculus, Volume I: One-variable calculus with an introduction to linear algebra*, 2d. ed. New York: John Wiley & Sons.

[6] ——— . 1969. *Calculus*, 2d. ed., volume 2. Waltham, Massachusetts: Blaisdell.

[7] S. Axler. 1997. *Linear algebra done right*, 2d. ed. Undergraduate Texts in Mathematics. New York: Springer.

[8] A. Berman and A. Ben-Israel. 1971. More on linear inequalities with applications to matrix theory. *Journal of Mathematical Analysis and Applications* 33(3):482–496.
DOI: http://dx.doi.org/10.1016/0022-247X(71)90072-2

[9] K. C. Border. 2001. More than you wanted to know about quadratic forms. On-line note. `http://www.its.caltech.edu/~kcborder/Notes/QuadraticForms.pdf`

[10] C. Carathéodory. 1982. *Calculus of variations*, 2d. ed. New York: Chelsea. This was originally published in 1935 in two volumes by B. G. Teubner in Berlin as *Variationsrechnung und Partielle Differentialgleichungen erster Ordnung*. In 1956 the first volume was edited and updated by E. Hölder. The revised work was translated by Robert B. Dean and Julius J. Brandstatter and published in two volumes as *Calculus of variations and partial differential equations of the first order* by Holden-Day in 1965–66. The Chelsea second edition combines and revises the 1967 edition.

[11] J. Dieudonné. 1969. *Foundations of modern analysis*. Number 10-I in Pure and Applied Mathematics. New York: Academic Press. Volume 1 of Treatise on Analysis.

[12] J. Franklin. 2000. *Matrix theory*. Mineola, New York: Dover. Reprint of 1968 edition published by Prentice-Hall, Englewood Cliffs, N.J.

[13] F. R. Gantmacher. 1959. *Matrix theory*, volume 1. New York: Chelsea.

[14] P. R. Halmos. 1974. *Finite dimensional vector spaces*. New York: Springer–Verlag. Reprint of the edition published by Van Nostrand, 1958.

[15] P. N. Klein. 2013. *Coding the matrix: Linear algebra through computer science applications*. Newton, Massachusetts: Newtonian Press.

[16] L. H. Loomis and S. Sternberg. 1968. *Advanced calculus*. Reading, Massachusetts: Addison–Wesley.

[17] S. MacLane and G. Birkhoff. 1993. *Algebra*, 3d. ed. New York: Chelsea.

[18] L. W. McKenzie. 1960. Matrices with dominant diagonals and economic theory. In K. J. Arrow, S. Karlin, and P. Suppes, eds., *Mathematical Methods in the Social Sciences, 1959*, number 4 in Stanford Mathematical Studies in the Social Sciences, chapter 4, pages 47–62. Stanford, California: Stanford University Press.

[19] F. J. Murray. 1941. *An introduction to linear transformations in Hilbert space*. Number 4 in Annals of Mathematics Studies. Princeton, New Jersey: Princeton University Press. Reprinted 1965 by Kraus Reprint Corporation, New York.

[20] C. R. Rao. 1973. *Linear statistical inference and its applications*, 2d. ed. Wiley Series in Probability and Mathematical Statistics. New York: Wiley.

[21] H. Theil. 1971. *Principles of econometrics*. New York: Wiley.

[22] B. L. van der Waerden. 1969. *Mathematical statistics*. Number 156 in Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete. New York, Berlin, and Heidelberg: Springer–Verlag. Translated by Virginia Thompson and Ellen Sherman from *Mathematische Statistik*, published by Springer-Verlag in 1965, as volume 87 in the series Grundlerhen der mathematischen Wissenschaften.

Index