# Linear Algebra

Joe Erickson

# Table of Contents

# 1

# Euclidean Vectors

## 1.1 – Groups, Rings and Fields

It is assumed that the reader is well familiar with sets and functions. Given a set $S$, a **binary operation** from $S \times S$ to $S$ is a function $* : S \times S \to S$, so that for each $(a, b) \in S \times S$ we have $*(a, b) \in S$. As is customary we will usually write $a * b$ instead of $*(a, b)$. The operation $*$ is **commutative** if, for every $a, b \in S$,

$$*(a, b) = a * b = b * a = *(b, a),$$

and **associative** if, for every $a, b, c \in S$,

$$*(a, *(b, c)) = a * (b * c) = (a * b) * c = *(*(a, b), c).$$

Common binary operations are addition of real numbers, $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, and multiplication of real numbers, $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, both of which are commutative and associative. Recall that subtraction and division of real numbers is neither commutative nor associative, and indeed $a \div b$ is not even defined in the case when $b = 0$!

Linear algebra is foremost the study of vector spaces, and the functions between vector spaces called mappings. However, underlying every vector space is a structure known as a field, and underlying every field there is what is known as a ring. Thus we begin with the definition of a ring and proceed thence.

**Definition 1.1.** *A **ring** is a triple $(R, +, \cdot)$ consisting of a set $R$ of objects, along with binary operations **addition** $+ : R \times R \to R$ and **multiplication** $\cdot : R \times R \to R$ subject to the following axioms:*

R1. $a + b = b + a$ *for any* $a, b \in R$.
R2. $a + (b + c) = (a + b) + c$ *for any* $a, b, c \in R$.
R3. *There exists some* $0 \in R$ *such that* $a + 0 = a$ *for any* $a \in R$.
R4. *For each* $a \in R$ *there exists some* $-a \in R$ *such that* $-a + a = 0$.
R5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for any* $a, b, c \in R$.
R6. $a \cdot (b + c) = a \cdot b + a \cdot c$ *for any* $a, b, c \in R$.

As in elementary algebra it is common practice to denote multiplication by omitting the symbol $\cdot$ and employing juxtaposition:

$$ab = a \cdot b, \quad a(bc) = a \cdot (b \cdot c), \quad a(b + c) = a \cdot (b + c),$$

and so on.

We call the object $-a$ in Axiom R4 the **additive identity** of $a$. From Axioms R1 and R4 we see that

$$(-a) + a = a + (-a) = 0.$$

As a matter of convenience we define a **subtraction** operation as follows:

$$a - b = a + (-b),$$

so that

$$a - a = 0$$

obtains just as in elementary algebra.

**Definition 1.2.** *A ring $(R, +, \cdot)$ is* ***commutative*** *if it satisfies the additional axiom*

R7. $a \cdot b = b \cdot a$ *for all* $a, b \in R$.

**Definition 1.3.** *A commutative ring $(R, +, \cdot)$ is a* ***unitary commutative ring*** *if it satisfies the additional axiom*

R8. *There exists some* $1 \in R$ *such that* $a \cdot 1 = a$ *for any* $a \in R$.

A ring that satisfies Axiom R8 but not R7 is simply called a **unitary ring**, but we will have no need for such an entity.

**Definition 1.4.** *Let $(R, +, \cdot)$ be a unitary ring. The* ***multiplicative inverse*** *of an object $a \in R$ is an object $a^{-1} \in R$ for which*

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

We now have all the necessary pieces in place in order to give the following simple definition of a field.

**Definition 1.5.** *A* ***field*** *is a unitary commutative ring $(R, +, \cdot)$ for which $1 \neq 0$, and every $a \in R$ such that $a \neq 0$ has a multiplicative inverse.*

*To summarize, a field is a set of objects $\mathbb{F}$, together with binary operations $+$ and $\cdot$ on $\mathbb{F}$, that are subject to the following* ***field axioms****:*

F1. $a + b = b + a$ *for any* $a, b \in \mathbb{F}$.
F2. $a + (b + c) = (a + b) + c$ *for any* $a, b, c \in \mathbb{F}$.
F3. *There exists some* $0 \in \mathbb{F}$ *such that* $a + 0 = a$ *for any* $a \in \mathbb{F}$.
F4. *For each* $a \in \mathbb{F}$ *there exists some* $-a \in \mathbb{F}$ *such that* $-a + a = 0$.
F5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for any* $a, b, c \in \mathbb{F}$.
F6. $a \cdot (b + c) = a \cdot b + a \cdot c$ *for any* $a, b, c \in \mathbb{F}$.
F7. $a \cdot b = b \cdot a$ *for all* $a, b \in \mathbb{F}$.
F8. *There exists some* $0 \neq 1 \in \mathbb{F}$ *such that* $a \cdot 1 = a$ *for any* $a \in \mathbb{F}$.

F9. *For each* $0 \neq a \in \mathbb{F}$ *there exists some* $a^{-1} \in \mathbb{F}$ *such that* $aa^{-1} = 1$.

Commonly encountered fields are the set of real numbers $\mathbb{R}$ under the usual operations of addition and multiplication, and also the set of complex numbers $\mathbb{C}$. Many results in linear algebra (but not all) are applicable to both the fields $\mathbb{R}$ and $\mathbb{C}$, in which case we will employ the symbol $\mathbb{F}$ to denote either. That is, anywhere $\mathbb{F}$ appears one can safely substitute either $\mathbb{R}$ or $\mathbb{C}$ as desired. Throughout these notes a **scalar** will be taken to be an object belonging to a field. Throughout the remainder of this chapter all scalars will be real numbers.

**Example 1.6.** The set of integers $\mathbb{Z}$ under the usual operations of addition and multiplication satisfies all the field axioms save for one: F9, the axiom that requires every nonzero element in a set of objects to have a multiplicative inverse *that also is an element of the set of objects.* The multiplicative inverse for $2 \in \mathbb{Z}$ is $2^{-1}$, and of course $2^{-1} = 1/2$ does not belong to $\mathbb{Z}$. Therefore $\mathbb{Z}$ is not a field under the usual operations of addition and multiplication.

In contrast, the set of rational numbers

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\}$$

is a field under the usual operations of addition and multiplication, since the reciprocal of any nonzero rational number is also a rational number. ■

**Example 1.7.** A **finite field** is a field that contains a finite number of elements. One example is the set $\mathbb{Z}_2 = \{0, 1\}$, with a binary operation $+$ defined by

$$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0,$$

and a binary operation $\cdot$ defined by

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

Note that the only departure from "usual" addition and multiplication in evidence is $1 + 1 = 0$. It is straightforward, albeit tedious, to directly verify that each of the nine field axioms are satisfied. ■

## 1.2 – Real Euclidean Space

Let $\mathbb{R}$ denote the set of real numbers. Given a positive integer $n$, we define **real Euclidean *n*-space**, or simply ***n*-space**, to be the set

$$\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{R} \text{ for } 1 \leq i \leq n\}. \tag{1.1}$$

Any ordered list of $n$ objects is called an ***n*-tuple**, and the $n$-tuple $(x_1, x_2, \ldots, x_n)$ of real numbers, when regarded as an element of $\mathbb{R}^n$, is called a **point** in $n$-space. Each value $x_i$ in $(x_1, x_2, \ldots, x_n)$ is called a **coordinate** of the point, with $x_1$ being the "first" coordinate, $x_2$ the "second" coordinate, and so on. If $x$ is a point in $\mathbb{R}^n$, we write $x \in \mathbb{R}^n$ and take this as meaning

$$x = (x_1, x_2, \ldots, x_n)$$

for some real numbers $x_1, x_2, \ldots, x_n$. If $x_i = 0$ for all $1 \leq i \leq n$, then we obtain the point $(0, 0, \ldots, 0)$ called the **origin**.

Euclidean 2-space is more commonly known as the **plane**, which is the set

$$\mathbb{R}^2 = \{(x_1, x_2) : x_1, x_2 \in \mathbb{R}\},$$

with each point $(x_1, x_2)$ in the plane (or "on the plane") being a 2-tuple usually called an **ordered pair**. Euclidean 3-space is customarily called simply **space**, which is the set

$$\mathbb{R}^3 = \{(x_1, x_2, x_3) : x_1, x_2, x_3 \in \mathbb{R}\},$$

with each point $(x_1, x_2, x_3)$ in space being a 3-tuple usually called an **ordered triple**.

It is natural to assign a geometrical interpretation to the notion of a point on a plane or in space. Specifically, in the case of a point $p = (p_1, p_2) \in \mathbb{R}^2$ (i.e. a point $p$ on a plane), it is convenient to think of $p$ as being "located" somewhere on the plane relative to the origin $(0, 0)$. Exactly how the coordinates $p_1$ and $p_2$ of the point $p$ are used to determine a location for $p$ on the plane depends on the **coordinate system** being used. In $\mathbb{R}^2$ the rectangular and polar coordinate systems are most commonly employed. In $\mathbb{R}^3$ there are the rectangular, cylindrical, and spherical coordinate systems, among others. *Unless otherwise specified, we will always use the rectangular coordinate system!* For those who may not have encountered the rectangular coordinate system in $\mathbb{R}^3$, Figure 2 should suffice to make its workings known. In the figure the

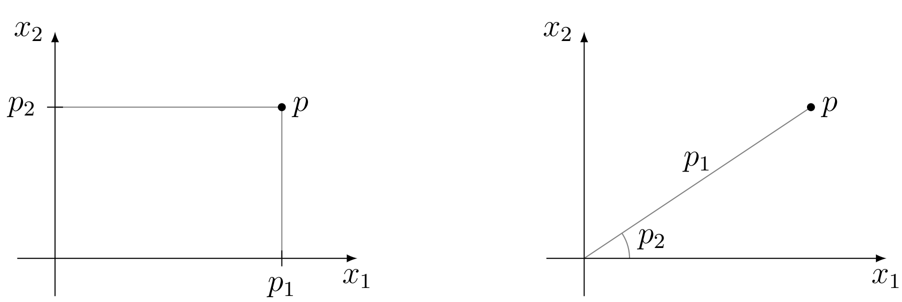



Figure 1. At left: $p = (p_1, p_2)$ in the rectangular coordinate system. At right: $p = (p_1, p_2)$ in the polar coordinate system.

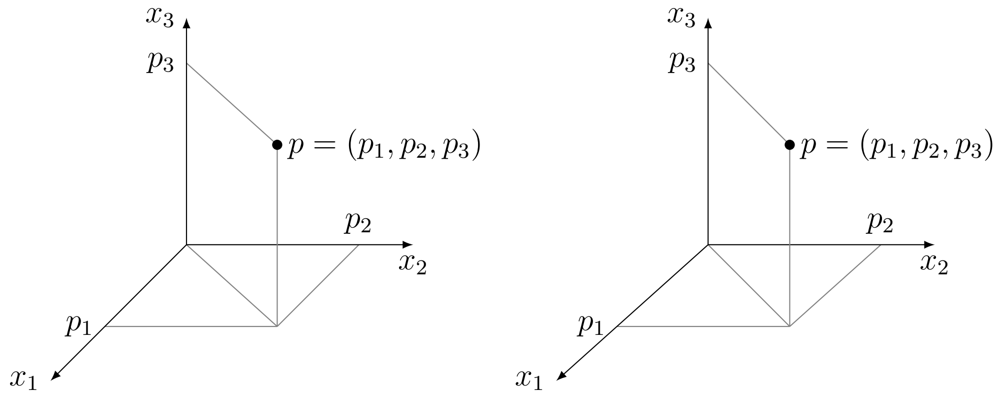



FIGURE 2. Stereoscopic image of $\mathbb{R}^3$ with $p = (p_1, p_2, p_3)$ in the rectangular coordinate system.

*positive* $x_i$-axis is labeled for $i = 1, 2, 3$, and so the point $p = (p_1, p_2, p_3)$ shown has coordinates $p_i > 0$ for each $i$.

It will be convenient to designate operations that allow for "adding" points, as well as "multiplying" them by real numbers and "subtracting" them. The definitions for these operations make use of the operations of addition and multiplication of real numbers which are taken to be understood.

**Definition 1.8.** *Let $p = (p_1, p_2, \ldots, p_n)$ and $q = (q_1, q_2, \ldots, q_n)$ be points in $\mathbb{R}^n$, and $c \in \mathbb{R}$. Then we define the **sum** $p + q$ of $p$ and $q$ to be the point*

$$p + q = (p_1 + q_1, p_2 + q_2, \ldots, p_n + q_n),$$

*and the **scalar multiple** $cp$ of $p$ by $c$ to be the point*

$$cp = (cp_1, cp_2, \ldots, cp_n).$$

*Defining $-p = (-p_1, -p_2, \ldots, -p_n)$, the **difference** $p - q$ of $p$ and $q$ is given to be*

$$p - q = p + (-q).$$

## 1.3 – Located Vectors

A **located vector** in $n$-space is an ordered pair of points $p, q \in \mathbb{R}^n$. We denote such an ordered pair by $\overrightarrow{pq}$ rather than $(p, q)$, both to help distinguish it from a point in $\mathbb{R}^2$ (which is an ordered pair of *numbers*), and also to reinforce the natural geometric interpretation of a located vector as an "arrow" in $n$-space that starts at $p$ and ends at $q$. We call $p$ the **initial point** of $\overrightarrow{pq}$, and $q$ the **terminal point**, and say that $\overrightarrow{pq}$ is "located at $p$." If the initial point $p$ is at the origin $(0, 0, \ldots, 0)$, then the located vector $\overrightarrow{pq}$ is called a **position vector** (a vector located at the origin).

The situation in $\mathbb{R}^2$ will be illustrative. In Figure 3 it can be seen that, if $p = (p_1, p_2)$ and $q = (q_1, q_2)$, then $\overrightarrow{pq}$ may be characterized as an arrow with initial point $p$ that decomposes into a horizontal translation of $q_1 - p_1$ and a vertical translation of $q_2 - p_2$.

Two located vectors $\overrightarrow{pq}$ and $\overrightarrow{uv}$ are **equivalent**, written $\overrightarrow{pq} \sim \overrightarrow{uv}$, if $q - p = v - u$. Again considering the situation in $\mathbb{R}^2$, if $p = (p_1, p_2)$, $q = (q_1, q_2)$, $u = (u_1, u_2)$, and $v = (v_1, v_2)$, then

$$\begin{aligned}
\overrightarrow{pq} \sim \overrightarrow{uv} \quad &\Leftrightarrow \quad q - p = v - u \\
&\Leftrightarrow \quad (q_1, q_2) - (p_1, p_2) = (v_1, v_2) - (u_1, u_2) \\
&\Leftrightarrow \quad (q_1 - p_1, q_2 - p_2) = (v_1 - u_1, v_2 - u_2) \\
&\Leftrightarrow \quad q_1 - p_1 = v_1 - u_1 \quad \text{and} \quad q_2 - p_2 = v_2 - u_2.
\end{aligned}$$

Thus $\overrightarrow{pq} \sim \overrightarrow{uv}$ in $\mathbb{R}^2$ if and only if the arrows corresponding to the two located vectors decompose into the same horizontal and vertical translations.

If $o = (0, \ldots, 0)$ is the origin in $\mathbb{R}^n$, $p = (p_1, \ldots, p_n)$, and $q = (q_1, \ldots, q_n)$, then

$$\overrightarrow{pq} \sim \overrightarrow{o(q - p)}.$$

This is verified by direct calculation:

$$q - p = (q_1 - p_1, q_2 - p_2) = (q_1 - p_1, q_2 - p_2) - (0, 0) = (q - p) - o.$$

Thus, any arbitrary location vector $\overrightarrow{pq}$ is equivalent to some position vector, and in the exercises it will be established that the position vector equivalent to $\overrightarrow{pq}$ must be unique.

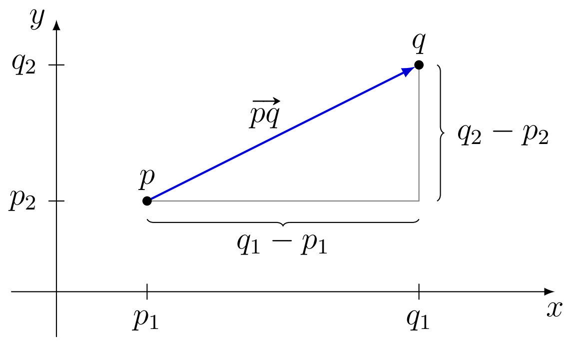



Figure 3. A vector in the plane $\mathbb{R}^2$ located at $p$.

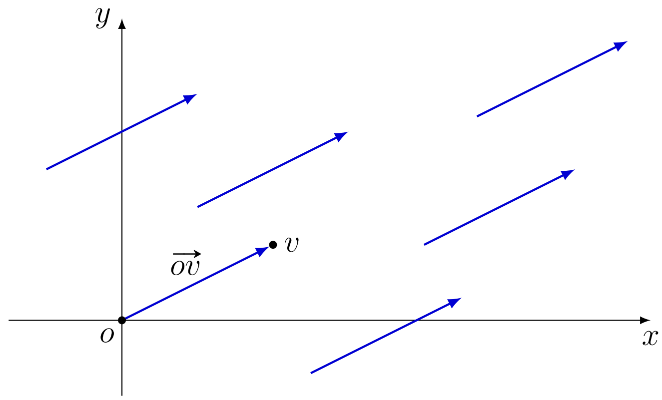



FIGURE 4. Equivalent located vectors, all belonging to $\mathbf{v}$.

**Definition 1.9.** *Let $\overrightarrow{ov}$ be a position vector in $\mathbb{R}^n$. The **equivalence class** of $\overrightarrow{ov}$, denoted by $\mathbf{v}$, is the set of all located vectors that are equivalent to $\overrightarrow{ov}$. That is,*

$$\mathbf{v} = \{\overrightarrow{pq} : \overrightarrow{ov} \sim \overrightarrow{pq}\}.$$

*The equivalence class $\mathbf{v}$ of a located vector $\overrightarrow{ov}$ is also called the **vector** $\mathbf{v}$.*

The symbol $\mathbf{v}$ is usually handwritten as $\vec{v}$. If $v = (v_1, \dots, v_n)$, then it is common to denote $\mathbf{v}$ by either

$$[v_1, \dots, v_n] \quad \text{or} \quad \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}.$$

The row format exhibited in the first symbol will be used throughout this chapter, but later on the column format of the second symbol will be favored. Thus $\mathbf{v} = [v_1, \dots, v_n]$ is the set of located vectors that are equivalent to the position vector having $v = (v_1, \dots, v_n)$ as its terminal point. A vector of the form $[v_1, \dots, v_n]$, where the $i$th **coordinate** $v_i$ is a real number for each $1 \leq i \leq n$, is called a **Euclidean vector** (or **coordinate vector**) to distinguish it from the more abstract notion of vector that will be introduced in Chapter 3. Put another way, a Euclidean vector is an equivalence class of located vectors in a Euclidean space $\mathbb{R}^n$, and it is fully determined by $n$ real-valued coordinates $v_1, \dots, v_n$.

The Euclidean **zero vector** is the vector $\mathbf{0}$ whose coordinates are all equal to 0; thus if $\mathbf{0} \in \mathbb{R}^n$, then

$$\mathbf{0} = [\underbrace{0, 0, \dots, 0}_{n \text{ zeros}}].$$

A useful way to think of a vector $\mathbf{v} \neq \mathbf{0}$ in Euclidean $n$-space is as an arrow with a fixed length and direction, but varying location. For instance we can take the located vector $\overrightarrow{ov}$, naturally depicted as an arrow with initial point at the origin $o$ and terminal point at the point $v$, and move the arrow around in a way that preserves its length and direction. See Figure 4.

**Remark.** If a located vector $\overrightarrow{pq}$ is equivalent to $\overrightarrow{ov}$, then strictly speaking we say that $\overrightarrow{pq}$ belongs to the equivalence class of located vectors known as vector $\mathbf{v}$. However, sometimes the symbol $\overrightarrow{pq}$ itself may be used to represent the vector $\mathbf{v}$, which is in keeping with the common practice

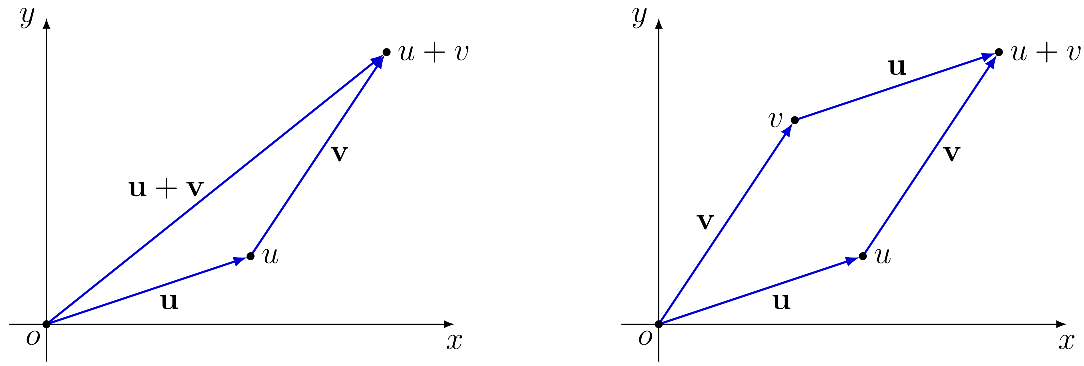



FIGURE 5. The geometry of vector addition.

in mathematics of letting any member of an equivalence class be a representative of that class. Other times we may be given a located vector $\overrightarrow{pq}$ in a situation when location is irrelevant, and so refer to $\overrightarrow{pq}$ as simply a vector.

**Example 1.10.** In $\mathbb{R}^3$ let $p = (2, -3, 4)$ and $q = (-5, -2, 8)$. Find $v = (v_1, v_2, v_3)$ so that $\overrightarrow{pq} \sim \overrightarrow{ov}$, where $o = (0, 0, 0)$.

**Solution.** By definition $\overrightarrow{pq} \sim \overrightarrow{ov}$ means $q - p = v - o$, or

$$(-5, -2, 8) - (2, -3, 4) = (v_1, v_2, v_3) - (0, 0, 0) = (v_1, v_2, v_3).$$

Thus we have

$$v = (v_1, v_2, v_3) = (-5 - 2, -2 - (-3), 8 - 4) = (-7, 1, 4).$$

It follows from this calculation that the located vector $\overrightarrow{pq}$ belongs to the equivalence class of located vectors known as the vector $\mathbf{v} = [-7, 1, 4]$. The symbol $\overrightarrow{pq}$ itself could be used to represent the vector $[-7, 1, 4]$, and we may even say that $\overrightarrow{pq}$ and $[-7, 1, 4]$ are the "same vector" if location in $\mathbb{R}^3$ is unimportant. ■

As with points we define operations that allow for adding and subtracting Euclidean vectors, and also multiplying them by real numbers.

**Definition 1.11.** *Let $\mathbf{u} = [u_1, \ldots, u_n]$ and $\mathbf{v} = [v_1, \ldots, v_n]$ be Euclidean vectors in $\mathbb{R}^n$, and $c \in \mathbb{R}$. Then we define the* ***sum*** $\mathbf{u} + \mathbf{v}$ *of* $\mathbf{u}$ *and* $\mathbf{v}$ *to be the vector*

$$\mathbf{u} + \mathbf{v} = [u_1 + v_1, \ldots, u_n + v_n],$$

*and the* ***scalar multiple*** $c\mathbf{v}$ *of* $\mathbf{v}$ *by $c$ to be the vector*

$$c\mathbf{v} = [cv_1, \ldots, cv_n].$$

*Defining $-\mathbf{v} = (-1)\mathbf{v}$, the* ***difference*** $\mathbf{u} - \mathbf{v}$ *of* $\mathbf{u}$ *and* $\mathbf{v}$ *is given to be*

$$\mathbf{u} - \mathbf{v} = \mathbf{u} + (-\mathbf{v}).$$

There is some geometrical significance to the sum of two vectors, and it suffices to consider the situation in $\mathbb{R}^2$ to appreciate it. Define vectors $\mathbf{u} = [u_1, u_2]$ and $\mathbf{v} = [v_1, v_2]$ in the plane. One representative of $\mathbf{u}$ is the located vector $\overrightarrow{ou}$. As for $\mathbf{v}$, from

$$(u+v) - u = u + v - u = v = v - o$$

we have

$$\overrightarrow{u(u+v)} \sim \overrightarrow{ov},$$

and so $\overrightarrow{u(u+v)}$ is a located vector—in fact the *only* located vector—having initial point $u$ that can represent $\mathbf{v}$. Finally, a representative for $\mathbf{u} + \mathbf{v}$ is the located vector

$$\overrightarrow{o(u+v)}.$$

Now, if the located vectors $\overrightarrow{ou}$, $\overrightarrow{u(u+v)}$, and $\overrightarrow{o(u+v)}$ are all drawn as arrows in $\mathbb{R}^2$, they will be seen to form a triangle such as the one at left in Figure 5. Indeed if $\overrightarrow{ov}$, also representing $\mathbf{v}$, and

$$\overrightarrow{v(u+v)}$$

—easily seen to be another representative of $\mathbf{u}$—are also drawn as arrows, then a parallelogram such as the one at right in Figure 5 results. In the figure, it should be pointed out, the various located vectors are labeled only by the vector ($\mathbf{u}$ or $\mathbf{v}$) that they represent.

After this section we will refer to located vectors only infrequently, and instead focus mostly on vectors. Until Chapter 3 the vectors will be strictly of the Euclidean variety, viewed naturally as arrows in $\mathbb{R}^n$ which have length and direction but no particular location. Also we will often use the symbol $\mathbb{R}^n$ to denote the set of all Euclidean vectors of the form $[x_1, \ldots, x_n]$, rather than the set of all points $(x_1, \ldots, x_n)$. That is,

$$\mathbb{R}^n = \{[x_1, \ldots, x_n] : x_i \in \mathbb{R} \text{ for } 1 \le i \le n\}.$$

There is no substantive difference between this definition for $\mathbb{R}^n$ and the one given by equation (1.1); there is only a difference in interpretation.

**Definition 1.12.** *Two vectors* $\mathbf{u}, \mathbf{v}$ *are* ***parallel*** *if there exists some scalar* $c \neq 0$ *such that* $\mathbf{u} = c\mathbf{v}$.

## 1.4 – The Dot Product

We have established operations that add and subtract vectors, and also multiply them by real numbers. Now we define a way of "multiplying" vectors that is known as the dot product.[1]

**Definition 1.13.** *Let* $\mathbf{u} = [u_1, \ldots, u_n]$ *and* $\mathbf{v} = [v_1, \ldots, v_n]$ *be two vectors in* $\mathbb{R}^n$*. Then the* ***dot product*** *of* $\mathbf{u}$ *and* $\mathbf{v}$ *is the real number*

$$\mathbf{u} \cdot \mathbf{v} = u_1v_1 + u_2v_2 + \cdots + u_nv_n = \sum_{i=1}^{n} u_iv_i.$$

Thus, if $\mathbf{u}$ and $\mathbf{v}$ are vectors in $\mathbb{R}^2$, then

$$\mathbf{u} \cdot \mathbf{v} = [u_1, u_2] \cdot [v_1, v_2] = u_1v_1 + u_2v_2.$$

Some properties of the dot product now follow.

**Theorem 1.14.** *For any vectors* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ *and scalar* $c$*,*

1. $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$
2. $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$
3. $(c\mathbf{u}) \cdot \mathbf{v} = c(\mathbf{u} \cdot \mathbf{v}) = \mathbf{u} \cdot (c\mathbf{v})$
4. $\mathbf{u} \cdot \mathbf{u} > 0$ *if* $\mathbf{u} \neq \mathbf{0}$

**Proof.** Proof of (2):

$$\begin{aligned}
\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) &= [u_1, \ldots, u_n] \cdot \big([v_1, \ldots, v_n] + [w_1, \ldots, w_n]\big) \\
&= [u_1, \ldots, u_n] \cdot [v_1 + w_1, \ldots, v_n + w_n] \\
&= \sum_{i=1}^{n} u_i(v_i + w_i) = \sum_{i=1}^{n} (u_iv_i + u_iw_i) \\
&= \sum_{i=1}^{n} u_iv_i + \sum_{i=1}^{n} u_iw_i = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w},
\end{aligned}$$

using the established summation property $\sum(a_i + b_i) = \sum a_i + \sum b_i$.

Proofs for the other dot product properties are left to the exercises. ∎

**Definition 1.15.** *Two vectors* $\mathbf{u}$*,* $\mathbf{v}$ *are* ***orthogonal****, written* $\mathbf{u} \perp \mathbf{v}$*, if* $\mathbf{u} \cdot \mathbf{v} = 0$.

Orthogonal vectors are also said to be **perpendicular**, and in the next section we shall see that this means precisely what we expect: the vectors form a right angle.

**Example 1.16.** Find two mutually perpendicular vectors in $\mathbb{R}^3$ that are each perpendicular to $\mathbf{v} = [2, -1, 3]$

[1] The dot product is also called the "scalar product" in some books.

**Solution.** We need to find vectors $\mathbf{u} = [u_1, u_2, u_3]$ and $\mathbf{w} = [w_1, w_2, w_3]$ such that

$$\mathbf{u} \cdot \mathbf{w} = \mathbf{u} \cdot \mathbf{v} = \mathbf{w} \cdot \mathbf{v} = 0.$$

From this we obtain a system of equations:

$$\begin{cases} 2u_1 - \quad u_2 + \quad 3u_3 = 0 \\ 2w_1 - \quad w_2 + \quad 3w_3 = 0 \\ u_1w_1 + u_2w_2 + u_3w_3 = 0 \end{cases}$$

There are six variables but only three equations, and so we can expect that there are an infinite number of solutions. To satisfy the third equation we may choose, quite arbitrarily, to let $u_1w_1 = 1$, $u_2w_2 = -2$, and $u_3w_3 = 1$, so that

$$w_1 = \frac{1}{u_1}, \quad w_2 = -\frac{2}{u_2}, \quad \text{and} \quad w_3 = \frac{1}{u_3}. \tag{1.2}$$

Substituting these into the system's second equation yields

$$\frac{2}{u_1} + \frac{2}{u_2} + \frac{3}{u_3} = 0. \tag{1.3}$$

Now, from the system's first equation we have $u_2 = 2u_1 + 3u_3$, which we substitute into (1.3) to obtain

$$\frac{2}{u_1} + \frac{2}{2u_1 + 3u_3} + \frac{3}{u_3} = 0.$$

From this, with a little algebra, we obtain a quadratic equation:

$$2u_3^2 + 5u_1u_3 + 2u_1^2 = 0.$$

We employ the quadratic formula to solve this equation for $u_3$:

$$u_3 = \frac{-5u_1 \pm \sqrt{25u_1^2 - 4(2)(2u_1^2)}}{2(2)} = \frac{-5u_1 \pm 3|u_1|}{4}.$$

If we set $u_1 = 1$ (again an arbitrary choice we're free to make), then we find that

$$u_3 = \frac{-5 \pm 3}{4} = -2, \ -\frac{1}{2}.$$

If we choose $u_3 = -2$, then we have

$$u_2 = 2u_1 + 3u_3 = 2(1) + 3(-2) = -4,$$

and so $\mathbf{u} = [1, -4, -2]$. Also from (1.2) we have

$$\mathbf{w} = \left[\frac{1}{u_1}, -\frac{2}{u_2}, \frac{1}{u_3}\right] = \left[1, \frac{1}{2}, -\frac{1}{2}\right].$$

Therefore

$$[1, -4, -2] \quad \text{and} \quad \left[1, \frac{1}{2}, -\frac{1}{2}\right]$$

are two mutually perpendicular vectors that are each perpendicular to $[2, -1, 3]$. There are infinitely many other possibilities. ■

## 1.5 – The Norm of a Vector

**Definition 1.17.** *The **norm** of a vector* $\mathbf{v} \in \mathbb{R}^n$ *is* $\|\mathbf{v}\| = \sqrt{\mathbf{v} \cdot \mathbf{v}}$.

If $\mathbf{v} = [v_1, \ldots, v_n]$, then

$$\|\mathbf{v}\| = \sqrt{[v_1, \ldots, v_n] \cdot [v_1, \ldots, v_n]} = \sqrt{\sum_{i=1}^{n} v_i^2} \tag{1.4}$$

The norm of a vector is also known as the vector's **magnitude** or **length**. Consider a located vector $\overrightarrow{ov}$ in the plane, which is a convenient representative of the vector $\mathbf{v} = [v_1, v_2]$. In §1.2 we saw that $\overrightarrow{ov}$ may be depicted as an arrow that starts at the origin $o = (0, 0)$ and ends at the point $v = (v_1, v_2)$. How long is the arrow? The answer is given by the conventional (Euclidean) distance $d(o, v)$ between $o$ and $v$ that is derived from the familiar Pythagorean Theorem:

$$d(o, v) = \sqrt{(v_1 - 0)^2 + (v_2 - 0)^2} = \sqrt{v_1^2 + v_2^2}.$$

On the other hand from (1.4) we have

$$\|\mathbf{v}\| = \sqrt{v_1^2 + v_2^2},$$

and so $\|\mathbf{v}\| = d(o, v)$, the length of the arrow $\overrightarrow{ov}$ representing $\mathbf{v}$. Note that if $\overrightarrow{pq} \sim \overrightarrow{ov}$, where $p = (p_1, p_2)$ and $q = (q_1, q_2)$, then

$$d(p, q) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2} = \sqrt{v_1^2 + v_2^2} = d(o, v) = \|\mathbf{v}\|$$

since $q_1 - p_1 = v_1$ and $q_2 - p_2 = v_2$, and so it does not matter which located vector we choose to represent $\mathbf{v}$: the length of the arrow will be the same! These truths stay true in $\mathbb{R}^3$ using the usual Euclidean conception of distance in three-dimensional space. In fact, in light of the following definition they remain true in $\mathbb{R}^n$ for all $n$.

**Definition 1.18.** *Let* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. *The **distance*** $d(\mathbf{x}, \mathbf{y})$, *between* $\mathbf{x}$ *and* $\mathbf{y}$ *is given by*

$$d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|.$$

Thus if $\mathbf{x} = [x_1, \ldots, x_n]$ and $\mathbf{y} = [y_1, \ldots, y_n]$, then

$$d(\mathbf{x}, \mathbf{y}) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2},$$

which reduces to the usual formula for the distance between points $x$ and $y$ when $n$ equals 2 or 3. That is, $d(\mathbf{x}, \mathbf{y}) = d(x, y)$ in $\mathbb{R}^2$ or $\mathbb{R}^3$.

**Remark.** From now on we will frequently use the bold-faced symbol $\mathbf{x}$ for the *vector* $[x_1, \ldots, x_n]$ to represent the *point* $x = (x_1, \ldots, x_n)$. The logic of doing this is thus: a point $x$ is naturally identified with its corresponding position vector $\overrightarrow{ox}$, and $\overrightarrow{ox}$ is naturally identified with $\mathbf{x}$. Such "vectorization" of points allows for a uniform notation in the statement of momentous results in vector calculus and the sciences. Moreover it places everything under consideration in the setting of a "vector space," which is the main object of study in linear algebra. So it must be

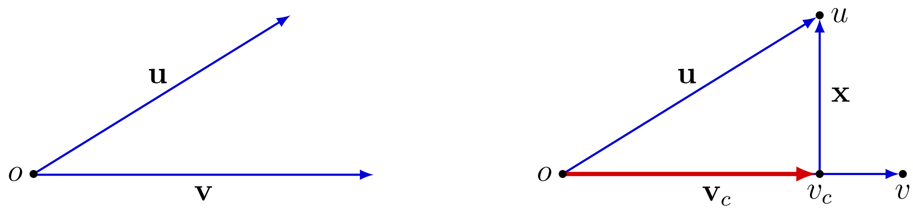



FIGURE 6.

remembered: depending on context, $\mathbf{x} = [x_1, \ldots, x_n]$ may be interpreted as a vector, a located vector, or a point![2]

We are now in a position to justify Definition 1.15, by which we mean ground the definition in more familiar geometric soil. Suppose $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ are orthogonal vectors, which is to say $\mathbf{u} \cdot \mathbf{v} = 0$ and (since the dot product is commutative) $\mathbf{v} \cdot \mathbf{u} = 0$. Recall that located vectors representing $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{u} + \mathbf{v}$ may be chosen so that their corresponding arrows form a triangle, as at left in Figure 5. A triangle is a planar figure so it does not matter if the located vectors are in an $n$-space for some $n > 2$: we can always orient the situation so that it lies on a plane. Now, $\|\mathbf{u} + \mathbf{v}\|$ is the length of the longest side of the triangle, and $\|\mathbf{u}\|$ and $\|\mathbf{v}\|$ are the lengths of the shorter sides. From the calculation

$$\begin{aligned}\|\mathbf{u} + \mathbf{v}\|^2 &= \left(\sqrt{(\mathbf{u} + \mathbf{v}) \cdot (\mathbf{u} + \mathbf{v})}\right)^2 = (\mathbf{u} + \mathbf{v}) \cdot (\mathbf{u} + \mathbf{v}) \\ &= (\mathbf{u} + \mathbf{v}) \cdot \mathbf{u} + (\mathbf{u} + \mathbf{v}) \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{u} + \mathbf{v} \cdot \mathbf{u} + \mathbf{u} \cdot \mathbf{v} + \mathbf{v} \cdot \mathbf{v} \\ &= \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2,\end{aligned}$$

it can be seen that the lengths of the triangle's sides obey the Pythagorean Theorem, and so it must be that the triangle is a right triangle. That is, the sides formed by the located vectors representing $\mathbf{u}$ and $\mathbf{v}$ must meet at a right angle and therefore be perpendicular! It is in this sense that orthogonal vectors are also said to be "perpendicular."

**Proposition 1.19.** *If $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ are orthogonal vectors, then $\|\mathbf{u} + \mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2$.*

The proof has already been furnished above.

**Definition 1.20.** *Let $\mathbf{v} \neq \mathbf{0}$. The **orthogonal projection of $\mathbf{u}$ onto $\mathbf{v}$**, $\operatorname{proj}_{\mathbf{v}} \mathbf{u}$, is given by*

$$\operatorname{proj}_{\mathbf{v}} \mathbf{u} = \left(\frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}}\right)\mathbf{v}.$$

Once again it should help to ground the definition in geometry, because ultimately it is geometry that motivates the definition. Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ with $\mathbf{v} \neq \mathbf{0}$. We represent these vectors by located vectors with common initial point $o$ as at left in Figure 6. For any $c \in \mathbb{R}$ let $\mathbf{v}_c = c\mathbf{v}$. We wish to find the value for $c$ so that the vector $\mathbf{x}$ represented by located vector $\overrightarrow{v_c u}$ at right in Figure 6 is orthogonal to $\mathbf{v}$. This means $c$ must be such that $\mathbf{x} \cdot \mathbf{v} = 0$, and since $\mathbf{v}_c + \mathbf{x} = \mathbf{u}$ we obtain

$$(\mathbf{u} - \mathbf{v}_c) \cdot \mathbf{v} = 0$$

[2]It was Henri Poincaré who said "Mathematics is the art of giving the same name to different things."

and thus

$$\mathbf{u} \cdot \mathbf{v} - \mathbf{v}_c \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{v} - (c\mathbf{v}) \cdot \mathbf{v} = 0.$$

Since $(c\mathbf{v}) \cdot \mathbf{v} = c(\mathbf{v} \cdot \mathbf{v})$ we finally arrive at

$$c = \frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}}. \tag{1.5}$$

Now, consider the right side of Figure 6 again. It can be seen that the vector $\mathbf{v}_c$, as pictured, would be the shadow that $\mathbf{u}$ would cast upon $\mathbf{v}$ were a light to be directed upon the scene from directly overhead. It is in this sense that $\mathbf{v}_c$ is a projection of $\mathbf{u}$ onto $\mathbf{v}$—in particular the *orthogonal* projection, since the "light rays" casting the "shadow" are perpendicular to $\mathbf{v}$. Multiplying both sides of equation (1.5) by $\mathbf{v}$ gives

$$\mathbf{v}_c = \left(\frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}}\right)\mathbf{v},$$

which is $\operatorname{proj}_{\mathbf{v}} \mathbf{u}$ as given in Definition 1.20.

**Lemma 1.21.** *If* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, $\mathbf{v} \neq \mathbf{0}$, *and* $c$ *is as in* (1.5), *then* $\mathbf{u} - c\mathbf{v}$ *is orthogonal to* $\mathbf{v}$.

**Proof.** Taking the dot product,

$$(\mathbf{u} - c\mathbf{v}) \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{v} - c(\mathbf{v} \cdot \mathbf{v}) = \mathbf{u} \cdot \mathbf{v} - \left(\frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}}\right)(\mathbf{v} \cdot \mathbf{v}) = \mathbf{u} \cdot \mathbf{v} - \mathbf{u} \cdot \mathbf{v} = 0,$$

we immediately conclude that $\mathbf{u} - c\mathbf{v} \perp \mathbf{v}$. ■

It's a worthwhile exercise to verify that if $\mathbf{u} \perp \mathbf{v}$, then $\mathbf{u} \perp a\mathbf{v}$ for any scalar $a$. The lemma will be used to prove the following.

**Theorem 1.22 (Schwarz Inequality).** *If* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, *then* $|\mathbf{u} \cdot \mathbf{v}| \leq \|\mathbf{u}\|\|\mathbf{v}\|$.

**Proof.** Suppose $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$. If $\mathbf{u} = \mathbf{0}$ or $\mathbf{v} = \mathbf{0}$, then

$$|\mathbf{u} \cdot \mathbf{v}| = |0| = 0 = \|\mathbf{u}\|\|\mathbf{v}\|,$$

which affirms the theorem's conclusion. So, suppose $\mathbf{u}, \mathbf{v} \neq \mathbf{0}$, and let $c \in \mathbb{R}$ be given by (1.5). Now,

$$(\mathbf{u} - c\mathbf{v}) \cdot (c\mathbf{v}) = c[(\mathbf{u} - c\mathbf{v}) \cdot \mathbf{v}] = c(0) = 0,$$

where $(\mathbf{u} - c\mathbf{v}) \cdot \mathbf{v} = 0$ by Lemma 1.21. Thus $\mathbf{u} - c\mathbf{v}$ and $c\mathbf{v}$ are orthogonal, and by Proposition 1.19

$$\|\mathbf{u}\|^2 = \|(\mathbf{u} - c\mathbf{v}) + c\mathbf{v}\|^2 = \|\mathbf{u} - c\mathbf{v}\|^2 + \|c\mathbf{v}\|^2.$$

Since $\|\mathbf{u} - c\mathbf{v}\|^2 \geq 0$, this implies that $\|c\mathbf{v}\|^2 \leq \|\mathbf{u}\|^2$. However,

$$\|c\mathbf{v}\|^2 = c^2\|\mathbf{v}\|^2 = \left(\frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}}\right)^2(\mathbf{v} \cdot \mathbf{v}) = \frac{(\mathbf{u} \cdot \mathbf{v})^2}{\mathbf{v} \cdot \mathbf{v}} = \frac{(\mathbf{u} \cdot \mathbf{v})^2}{\|\mathbf{v}\|^2},$$

and so from $\|c\mathbf{v}\|^2 \leq \|\mathbf{u}\|^2$ we obtain

$$\frac{(\mathbf{u} \cdot \mathbf{v})^2}{\|\mathbf{v}\|^2} \leq \|\mathbf{u}\|^2,$$

whence comes $(\mathbf{u} \cdot \mathbf{v})^2 \leq \|\mathbf{u}\|^2\|\mathbf{v}\|^2$. Taking the square root of both sides completes the proof. ■

From the Schwarz inequality we have

$$-\|\mathbf{u}\|\|\mathbf{v}\| \le \mathbf{u}\cdot\mathbf{v} \le \|\mathbf{u}\|\|\mathbf{v}\|,$$

and thus

$$-1 \le \frac{\mathbf{u}\cdot\mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|} \le 1$$

for any $\mathbf{u}, \mathbf{v} \neq 0$. This observation justifies the following definition.

**Definition 1.23.** *Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ be nonzero vectors. The **angle** between $\mathbf{u}$ and $\mathbf{v}$ is the number $\theta \in [0, \pi]$ for which*

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|}. \tag{1.6}$$

Since the function $\cos : [0, \pi] \to [-1, 1]$ is one-to-one and onto, and the fraction in (1.6) only takes values in $[-1, 1]$, there will always exist a *unique* value $\theta \in [0, \pi]$ that satisfies (1.6). From Definition 1.23 we have a new formula for the dot product:

$$\mathbf{u}\cdot\mathbf{v} = \|\mathbf{u}\|\|\mathbf{v}\|\cos\theta. \tag{1.7}$$

Some textbooks give this formula as the *definition* of the dot product, but it is less desirable since the idea of a dot product is then founded on a geometric notion of angle that becomes problematic to visualize in $\mathbb{R}^n$ for $n > 3$. However it is worthwhile verifying that the definition of angle between vectors, as given here, agrees with our geometric intuition. For the sake of simplicity we can assume that $\mathbf{u}$ and $\mathbf{v}$ are nonzero vectors in $\mathbb{R}^2$, though the situation does not alter in $\mathbb{R}^n$ for $n > 2$ since two vectors can always be represented by coplanar located vectors.[3] The approach will be to let $\theta$ be the geometric angle between $\mathbf{u}$ and $\mathbf{v}$, and then show that (1.7) must necessarily follow.

Let $0 < \theta < \pi$. The vectors $\mathbf{u}$, $\mathbf{v}$, and $\mathbf{u} - \mathbf{v}$ may be represented by located vectors that form the triangle in Figure 7 (for convenience we depict $\theta$ as an acute angle).

By the Law of Cosines we obtain

$$\|\mathbf{u} - \mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\|\mathbf{u}\|\|\mathbf{v}\|\cos\theta,$$

and since we're assuming that $\mathbf{u} = [u_1, u_2]$ and $\mathbf{v} = [v_1, v_2]$, we obtain $\mathbf{u} - \mathbf{v} = [u_1 - v_1, u_2 - v_2]$ so that

$$(u_1 - v_1)^2 + (u_2 - v_2)^2 = (u_1^2 + u_2^2) + (v_1^2 + v_2^2) - 2\|\mathbf{u}\|\|\mathbf{v}\|\cos\theta,$$

[3] This is because two located vectors can be defined by three points $p$, $q$, and $r$, such as $\overrightarrow{pq}$ and $\overrightarrow{pr}$, and three points define a plane.

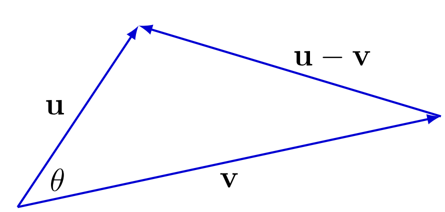



FIGURE 7.

and hence

$$\|\mathbf{u}\|\|\mathbf{v}\|\cos\theta = u_1v_1 + u_2v_2 = \mathbf{u}\cdot\mathbf{v}.$$

In the cases when $\theta = 0$ or $\theta = \pi$ we find that $\mathbf{v} = k\mathbf{u} = [ku_1, ku_2]$ for some nonzero scalar $k$; that is, $\mathbf{u}$ and $\mathbf{v}$ are parallel vectors, and we have

$$\|\mathbf{u}\|\|\mathbf{v}\|\cos\theta = \|\mathbf{u}\|\|k\mathbf{u}\|\cos\theta = |k|(u_1^2 + u_2^2)\cos\theta. \tag{1.8}$$

If $\theta = 0$, then $k > 0$ so that $|k| = k$ and $\cos\theta = 1$; and if $\theta = \pi$, then $k < 0$ so that $|k| = -k$ and $\cos\theta = -1$. In either case, from (1.8) we obtain

$$\|\mathbf{u}\|\|\mathbf{v}\|\cos\theta = k(u_1^2 + u_2^2) = [u_1, u_2]\cdot[ku_1, ku_2] = \mathbf{u}\cdot\mathbf{v}$$

as desired.

**Example 1.24.** Let $\mathbf{u} = [2, -1, 5]$ and $\mathbf{v} = [-1, 1, 1]$.
(a) Find $\|\mathbf{u}\|$ and $\|\mathbf{v}\|$.
(b) Find $\operatorname{proj}_{\mathbf{v}}\mathbf{u}$, the orthogonal projection of $\mathbf{u}$ onto $\mathbf{v}$.
(c) Find $\operatorname{proj}_{\mathbf{u}}\mathbf{v}$, the orthogonal projection of $\mathbf{v}$ onto $\mathbf{u}$.
(d) Find the angle between $\mathbf{u}$ and $\mathbf{v}$ to the nearest tenth of a degree.

**Solution.**
(a) We have

$$\|\mathbf{u}\| = \sqrt{2^2 + (-1)^2 + 5^2} = \sqrt{30} \quad \text{and} \quad \|\mathbf{v}\| = \sqrt{(-1)^2 + 1^2 + 1^2} = \sqrt{3}.$$

(b) Since

$$\mathbf{u}\cdot\mathbf{v} = (2)(-1) + (-1)(1) + (5)(1) = 2 \quad \text{and} \quad \mathbf{v}\cdot\mathbf{v} = \|\mathbf{v}\|^2 = (\sqrt{3})^2 = 3,$$

we have

$$\operatorname{proj}_{\mathbf{v}}\mathbf{u} = \left(\frac{\mathbf{u}\cdot\mathbf{v}}{\mathbf{v}\cdot\mathbf{v}}\right)\mathbf{v} = \frac{2}{3}[-1, 1, 1] = \left[-\frac{2}{3}, \frac{2}{3}, \frac{2}{3}\right].$$

(c) Since

$$\mathbf{v}\cdot\mathbf{u} = \mathbf{u}\cdot\mathbf{v} = 2 \quad \text{and} \quad \mathbf{u}\cdot\mathbf{u} = \|\mathbf{u}\|^2 = (\sqrt{30})^2 = 30,$$

we have

$$\operatorname{proj}_{\mathbf{u}}\mathbf{v} = \left(\frac{\mathbf{v}\cdot\mathbf{u}}{\mathbf{u}\cdot\mathbf{u}}\right)\mathbf{u} = \frac{2}{30}[2, -1, 5] = \left[\frac{2}{15}, -\frac{1}{15}, \frac{1}{3}\right].$$

(d) By definition,

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|} = \frac{2}{\sqrt{30}\sqrt{3}} = \frac{2}{3\sqrt{10}},$$

and thus

$$\theta = \cos^{-1}\left(\frac{2}{3\sqrt{10}}\right) \approx 77.8^\circ.$$

■

**Example 1.25.** Find the measure of the angle $\theta$ between the diagonal of a cube and the diagonal of one of its faces, as shown in Figure 8.

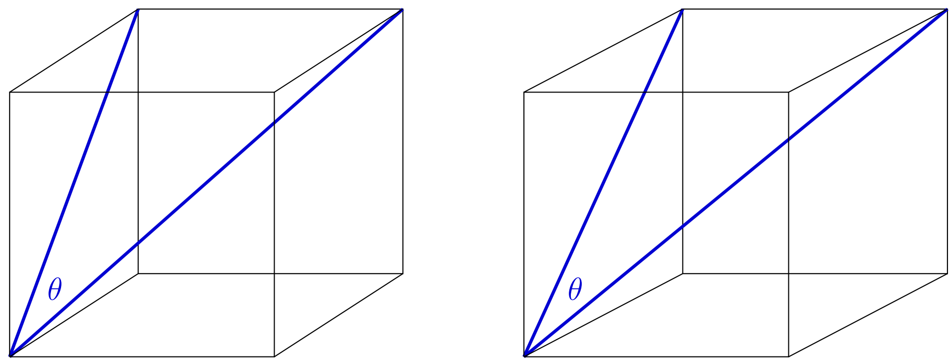



Figure 8.

**Solution.** It will be convenient to regard the cube as existing in $\mathbb{R}^3$, with edges of length 1, and the vertex where the two diagonals meet situated at the origin $(0, 0, 0)$. We can then set up coordinate axes such that the cube diagonal has endpoints $(0, 0, 0)$ and $(1, 1, 1)$, and the face diagonal has endpoints $(0, 0, 0)$ and $(0, 1, 1)$. Thus the diagonals can be characterized as positions vectors $\mathbf{u} = [1, 1, 1]$ and $\mathbf{v} = [0, 1, 1]$. Now,

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|} = \frac{[1,1,1]\cdot[0,1,1]}{\sqrt{1^2+1^2+1^2}\sqrt{0^2+1^2+1^2}} = \frac{2}{\sqrt{6}},$$

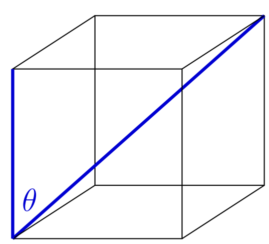
and so

$$\theta = \cos^{-1}\left(\frac{2}{\sqrt{6}}\right) \approx 35.264^\circ$$

is the angle's measure. ■

## Problems

1. Find the measure of the angle $\theta$ between the diagonal of a cube and one of its edges, as shown below.



## 1.6 – Lines and Planes

In $\mathbb{R}^2$ a line $L$ is typically defined to be the solution set to an equation of the form $ax+by=c$ for constants $a,b,c\in\mathbb{R}$, where $a$ and $b$ are not both zero. That is, $L$ is the set of points

$$\{(x,y) : ax+by=C\},$$

and $ax+by=C$ is called the **Cartesian equation** (or **algebraic equation**) for $L$. In $\mathbb{R}^n$ for $n>2$ we can still speak geometrically of lines, of course, but it becomes impossible to define the line using a single Cartesian equation. The most convenient remedy for this is to use vectors, thereby motivating the following definition.

**Definition 1.26.** *Let $\mathbf{p},\mathbf{v}\in\mathbb{R}^n$ with $\mathbf{v}\neq\mathbf{0}$. The **line** through $\mathbf{p}$ and parallel to $\mathbf{v}\in\mathbb{R}^n$ is the set of vectors of the form*

$$\{\mathbf{p}+t\mathbf{v} : t\in\mathbb{R}\}.$$

A **parametric equation** (or **parametrization**) of a line $L=\{\mathbf{p}+t\mathbf{v} : t\in\mathbb{R}\}\subseteq\mathbb{R}^n$ is any vector-valued function $\mathbf{x}:\mathbb{R}\to\mathbb{R}^n$ given by

$$\mathbf{x}(t)=\tilde{\mathbf{p}}+t\tilde{\mathbf{v}}$$

for some $\tilde{\mathbf{p}}\in L$ and vector $\tilde{\mathbf{v}}$ parallel to $\mathbf{v}$. (Here $t$ is called a **parameter**.) Thus we find that

$$\mathbf{x}(t)=\mathbf{p}+t\mathbf{v}$$

is one parametrization for $L$, but there are infinitely many others in existence.

Given a parametrization $\mathbf{x}(t)=\mathbf{p}+t\mathbf{v}$ for some line in $\mathbb{R}^n$, the vector $\mathbf{p}=[p_1,\ldots,p_n]$ may more naturally be thought of as the position vector $\overrightarrow{op}$ of the point $p=(p_1,\ldots,p_n)$, and so in everyday speech $\mathbf{p}$ may be referred to as a point even though mathematically it is handled as a vector. The same applies to the vector

$$\mathbf{x}(t)=[x_1(t),\ldots,x_n(t)]$$

for each $t\in\mathbb{R}$: we may regard it, if desired, as the position vector of the point

$$x(t)=(x_1(t),\ldots,x_n(t)),$$

and so refer to it as a point. In contrast, for each $t\in\mathbb{R}$ the vector $t\mathbf{v}$ may be thought of as a localized vector (i.e. an arrow) with initial point at $p$ and terminal point located at another point on the line.

**Definition 1.27.** *The **line segment** in $\mathbb{R}^n$ with endpoints $\mathbf{p},\mathbf{q}\in\mathbb{R}^n$ is the set of vectors of the form*

$$\{\mathbf{p}+t(\mathbf{q}-\mathbf{p}) : t\in[0,1]\}.$$

A natural parametrization for a line segment with endpoints $\mathbf{p}$ and $\mathbf{q}$ is the vector-valued function $\mathbf{x}:[0,1]\to\mathbb{R}^n$ given by

$$\mathbf{x}(t)=\mathbf{p}+t(\mathbf{q}-\mathbf{p}), \tag{1.9}$$

though it is frequently the case in applications that other parametrizations may be considered. In (1.9) we have $\mathbf{x}(0) = \mathbf{p}$ and $\mathbf{x}(1) = \mathbf{q}$, and so as $t$ increases from 0 to 1 we see that we "travel" along the line segment from $\mathbf{p}$ to $\mathbf{q}$. However, the alternative parametrization

$$\mathbf{x}(t) = \mathbf{q} + t(\mathbf{p} - \mathbf{q})$$

reverses the direction of travel.

**Example 1.28.** Find a parametrization $\mathbf{x}(t)$ of the line containing the points $p = (2, -6, 9)$ and $q = (0, 8, 1)$, such that $\mathbf{x}(1) = \mathbf{p}$ and $\mathbf{x}(-2) = \mathbf{q}$.

**Solution.** We must have $\mathbf{x}(t) = \mathbf{p} + f(t)(\mathbf{q} - \mathbf{p})$ for some function $f$ such that $f(1) = 0$ and $f(-2) = 1$. The simplest such function is a linear one, which is to say $f(t) = mt + b$ for constants $m$ and $b$. With the condition $f(1) = 0$ we obtain $b = -m$, so that $f(t) = m(t-1)$. With the condition $f(-2) = 1$ we obtain $1 = m(-2-1)$, or $m = -1/3$, and hence $b = 1/3$. Now we have

$$\mathbf{x}(t) = \mathbf{p} + \big(-\tfrac{1}{3}t + \tfrac{1}{3}\big)(\mathbf{q} - \mathbf{p})$$

for $\mathbf{p} = [2, -6, 9]$ and $\mathbf{q} = [0, 8, 1]$, giving

$$\mathbf{x}(t) = \big[\tfrac{4}{3}, -\tfrac{4}{3}, \tfrac{19}{3}\big] + t\big[\tfrac{2}{3}, -\tfrac{14}{3}, \tfrac{8}{3}\big].$$

Other answers are possible if we choose $f$ to be a nonlinear function. ■

In $\mathbb{R}^3$ a line $P$ is sometimes defined to be the solution set to an equation of the form $ax + by + cz = d$ for constants $a, b, c, d \in \mathbb{R}$, where $a$, $b$, $c$ are not all zero. That is, $P$ is the set of points

$$\{(x, y, z) : ax + by + cz = d\},$$

where $ax + by + cz = d$ is the **Cartesian equation** for $P$. In $\mathbb{R}^n$ for $n > 3$ we may still wish to conceive of planes, but it is no longer possible to define the plane using a single Cartesian equation. The following definition uses vectors to define the notion of a plane for all $\mathbb{R}^n$ with $n \geq 3$.

**Definition 1.29.** *Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ be nonzero, nonparallel vectors. The **plane** through point $\mathbf{p} \in \mathbb{R}^n$ and parallel to $\mathbf{u}, \mathbf{v}$ is the set of vectors of the form*

$$\{\mathbf{p} + s\mathbf{u} + t\mathbf{v} : s, t \in \mathbb{R}\}.$$

A **parametric equation** (or **parametrization**) of a plane $P = \{\mathbf{p} + s\mathbf{u} + t\mathbf{v} : t \in \mathbb{R}\} \subseteq \mathbb{R}^n$ is any vector-valued function $\mathbf{x} : \mathbb{R}^2 \to \mathbb{R}^n$ given by

$$\mathbf{x}(s, t) = \tilde{\mathbf{p}} + s\tilde{\mathbf{u}} + t\tilde{\mathbf{v}}$$

for some $\tilde{\mathbf{p}} \in P$ and vectors $\tilde{\mathbf{u}}$ and $\tilde{\mathbf{v}}$ parallel to $\mathbf{u}$ and $\mathbf{v}$, respectively. (Here and $s$ and $t$ are called the **parameters**.) Thus

$$\mathbf{x}(s, t) = \mathbf{p} + s\mathbf{u} + t\mathbf{v} \tag{1.10}$$

is one parametrization for $P$ among infinitely many.

A **normal vector** for a plane $P$ having parametrization (1.10) is a nonzero vector $\mathbf{n}$ such that $\mathbf{n} \cdot \mathbf{u} = 0$ and $\mathbf{n} \cdot \mathbf{v} = 0$. A line $L$ is said to be **orthogonal** to $P$ if $L$ is parallel to $\mathbf{n}$. If $L$

is orthogonal to $P$ and $p \in L \cap P$ (i.e. $p$ is the point of intersection between $L$ and $P$), then the **distance** between any point $q \in L$ and $P$ is the length of the line segment $\overline{pq}$.

**Example 1.30.** Find both a parametric and Cartesian equation for the plane $P$ containing the point $(0,0,0)$ that is orthogonal to the line $L$ having parametric equation

$$\mathbf{x}(t) = [3,-2,1] + t[2,1,-3].$$

**Solution.** By definition any normal vector $\mathbf{n}$ for $P$ must be parallel to $L$, which in turn means that $\mathbf{n}$ must be parallel to a direction vector of $L$. Since $[2,1,-3]$ is an obvious direction vector of $L$, we may let $\mathbf{n} = [2,1,-3]$. Geometrically speaking, since $P$ contains the point $o = (0,0,0)$, $P$ will consist precisely of those points $(x,y,z)$ for which the vector $[x,y,z] - [0,0,0] = [x,y,z]$ is orthogonal to $\mathbf{n}$. Since

$$\mathbf{n} \cdot [x,y,z] = 0 \quad \Leftrightarrow \quad [2,1,-3] \cdot [x,y,z] = 0 \quad \Leftrightarrow \quad 2x + y - 3z = 0,$$

we conclude that $2x + y - 3z = 0$ is a Cartesian equation for $P$.

To find a parametric equation, we use the Cartesian equation to find two other points on $P$ besides $(0,0,0)$, such as $p = (1,-2,0)$ and $q = (0,3,1)$. Now let

$$\mathbf{u} = \mathbf{p} - \mathbf{0} = [1,-2,0] \quad \text{and} \quad \mathbf{v} = \mathbf{q} - \mathbf{0} = [0,3,1].$$

A parametric equation for $P$ is $\mathbf{x}(s,t) = \mathbf{0} + s\mathbf{u} + t\mathbf{v}$, or

$$\mathbf{x}(s,t) = s[1,-2,0] + t[0,3,1]$$

for $s,t \in \mathbb{R}$. ■

**Example 1.31.** Find a normal vector for the plane $3x + 2y - 2z = 3$.

**Solution.** We first find three points on the plane that are not collinear. This can be done by substituting values for $x$ and $y$ in the equation, say, and then solving for $z$. In this way we find points $(0,0,1/7)$, $(1,1,1)$, and $(1,2,2)$.

**Example 1.32.** Find the distance between the point $q = (1,-2,4)$ and the plane $3x+2y-2z = 3$.

**Solution.** Letting $x = y = 0$ in the plane's equation gives $z = 1/7$, so $p = (0,0,1/7)$ is a point on the plane. Let

$$\mathbf{v} = \overrightarrow{pq} = \mathbf{q} - \mathbf{p} = \left[5, 2, -\tfrac{22}{7}\right].$$

A normal vector for the plane is $\mathbf{n} = [4,-4,7]$. We project $\mathbf{v}$ onto $\mathbf{n}$:

$$\operatorname{proj}_{\mathbf{n}}(\mathbf{v}) = \left(\frac{\mathbf{v} \cdot \mathbf{n}}{\mathbf{n} \cdot \mathbf{n}}\right)\mathbf{n} = -\tfrac{10}{81}[4,-4,7].$$

The magnitude of this vector,

$$D = \|\operatorname{proj}_{\mathbf{n}}(\mathbf{v})\| = \tfrac{10}{9},$$

is the sought-after distance. ■

## Problems

1. Let $L_1$ be the line given by $\mathbf{x}(t) = [1, 1, 1] + t[2, 1, -1]$, and let $L_2$ be the line with Cartesian equations
$$x = 5, \quad y - 4 = \frac{z-1}{2}.$$
   (a) Show that the lines $L_1$ and $L_2$ intersect, and find the point of intersection.
   (b) Find a Cartesian equation of the plane containing $L_1$ and $L_2$.

2. Let $P$ be the plane in $\mathbb{R}^3$ which has normal vector $\mathbf{n} = [1, -4, 2]$ and contains the point $a = (5, 1, 3)$.
   (a) Find a Cartesian equation for $P$.
   (b) Find a parametric equation for $P$.

# 2

# Matrices and Systems

## 2.1 – Matrices

Let $m, n \in \mathbb{N}$, and let $\mathbb{F}$ be a field. An $\boldsymbol{m \times n}$ **matrix over** $\mathbb{F}$ is a rectangular array of elements of $\mathbb{F}$ arranged in $m$ rows and $n$ columns:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}. \tag{2.1}$$

The values $m$ and $n$ are called the **dimensions** of the matrix. The scalar (i.e. element of $\mathbb{F}$) in the $i$th row and $j$th column of the matrix, $a_{ij}$, is known as the $\boldsymbol{ij}$**-entry**. To be clear, throughout these notes the entries $a_{ij}$ of a matrix are always taken to be elements of some field $\mathbb{F}$, which could be the real number system $\mathbb{R}$, the complex number system $\mathbb{C}$, or some other field.

A $1 \times 1$ matrix $[a]$ is usually identified with the scalar $a \in \mathbb{F}$ that constitutes its sole entry. For $n \geq 2$, both $n \times 1$ and $1 \times n$ matrices are called **vector matrices** (or simply **vectors**). In particular an $n \times 1$ matrix

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \tag{2.2}$$

is a **column vector** (or **column matrix**), and a $1 \times n$ matrix

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \end{bmatrix}$$

is a **row vector** (or **row matrix**). Henceforth the Euclidean vector $[x_1, \ldots, x_n]$ introduced in Chapter 1 will most of the time be represented by its corresponding column vector (2.2) so as to take advantage of the convenient properties of matrix arithmetic.

The matrix (2.1) we typically denote more compactly by the symbol

$$[a_{ij}]_{m,n},$$

which indicates that the $ij$-entry is the scalar $a_{ij}$, where $i \in \{1, \ldots, m\}$ is the row number and $j \in \{1, \ldots, n\}$ is the column number. We call the sets $\{1, \ldots, m\}$ and $\{1, \ldots, n\}$ the **range** of the indexes $i$ and $j$, respectively. If $m = n$ then a **square matrix** results, and we define

$$[a_{ij}]_n = [a_{ij}]_{n,n}.$$

(Care should be taken with this notation: $[a_{ij}]_{m,n}$ denotes an $m \times n$ matrix, while $[a_{ij}]_{mn}$ denotes an $mn \times mn$ square matrix!) If the range of the indexes $i$ and $j$ are known or irrelevant, we will write (2.1) as simply $[a_{ij}]$. Another word about square matrices: The **diagonal entries** of a square matrix $[a_{ij}]_n$ are the entries with matching row and column number: $a_{11}, \ldots, a_{nn}$.

Very often we have no need to make any reference to the entries of a matrix, in which case we will usually designate the matrix by a bold-faced upper-case letter such as $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, and so on. The exception is vector matrices, which are normally labeled with bold-faced lower-case letters such as $\mathbf{a}$, $\mathbf{b}$, $\mathbf{x}$, $\mathbf{y}$ and so on. If we need to make reference to the $ij$-entry of a matrix $\mathbf{A}$, then the symbol $[\mathbf{A}]_{ij}$ stands ready to denote it. Thus if $\mathbf{A} = [a_{ij}]_{m,n}$, then

$$[\mathbf{A}]_{ij} = a_{ij}.$$

The set of all $m \times n$ matrices with entries in the field $\mathbb{F}$ will be denoted by $\mathbb{F}^{m\times n}$. That is,

$$\mathbb{F}^{m\times n} = \big\{[a_{ij}]_{m,n} : a_{ij} \in \mathbb{F} \text{ for all } 1 \le i \le m,\ 1 \le j \le n\big\}.$$

From this point onward we also define

$$\mathbb{F}^n = \mathbb{F}^{n\times 1}$$

in these notes; that is, $\mathbb{F}^n$ is the set of matrices consisting of $n$ entries from $\mathbb{F}$ arranged in a single column. The exception has already been encountered: throughout the first chapter (and *only* the first chapter) we always took $\mathbb{R}^n$ to signify $\mathbb{R}^{1\times n}$. In the wider world of mathematics beyond these notes the symbol $\mathbb{F}^n$ denotes either row vectors (elements of $\mathbb{F}^{1\times n}$) or column vectors (elements of $\mathbb{F}^{n\times 1}$), depending on an author's whim.

If $a_{ij} = 0$ for all $1 \le i \le m$ and $1 \le j \le n$, then we obtain the $m \times n$ **zero matrix**

$$\mathbf{O}_{m,n} = [0]_{m,n} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

having $m$ rows and $n$ columns of zeros. In particular we define

$$\mathbf{O}_n = \mathbf{O}_{n,n}.$$

In any case the symbol $\mathbf{O}$ will always denote a zero matrix of some kind, whereas $\mathbf{0}$ will continue to denote more specifically a zero vector (i.e. a row or column matrix consisting of zeros).

**Definition 2.1.** *If* $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{m\times n}$ *and* $c \in \mathbb{F}$, *then we define* ***sum*** $\mathbf{A} + \mathbf{B}$ *and* ***scalar multiple*** $c\mathbf{A}$ *to be the matrices in* $\mathbb{F}^{m\times n}$ *with* $ij$*-entry*

$$[\mathbf{A} + \mathbf{B}]_{ij} = [\mathbf{A}]_{ij} + [\mathbf{B}]_{ij} \quad \text{and} \quad [c\mathbf{A}]_{ij} = c[\mathbf{A}]_{ij}$$

*for all* $1 \le i \le m$ *and* $1 \le j \le n$.

Put another way, letting $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$, we have

$$\mathbf{A} + \mathbf{B} = [a_{ij} + b_{ij}] = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{bmatrix}$$

and

$$c\mathbf{A} = [ca_{ij}] = \begin{bmatrix} ca_{11} & ca_{12} & \cdots & ca_{1n} \\ ca_{21} & ca_{22} & \cdots & ca_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ ca_{m1} & ca_{m2} & \cdots & ca_{mn} \end{bmatrix}.$$

Thus matrix addition and matrix scalar multiplications is analogous to the addition and scalar multiplication of Euclidean vectors. Clearly matrix addition is commutative, which is to say

$$\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$$

for any $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{m\times n}$. We define the **additive inverse** of $\mathbf{A}$ to be the matrix $-\mathbf{A}$ given by

$$-\mathbf{A} = (-1)\mathbf{A} = [-a_{ij}].$$

That

$$\mathbf{A} + (-\mathbf{A}) = -\mathbf{A} + \mathbf{A} = \mathbf{O}$$

is straightforward to check.

**Definition 2.2.** *Let $\mathbf{A} \in \mathbb{F}^{m\times n}$. The* ***transpose*** *of $\mathbf{A}$ is the matrix $\mathbf{A}^\top \in \mathbb{F}^{n\times m}$ such that*

$$[\mathbf{A}^\top]_{ij} = [\mathbf{A}]_{ji}$$

*for all $1 \le i \le n$ and $1 \le j \le m$.*

Put another way, if $\mathbf{A} = [a_{ij}]_{m,n}$, then the transpose of $\mathbf{A}$ is the matrix $\mathbf{A}^\top = [\alpha_{ji}]_{n,m}$ with $\alpha_{ji} = a_{ij}$ for each $1 \le j \le n$, $1 \le i \le m$. Thus the number $a_{ij}$ in the $i$th row and $j$th column of $\mathbf{A}$ is in the $j$th row and $i$th column of $\mathbf{A}^\top$, so that

$$\mathbf{A}^\top = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}. \tag{2.3}$$

Comparing (2.3) with (2.1), it can be seen that the rows of $\mathbf{A}$ simply become the columns of $\mathbf{A}^\top$. For example if

$$\mathbf{A} = \begin{bmatrix} -3 & 7 & 4 \\ 6 & -5 & 10 \end{bmatrix},$$

then

$$\mathbf{A}^\top = \begin{bmatrix} -3 & 6 \\ 7 & -5 \\ 4 & 10 \end{bmatrix}.$$

It is easy to see that $(\mathbf{A}^\top)^\top = \mathbf{A}$. We say $\mathbf{A}$ is **symmetric** if $\mathbf{A}^\top = \mathbf{A}$, and **skew-symmetric** if $\mathbf{A}^\top = -\mathbf{A}$. The set of all symmetric $n \times n$ matrices with entries in the field $\mathbb{F}$ will be denoted by $\mathrm{Sym}_n(\mathbb{F})$; that is,

$$\mathrm{Sym}_n(\mathbb{F}) = \left\{\mathbf{A} \in \mathbb{F}^{n\times n} : \mathbf{A}^\top = \mathbf{A}\right\}.$$

The symbol $\mathrm{Skw}_n(\mathbb{F})$ will denote the set of all skew-symmetric $n \times n$ matrices with entries in $\mathbb{F}$:

$$\mathrm{Skw}_n(\mathbb{F}) = \left\{\mathbf{A} \in \mathbb{F}^{n\times n} : \mathbf{A}^\top = -\mathbf{A}\right\}.$$

A standard approach to proving that two matrices $\mathbf{A}$ and $\mathbf{B}$ are equal is to first confirm that they have the same dimensions, and then show that the $ij$-entry of the matrices are equal for any $i$ and $j$. Thus we verify that $\mathbf{A}$ and $\mathbf{B}$ are $m \times n$ matrices (a step that may be omitted if it is clear), then verify that $[\mathbf{A}]_{ij} = [\mathbf{B}]_{ij}$ for arbitrary $1 \le i \le m$ and $1 \le j \le n$. The proof of the following proposition illustrates the method.

**Proposition 2.3.** *Let* $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{m\times n}$*, and let* $c \in \mathbb{F}$*. Then*
1. $(c\mathbf{A})^\top = c\mathbf{A}^\top$
2. $(\mathbf{A}+\mathbf{B})^\top = \mathbf{A}^\top + \mathbf{B}^\top$
3. $(\mathbf{A}^\top)^\top = \mathbf{A}$.

**Proof.**
*Proof of Part (1).* Fix $1 \le i \le m$ and $1 \le j \le n$. Then, applying Definitions 2.1 and 2.2,

$$[(c\mathbf{A})^\top]_{ij} = [c\mathbf{A}]_{ji} = c[\mathbf{A}]_{ji} = c[\mathbf{A}^\top]_{ij} = [c\mathbf{A}^\top]_{ij}.$$

So we see that the $ij$-entry of $(c\mathbf{A})^\top$ equals the $ij$-entry of $c\mathbf{A}^\top$, and since $i$ and $j$ were arbitrary, it follows that $(c\mathbf{A})^\top = c\mathbf{A}^\top$.

*Proof of Part (2).* We have

$$[(\mathbf{A}+\mathbf{B})^\top]_{ij} = [\mathbf{A}+\mathbf{B}]_{ji} = [\mathbf{A}]_{ji} + [\mathbf{B}]_{ji} = [\mathbf{A}^\top]_{ij} + [\mathbf{B}^\top]_{ij} = [\mathbf{A}^\top + \mathbf{B}^\top]_{ij},$$

so the $ij$-entries of $(\mathbf{A}+\mathbf{B})^\top$ and $\mathbf{A}^\top + \mathbf{B}^\top$ are equal. ■

The proof of part (3) of Proposition 2.3, which can be done using the same "entrywise" technique, is left as a problem.

The **trace** of a square matrix $\mathbf{A} = [a_{ij}]_{n,n}$, written $\mathrm{tr}(\mathbf{A})$, is the sum of the diagonal entries of $\mathbf{A}$:

$$\mathrm{tr}(\mathbf{A}) = \sum_{i=1}^{n} a_{ii}. \tag{2.4}$$

Since $\mathbf{A}^\top = [\alpha_{ij}]_{n,n}$ such that $\alpha_{ij} = a_{ji}$, we readily obtain

$$\mathrm{tr}(\mathbf{A}^\top) = \sum_{i=1}^{n} \alpha_{ii} = \sum_{i=1}^{n} a_{ii} = \mathrm{tr}(\mathbf{A}).$$

Other properties of the trace and transpose operations will be established in future sections.

A **block matrix** is a matrix whose entries are themselves matrices. The matrices that constitute a block matrix are called **submatrices**. In practice a block matrix is typically constructed from an ordinary matrix $\mathbf{A} \in \mathbb{F}^{m\times n}$ by partitioning the entries into two or more smaller arrays with the placement of vertical or horizontal rules, such as

$$\left[\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1s} & a_{1,s+1} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{r1} & \cdots & a_{rs} & a_{r,s+1} & \cdots & a_{rn} \\ \hline a_{r+1,1} & \cdots & a_{r+1,s} & a_{r+1,s+1} & \cdots & a_{r+1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{ms} & a_{m,s+1} & \cdots & a_{mn} \end{array}\right], \tag{2.5}$$

which partitions the matrix $\mathbf{A} = [a_{ij}]_{m,n}$ into four submatrices

$$\begin{bmatrix} a_{11} & \cdots & a_{1s} \\ \vdots & \ddots & \vdots \\ a_{r1} & \cdots & a_{rs} \end{bmatrix}, \quad \begin{bmatrix} a_{1,s+1} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{r,s+1} & \cdots & a_{rn} \end{bmatrix}, \quad \begin{bmatrix} a_{r+1,1} & \cdots & a_{r+1,s} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{ms} \end{bmatrix}, \quad \begin{bmatrix} a_{r+1,s+1} & \cdots & a_{r+1,n} \\ \vdots & \ddots & \vdots \\ a_{m,s+1} & \cdots & a_{mn} \end{bmatrix},$$

where of course $1 \leq r < m$ and $1 \leq s < n$. If we designate the above submatrices as $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, and $\mathbf{A}_4$, respectively, then we may write (2.5) as the block matrix

$$\left[\begin{array}{c|c} \mathbf{A}_1 & \mathbf{A}_2 \\ \hline \mathbf{A}_3 & \mathbf{A}_4 \end{array}\right] \quad \text{or} \quad \begin{bmatrix} \mathbf{A}_1 & \mathbf{A}_2 \\ \mathbf{A}_3 & \mathbf{A}_4 \end{bmatrix},$$

with the latter representation being preferred in these notes except in certain situations. A block matrix is also known as a **partitioned matrix**.

## Problems

1. Prove that $(\mathbf{A}^\top)^\top = \mathbf{A}$ for any $\mathbf{A} \in \mathbb{F}^{m\times n}$.

2. Prove that $(\mathbf{A} + \mathbf{B} + \mathbf{C})^\top = \mathbf{A}^\top + \mathbf{B}^\top + \mathbf{C}^\top$ for any $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbb{F}^{m\times n}$.

3. Prove that $(a\mathbf{A} + b\mathbf{B})^\top = a\mathbf{A}^\top + b\mathbf{B}^\top$ for any $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{m\times n}$ and $a, b \in \mathbb{F}$.

## 2.2 – Matrix Multiplication

The definition of the product of two matrices is relatively more involved than that for addition or scalar multiplication.

**Definition 2.4.** *Let* $\mathbf{A} \in \mathbb{F}^{m\times n}$ *and* $\mathbf{B} \in \mathbb{F}^{n\times p}$. *Then the* ***product*** *of* $\mathbf{A}$ *and* $\mathbf{B}$ *is the matrix* $\mathbf{AB} \in \mathbb{F}^{m\times p}$ *with* $ij$*-entry given by*

$$[\mathbf{AB}]_{ij} = \sum_{k=1}^{n} [\mathbf{A}]_{ik}[\mathbf{B}]_{kj}$$

*for* $1 \le i \le m$ *and* $1 \le j \le p$.

Letting $\mathbf{A} = [a_{ij}]_{m,n}$ and $\mathbf{B} = [b_{ij}]_{n,p}$, it is immediate that $\mathbf{AB} = [c_{ij}]_{m,p}$ with $ij$-entry

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

That is,

$$\mathbf{AB} = [a_{ij}]_{m,n}[b_{ij}]_{n,p} = \left[\textstyle\sum_{k=1}^{n} a_{ik}b_{kj}\right]_{m,p}, \tag{2.6}$$

where it's understood that $1 \le i \le m$ is the row number and $1 \le j \le p$ is the column number of the entry $\sum_{k=1}^{n} a_{ik}b_{kj}$.

**Example 2.5.** If

$$\mathbf{A} = \begin{bmatrix} -3 & 0 & 6 \\ 2 & 11 & -5 \end{bmatrix} \quad \text{and} \quad \mathbf{B} = \begin{bmatrix} 4 & 9 & -6 \\ 0 & -1 & 2 \\ -4 & 0 & -3 \end{bmatrix},$$

so that $\mathbf{A}$ is a $2 \times 3$ matrix and $\mathbf{B}$ is a $3 \times 3$ matrix, then $\mathbf{AB}$ is a $2 \times 3$ matrix given by

$$\begin{aligned}
\mathbf{AB} &= \begin{bmatrix} -3 & 0 & 6 \\ 2 & 11 & -5 \end{bmatrix} \begin{bmatrix} 4 & 9 & -6 \\ 0 & -1 & 2 \\ -4 & 0 & -3 \end{bmatrix} \\
&= \begin{bmatrix} \begin{bmatrix} -3 & 0 & 6 \end{bmatrix}\begin{bmatrix} 4 \\ 0 \\ -4 \end{bmatrix} & \begin{bmatrix} -3 & 0 & 6 \end{bmatrix}\begin{bmatrix} 9 \\ -1 \\ 0 \end{bmatrix} & \begin{bmatrix} -3 & 0 & 6 \end{bmatrix}\begin{bmatrix} -6 \\ 2 \\ -3 \end{bmatrix} \\ \begin{bmatrix} 2 & 11 & -5 \end{bmatrix}\begin{bmatrix} 4 \\ 0 \\ -4 \end{bmatrix} & \begin{bmatrix} 2 & 11 & -5 \end{bmatrix}\begin{bmatrix} 9 \\ -1 \\ 0 \end{bmatrix} & \begin{bmatrix} 2 & 11 & -5 \end{bmatrix}\begin{bmatrix} -6 \\ 2 \\ -3 \end{bmatrix} \end{bmatrix} \\
&= \begin{bmatrix} -36 & -27 & 0 \\ 28 & 7 & 25 \end{bmatrix}.
\end{aligned}$$

The product $\mathbf{BA}$ is undefined. ■

Vectors may be used to better see how the product **AB** is formed. Let

$$\mathbf{a}_i = \begin{bmatrix} a_{i1} & \cdots & a_{in} \end{bmatrix}$$

denote the **row vectors** of **A** for $1 \le i \le m$,

$$\begin{matrix} \mathbf{a}_1 \rightarrow \\ \mathbf{a}_2 \rightarrow \\ \vdots \\ \mathbf{a}_m \rightarrow \end{matrix} \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = \mathbf{A} \tag{2.7}$$

and let

$$\mathbf{b}_j = \begin{bmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{bmatrix}$$

denote the **column vectors** of **B** for $1 \le j \le p$,

$$\mathbf{B} = \begin{matrix} \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_p \\ \downarrow & \downarrow & & \downarrow \\ \end{matrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1p} \\ b_{21} & b_{22} & \cdots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{np} \end{bmatrix}. \tag{2.8}$$

Then by definition

$$\mathbf{AB} = [\mathbf{a}_i\mathbf{b}_j]_{m,p} = \begin{bmatrix} \mathbf{a}_1\mathbf{b}_1 & \mathbf{a}_1\mathbf{b}_2 & \cdots & \mathbf{a}_1\mathbf{b}_p \\ \mathbf{a}_2\mathbf{b}_1 & \mathbf{a}_2\mathbf{b}_2 & \cdots & \mathbf{a}_2\mathbf{b}_p \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_m\mathbf{b}_1 & \mathbf{a}_m\mathbf{b}_2 & \cdots & \mathbf{a}_m\mathbf{b}_p \end{bmatrix},$$

which makes clear that the $ij$-entry is

$$[\mathbf{AB}]_{ij} = \mathbf{a}_i\mathbf{b}_j = \begin{bmatrix} a_{i1} & \cdots & a_{in} \end{bmatrix} \begin{bmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{bmatrix} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj},$$

in agreement with Definition 2.4. Note that **AB** is not defined if the number of columns in **A** is not equal to the number of rows in **B**!

It is common—and convenient—to denote matrices (2.7) and (2.8) by the symbols

$$\begin{bmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_m \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_p \end{bmatrix},$$

respectively, and so we have

$$\mathbf{AB} = \begin{bmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_m \end{bmatrix} \begin{bmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_p \end{bmatrix} = \begin{bmatrix} \mathbf{a}_1\mathbf{b}_1 & \mathbf{a}_1\mathbf{b}_2 & \cdots & \mathbf{a}_1\mathbf{b}_p \\ \mathbf{a}_2\mathbf{b}_1 & \mathbf{a}_2\mathbf{b}_2 & \cdots & \mathbf{a}_2\mathbf{b}_p \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_m\mathbf{b}_1 & \mathbf{a}_m\mathbf{b}_2 & \cdots & \mathbf{a}_m\mathbf{b}_p \end{bmatrix}. \tag{2.9}$$

For any $j = 1, \dots, p$ we have $\mathbf{b}_j \in \mathbb{F}^n$, which is to say $\mathbf{b}_j$ has $n$ rows and so $\mathbf{A}\mathbf{b}_j$ can be computed following the pattern of (2.9):

$$\mathbf{A}\mathbf{b}_j = \begin{bmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_m \end{bmatrix} \mathbf{b}_j = \begin{bmatrix} \mathbf{a}_1\mathbf{b}_j \\ \mathbf{a}_2\mathbf{b}_j \\ \vdots \\ \mathbf{a}_m\mathbf{b}_j \end{bmatrix}.$$

(This can be verified easily by working directly with Definition 2.4.) Comparing this result with the right-hand side of (2.9), we see that $\mathbf{A}\mathbf{b}_j$ is the $j$th column vector of $\mathbf{AB}$; that is, we have the following.

**Proposition 2.6.** *If* $\mathbf{A} \in \mathbb{F}^{m\times n}$ *and* $\mathbf{B} = \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_p \end{bmatrix} \in \mathbb{F}^{n\times p}$, *then*

$$\mathbf{AB} = \mathbf{A}\begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_p \end{bmatrix} = \begin{bmatrix} \mathbf{A}\mathbf{b}_1 & \cdots & \mathbf{A}\mathbf{b}_p \end{bmatrix}.$$

We see how a judicious use of notation can reap significant labor-saving rewards, leading from the unfamiliar characterization of $\mathbf{AB}$ given in Definition 2.4 to the perfectly natural formula in Proposition 2.6.

**Theorem 2.7.** *Let* $\mathbf{A} \in \mathbb{F}^{m\times n}$, $\mathbf{B}, \mathbf{C} \in \mathbb{F}^{n\times p}$, $\mathbf{D} \in \mathbb{F}^{p\times q}$, *and* $c \in \mathbb{F}$. *Then*

1. $\mathbf{A}(c\mathbf{B}) = c(\mathbf{AB})$.
2. $\mathbf{A}(\mathbf{B}+\mathbf{C}) = \mathbf{AB} + \mathbf{AC}$ *(the* ***distributive property****).*
3. $(\mathbf{AB})\mathbf{D} = \mathbf{A}(\mathbf{BD})$ *(the* ***associative property****).*

**Proof.**

*Proof of Part (1).* Clearly $\mathbf{A}(c\mathbf{B})$ and $c(\mathbf{AB})$ are both $m \times p$ matrices. Now, for any $1 \le i \le m$ and $1 \le j \le p$,

$$\begin{aligned} [\mathbf{A}(c\mathbf{B})]_{ij} &= \sum_{k=1}^{n} [\mathbf{A}]_{ik}[c\mathbf{B}]_{kj} && \text{Definition 2.4} \\ &= \sum_{k=1}^{n} [\mathbf{A}]_{ik}\big(c[\mathbf{B}]_{kj}\big) && \text{Definition 2.1} \\ &= c\sum_{k=1}^{n} [\mathbf{A}]_{ik}[\mathbf{B}]_{kj} && \text{Definition 1.5(F5,6,7)} \\ &= c[\mathbf{AB}]_{ij} && \text{Definition 2.4,} \\ &= [c(\mathbf{AB})]_{ij} && \text{Definition 2.1,} \end{aligned}$$

and so we see the $ij$-entries of $\mathbf{A}(c\mathbf{B})$ and $c(\mathbf{AB})$ are equal.

*Proof of Part (2).* Clearly $\mathbf{A}(\mathbf{B}+\mathbf{C})$ and $\mathbf{AB}+\mathbf{AC}$ are both $m \times p$ matrices. For $1 \le i \le m$ and $1 \le j \le p$,

$$[\mathbf{A}(\mathbf{B}+\mathbf{C})]_{ij} = \sum_{k=1}^{n} [\mathbf{A}]_{ik}[\mathbf{B}+\mathbf{C}]_{kj} \qquad \text{Definition 2.4}$$

$$
\begin{aligned}
&= \sum_{k=1}^{n} [\mathbf{A}]_{ik}\big([\mathbf{B}]_{kj} + [\mathbf{C}]_{kj}\big) && \text{Definition 2.1} \\
&= \sum_{k=1}^{n} [\mathbf{A}]_{ik}[\mathbf{B}]_{kj} + \sum_{k=1}^{n} [\mathbf{A}]_{ik}[\mathbf{C}]_{kj} && \text{Definition 1.5(F6)} \\
&= \mathbf{AB} + \mathbf{AC}. && \text{Definition 2.4,}
\end{aligned}
$$

which shows equality of the $ij$ entries.

*Proof of Part (3).* Both matrices will be $m \times q$. Using basic summation properties and Definition 2.4,

$$
\begin{aligned}
[(\mathbf{AB})\mathbf{D}]_{ij} &= \sum_{k=1}^{p} [\mathbf{AB}]_{ik}[\mathbf{D}]_{kj} = \sum_{k=1}^{p} \left[ \left( \sum_{\ell=1}^{n} [\mathbf{A}]_{i\ell}[\mathbf{B}]_{\ell k} \right) [\mathbf{D}]_{kj} \right] = \sum_{\ell=1}^{n} \sum_{k=1}^{p} [\mathbf{A}]_{i\ell}[\mathbf{B}]_{\ell k}[\mathbf{D}]_{kj} \\
&= \sum_{\ell=1}^{n} \left( [\mathbf{A}]_{i\ell} \sum_{k=1}^{p} [\mathbf{B}]_{\ell k}[\mathbf{D}]_{kj} \right) = \sum_{\ell=1}^{n} [\mathbf{A}]_{i\ell}[\mathbf{BD}]_{\ell j} = [\mathbf{A}(\mathbf{BD})]_{ij},
\end{aligned}
$$

and the proof is done. ∎

In light of the associative property of matrix multiplication it is not considered ambiguous to write $\mathbf{ABD}$, since whether we interpret it as meaning $(\mathbf{AB})\mathbf{D}$ or $\mathbf{A}(\mathbf{BD})$ makes no difference. The order of operations conventions dictate that $\mathbf{ABD}$ be computed in the order indicated by $(\mathbf{AB})\mathbf{D}$, however.

**Proposition 2.8.** *If* $\mathbf{A} \in \mathbb{F}^{m\times n}$, $\mathbf{B} \in \mathbb{F}^{n\times p}$, $\mathbf{C} \in \mathbb{F}^{p\times q}$, *and* $\mathbf{D} \in \mathbb{F}^{q\times r}$, *then*

$$(\mathbf{AB})(\mathbf{CD}) = \mathbf{A}(\mathbf{BC})\mathbf{D}.$$

**Proof.** Let $\mathbf{AB} = \mathbf{P}$. We have

$$(\mathbf{AB})(\mathbf{CD}) = \mathbf{P}(\mathbf{CD}) = (\mathbf{PC})\mathbf{D} = [(\mathbf{AB})\mathbf{C}]\mathbf{D} = [\mathbf{A}(\mathbf{BC})]\mathbf{D}, \tag{2.10}$$

where the second and fourth equalities follow from Theorem 2.7(3). Next we obtain

$$[\mathbf{A}(\mathbf{BC})]\mathbf{D} = \mathbf{A}(\mathbf{BC})\mathbf{D}, \tag{2.11}$$

since the order of operations in evaluating either expression is precisely the same: (1) execute $\mathbf{B}$ times $\mathbf{C}$ to obtain $\mathbf{BC}$; (2) execute $\mathbf{A}$ times $\mathbf{BC}$ to obtain $\mathbf{A}(\mathbf{BC})$; (3) execute $\mathbf{A}(\mathbf{BC})$ times $\mathbf{D}$ to obtain $\mathbf{A}(\mathbf{BC})\mathbf{D}$.

Combining (2.10) and (2.11) yields $(\mathbf{AB})(\mathbf{CD}) = \mathbf{A}(\mathbf{BC})\mathbf{D}$. ∎

There is no useful way to divide matrices, but we can easily define what it means to exponentiate a matrix by a positive integer.

**Definition 2.9.** *If* $\mathbf{A} \in \mathbb{F}^{n\times n}$ *and* $m \in \mathbb{N}$*, then*

$$\mathbf{A}^m = \underbrace{\mathbf{A}\mathbf{A}\cdots\mathbf{A}}_{m \text{ factors}} = \prod_{k=1}^{m} \mathbf{A}.$$

*In particular* $\mathbf{A}^1 = \mathbf{A}$.

The definition makes use of so-called product notation,

$$\prod_{k=1}^{m} x_k = x_1 x_2 x_3 \cdots x_m,$$

which does for products what summation notation does for sums.

The **Kronecker delta** is a function $\delta_{ij} : \mathbb{Z} \times \mathbb{Z} \to \{0, 1\}$ defined as follows for integers $i$ and $j$:

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

We use the Kronecker delta to define the $n \times n$ **identity matrix**,

$$\mathbf{I}_n = [\delta_{ij}]_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

the $n \times n$ matrix with diagonal entries 1 and all other entries 0. In particular we have

$$\mathbf{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{I}_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

**Definition 2.10.** *For any* $\mathbf{A} \in \mathbb{F}^{n\times n}$ *we define* $\mathbf{A}^0 = \mathbf{I}_n$.

If the dimensions of an identity matrix are known or irrelevant, then the abbreviated symbol $\mathbf{I}$ may be used. The reason $\mathbf{I}_n$ is called the identity matrix is because, for any $n \times n$ matrix $\mathbf{A}$, it happens that

$$\mathbf{I}_n\mathbf{A} = \mathbf{A}\mathbf{I}_n = \mathbf{A}.$$

Thus $\mathbf{I}_n$ acts as an identity with respect to matrix multiplication, just as 1 is the identity with respect to multiplication of real numbers. In fact it can be shown that $\mathbf{I}_n$ is *the* identity for matrix multiplication, as there can be no others.

**Example 2.11.** Show that $\mathbf{I}_2$ is the only matrix for which $\mathbf{I}_2\mathbf{A} = \mathbf{A}\mathbf{I}_2 = \mathbf{A}$ holds for all $2 \times 2$ matrices $\mathbf{A}$.

**Solution.** Given any $2 \times 2$ matrix

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

we have

$$\mathbf{AI}_2 = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_{11}(1) + a_{12}(0) & a_{11}(0) + a_{12}(1) \\ a_{21}(1) + a_{22}(0) & a_{21}(0) + a_{22}(1) \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \mathbf{A}$$

and

$$\mathbf{I}_2\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} (1)a_{11} + (0)a_{12} & (0)a_{11} + (1)a_{12} \\ (1)a_{21} + (0)a_{22} & (0)a_{21} + (1)a_{22} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \mathbf{A},$$

so certainly $\mathbf{I}_2\mathbf{A} = \mathbf{AI}_2 = \mathbf{A}$ holds for all $\mathbf{A}$.

Now, let $\mathbf{B}$ be a $2 \times 2$ matrix such that

$$\mathbf{BA} = \mathbf{AB} = \mathbf{A} \tag{2.12}$$

for all $2 \times 2$ matrices $\mathbf{A}$. If we set $\mathbf{A} = \mathbf{I}_2$ in (2.12) we obtain $\mathbf{BI}_2 = \mathbf{I}_2$ in particular, whence $\mathbf{B} = \mathbf{I}_2$. Therefore $\mathbf{I}_2$ is the *only* matrix for which $\mathbf{I}_2\mathbf{A} = \mathbf{AI}_2 = \mathbf{A}$ holds for all $\mathbf{A}$. ■

To show more generally that $\mathbf{I}_n$ is the only matrix for which

$$\mathbf{I}_n\mathbf{A} = \mathbf{AI}_n = \mathbf{A}$$

for all $\mathbf{A} \in \mathbb{F}^{n\times n}$ involves a nearly identical argument.

**Proposition 2.12.** *Let* $\mathbf{A} \in \mathbb{F}^{n\times n}$*.*

1. *If* $\mathbf{Ax} = \mathbf{x}$ *for every* $n \times 1$ *column vector* $\mathbf{x}$*, then* $\mathbf{A} = \mathbf{I}_n$*.*
2. *If* $\mathbf{Ax} = \mathbf{0}$ *for every* $n \times 1$ *column vector* $\mathbf{x}$*, then* $\mathbf{A} = \mathbf{O}_n$*.*

**Proof.**
*Proof of Part (1).* Suppose that $\mathbf{Ax} = \mathbf{x}$ for all $n \times 1$ column vectors $\mathbf{x}$. For each $1 \le j \le n$ let

$$\mathbf{e}_j = [\delta_{ij}]_{n,1} = \begin{bmatrix} \delta_{1j} \\ \vdots \\ \delta_{nj} \end{bmatrix},$$

where once again we make use of the Kronecker delta. Thus $\mathbf{e}_j$ is the $n \times 1$ column vector with 1 in the $j$th row and 0 in all other rows.

Now, for each $1 \le j \le n$, $\mathbf{Ae}_j$ is an $n \times 1$ column vector with $i1$-entry equalling

$$\sum_{k=1}^{n} a_{ik}\delta_{kj} = a_{ij}\delta_{jj} = a_{ij}.$$

for each $1 \le i \le n$. On the other hand $\mathbf{Ae}_j = \mathbf{e}_j$ by hypothesis, and so

$$a_{ij} = \delta_{ij} = \begin{cases} 0, & \text{if } i \ne j \\ 1, & \text{if } i = j \end{cases}$$

for all $1 \le i, j \le n$. But this is precisely the definition for $\mathbf{I}_n$, and therefore $\mathbf{A} = \mathbf{I}_n$. ■

The proof of part (2) of the proposition is similar and left as a problem. Observe that, in the notation established in the proof of part (1), we have

$$\mathbf{I}_n = \begin{bmatrix} [\delta_{i1}]_{n,1} & \cdots & [\delta_{in}]_{n,1} \end{bmatrix} = \begin{bmatrix} \mathbf{e}_1 & \cdots & \mathbf{e}_n \end{bmatrix}. \tag{2.13}$$

**Proposition 2.13.** *Let* $\mathbf{A} \in \mathbb{F}^{m\times n}$ *and* $\mathbf{B} \in \mathbb{F}^{n\times p}$. *Then*

$$(\mathbf{AB})^\top = \mathbf{B}^\top \mathbf{A}^\top.$$

**Proof.** Note that $\mathbf{B}^\top$ is $p \times n$ and $\mathbf{A}^\top$ is $n \times m$, so the product $\mathbf{B}^\top\mathbf{A}^\top$ is defined as a $p \times m$ matrix. Fix $1 \le i \le p$ and $1 \le j \le m$. We have, using Definition 2.4 and Definition 2.2 twice each,

$$[\mathbf{B}^\top\mathbf{A}^\top]_{ij} = \sum_{k=1}^{n} [\mathbf{B}^\top]_{ik}[\mathbf{A}^\top]_{kj} = \sum_{k=1}^{n} [\mathbf{B}]_{ki}[\mathbf{A}]_{jk} = \sum_{k=1}^{n} [\mathbf{A}]_{jk}[\mathbf{B}]_{ki} = [\mathbf{AB}]_{ji} = \left[(\mathbf{AB})^\top\right]_{ij}.$$

Thus the $ij$-entry of $\mathbf{B}^\top\mathbf{A}^\top$ is equal to the $ij$-entry of $(\mathbf{AB})^\top$, so $\mathbf{B}^\top\mathbf{A}^\top = (\mathbf{AB})^\top$ as was to be shown. ∎

## Problems

1. Given that

$$\mathbf{x} = \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix}, \quad \mathbf{A} = \begin{bmatrix} 1 & 2 & -3 \\ 3 & 0 & -1 \\ -2 & 1 & 4 \end{bmatrix}, \quad \mathbf{C} = \begin{bmatrix} -4 & 2 \\ 1 & -1 \\ 0 & 3 \end{bmatrix}$$

compute the following.

(a) $\mathbf{x}^\top\mathbf{x}$

(b) $\mathbf{x}\mathbf{x}^\top$

(c) $\mathbf{AC}$

## 2.3 – Row and Column Operations

We start by establishing some necessary notation. The symbol $\mathbf{E}_{n,lm}$ will denote the $n \times n$ matrix with $lm$-entry 1 and all other entries 0; that is,

$$\mathbf{E}_{n,lm} = [\delta_{il}\delta_{mj}]_n$$

for any fixed $1 \leq l, m \leq n$, making use of the Kronecker delta introduced in the last section. Put yet another way, $\mathbf{E}_{n,lm}$ is the $n \times n$ matrix with $ij$-entry $\delta_{il}\delta_{mj}$:

$$[\mathbf{E}_{n,lm}]_{ij} = \delta_{il}\delta_{mj}. \tag{2.14}$$

Usually the $n$ in the symbol $\mathbf{E}_{n,lm}$ may be suppressed without leading to ambiguity, so that the more compact symbol $\mathbf{E}_{lm}$ may be used. This will usually be done except in the statement of theorems.

**Proposition 2.14.** *Let $n \in \mathbb{N}$ and $1 \leq l, m, p, q \leq n$.*

1. $\mathbf{E}_{n,lm}\mathbf{E}_{n,mp} = \mathbf{E}_{n,lp}$.
2. *If $m \neq p$, then* $\mathbf{E}_{n,lm}\mathbf{E}_{n,pq} = \mathbf{O}_n$.

**Proof.**
*Proof of Part (1).* Using Definition 2.4 and equation (2.14), the $ij$-entry of $\mathbf{E}_{lm}\mathbf{E}_{mp}$ is

$$[\mathbf{E}_{lm}\mathbf{E}_{mp}]_{ij} = \sum_{k=1}^{n} [\mathbf{E}_{lm}]_{ik}[\mathbf{E}_{mp}]_{kj} = \sum_{k=1}^{n} (\delta_{il}\delta_{mk})(\delta_{km}\delta_{pj}) = (\delta_{il}\delta_{mm})(\delta_{mm}\delta_{pj}) = \delta_{il}\delta_{pj},$$

where the third equality is justified since $\delta_{mk} = 0$ for all $k \neq m$, and then we need only recall that $\delta_{mm} = 1$. So $\mathbf{E}_{lm}\mathbf{E}_{mp}$ is the $n \times n$ matrix with $ij$-entry $\delta_{il}\delta_{pj}$, and therefore $\mathbf{E}_{lm}\mathbf{E}_{mp} = \mathbf{E}_{lp}$.

*Proof of Part (2).* Suppose $m \neq p$. Again using Definition 2.4 and equation (2.14), the $ij$-entry of $\mathbf{E}_{lm}\mathbf{E}_{mp}$ is

$$[\mathbf{E}_{lm}\mathbf{E}_{pq}]_{ij} = \sum_{k=1}^{n} [\mathbf{E}_{lm}]_{ik}[\mathbf{E}_{pq}]_{kj} = \sum_{k=1}^{n} (\delta_{il}\delta_{mk})(\delta_{kp}\delta_{qj}) = 0,$$

where the third equality is justified since, for any $1 \leq k \leq n$, either $k \neq m$ or $k \neq p$, and so either $\delta_{mk} = 0$ or $\delta_{kp} = 0$. Therefore $\mathbf{E}_{lm}\mathbf{E}_{pq} = \mathbf{O}_n$. ■

Let $n \in \mathbb{N}$. For any scalar $c \neq 0$ define

$$\mathbf{M}_i(c) = \mathbf{I}_n + (c-1)\mathbf{E}_{ii},$$

which is the $n \times n$ matrix obtained by multiplying the $i$th row of $\mathbf{I}_n$ by $c$. Also define

$$\mathbf{M}_{i,j} = \mathbf{I}_n - \mathbf{E}_{ii} - \mathbf{E}_{jj} + \mathbf{E}_{ij} + \mathbf{E}_{ji}$$

for $i, j \in \{1, \ldots, n\}$ with $i \neq j$, which is the matrix obtained by interchanging the $i$th and $j$th rows of $\mathbf{I}_n$ (notice that $\mathbf{M}_{i,j} = \mathbf{M}_{j,i}$). Finally, for $i, j \in \{1, \ldots, n\}$ with $i \neq j$, and scalar $c \neq 0$, define

$$\mathbf{M}_{i,j}(c) = \mathbf{I}_n + c\mathbf{E}_{ji},$$

which is the matrix obtained by adding $c$ times the $i$th row of $\mathbf{I}_n$ to the $j$th row of $\mathbf{I}_n$. Any matrix of the form $\mathbf{M}_{i,j}(c)$, $\mathbf{M}_{i,j}$, or $\mathbf{M}_i(c)$ is called an **elementary matrix**.

**Definition 2.15.** *Given $\mathbf{A} \in \mathbb{F}^{m\times n}$, an **elementary row operation** on $\mathbf{A}$ is any one of the multiplications*

$$\mathbf{M}_{i,j}(c)\mathbf{A}, \quad \mathbf{M}_{i,j}\mathbf{A}, \quad \mathbf{M}_i(c)\mathbf{A}.$$

*More specifically we call left-multiplication by $\mathbf{M}_{i,j}(c)$ an* R1 *operation, left-multiplication by $\mathbf{M}_{i,j}$ an* R2 *operation, and left-multiplication by $\mathbf{M}_i(c)\mathbf{A}$ an* R3 *operation. A matrix $\mathbf{A}'$ is called **row-equivalent** to $\mathbf{A}$ if there exist elementary matrices $\mathbf{M}_1, \dots, \mathbf{M}_k$ such that*

$$\mathbf{A}' = \mathbf{M}_k \cdots \mathbf{M}_1\mathbf{A}.$$

*An **elementary column operation** on $\mathbf{A}$ is any one of the multiplications*

$$\mathbf{A}\mathbf{M}_{i,j}^\top(c), \quad \mathbf{A}\mathbf{M}_{i,j}^\top, \quad \text{or} \quad \mathbf{A}\mathbf{M}_i^\top(c).$$

*More specifically we call right-multiplication by $\mathbf{M}_{i,j}^\top(c)$ a* C1 *operation, right-multiplication by $\mathbf{M}_{i,j}^\top$ a* C2 *operation, and right-multiplication by $\mathbf{M}_i^\top(c)$ a* C3 *operation. A matrix $\mathbf{A}'$ is called **column-equivalent** to $\mathbf{A}$ if there exist elementary matrices $\mathbf{M}_1, \dots, \mathbf{M}_k$ such that*

$$\mathbf{A}' = \mathbf{A}\mathbf{M}_1^\top \cdots \mathbf{M}_k^\top.$$

It's understood that the elementary matrices in the first part of Definition 2.15 must all be $m \times m$ matrices, and the elementary matrices in the second part must be $n \times n$. Also, to be clear, we define $\mathbf{M}_{i,j}^\top(c) = [\mathbf{M}_{i,j}(c)]^\top$ and $\mathbf{M}_i^\top(c) = [\mathbf{M}_i(c)]^\top$. Finally, we define any matrix $\mathbf{A}$ to be both row-equivalent and column-equivalent to itself.

When we need to denote a collection of, say, $p$ elementary matrices in a general way, we will usually use symbols $\mathbf{M}_1, \dots, \mathbf{M}_p$. So for each $k = 1, \dots, p$ the symbol $\mathbf{M}_k$ could represent any one of the three basic types of elementary matrix given in Definition 2.15.

**Proposition 2.16.** *Suppose $\mathbf{A} \in \mathbb{F}^{m\times n}$ has row vectors $\mathbf{a}_1, \dots, \mathbf{a}_m \in \mathbb{F}^n$. Let $c \neq 0$, and let $1 \le p, q \le m$ with $p \neq q$.*

1. *$\mathbf{M}_{p,q}(c)\mathbf{A}$ is the matrix obtained from $\mathbf{A}$ by replacing the row vector $\mathbf{a}_q$ by $\mathbf{a}_q + c\mathbf{a}_p$:*

$$\mathbf{M}_{p,q}(c)\begin{bmatrix} \vdots \\ \mathbf{a}_q \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ \mathbf{a}_q + c\mathbf{a}_p \\ \vdots \end{bmatrix}.$$

2. *$\mathbf{M}_{p,q}\mathbf{A}$ is the matrix obtained from $\mathbf{A}$ by interchanging $\mathbf{a}_p$ and $\mathbf{a}_q$:*

$$\mathbf{M}_{p,q}\begin{bmatrix} \vdots \\ \mathbf{a}_{\min\{p,q\}} \\ \vdots \\ \mathbf{a}_{\max\{p,q\}} \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ \mathbf{a}_{\max\{p,q\}} \\ \vdots \\ \mathbf{a}_{\min\{p,q\}} \\ \vdots \end{bmatrix}.$$

3. $\mathbf{M}_p(c)\mathbf{A}$ *is the matrix obtained from* $\mathbf{A}$ *by replacing* $\mathbf{a}_p$ *by* $c\mathbf{a}_p$*:*

$$\mathbf{M}_p(c)\begin{bmatrix} \vdots \\ \mathbf{a}_p \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ c\mathbf{a}_p \\ \vdots \end{bmatrix}.$$

**Proof.**
*Proof of Part (1).* Fix $1 \leq i \leq m$ and $1 \leq j \leq n$. Here $\mathbf{M}_{p,q}(c)$ must be $m \times m$, so that $\mathbf{M}_{p,q}(c) = \mathbf{I}_m + c\mathbf{E}_{m,qp}$, since $\mathbf{A}$ is $m \times n$. Then

$$\begin{aligned}\big[\mathbf{M}_{p,q}(c)\mathbf{A}\big]_{ij} &= \sum_{k=1}^{m} \big[\mathbf{M}_{p,q}(c)\big]_{ik}[\mathbf{A}]_{kj} = \sum_{k=1}^{m}[\mathbf{I}_m + c\mathbf{E}_{qp}]_{ik}[\mathbf{A}]_{kj} \\ &= \sum_{k=1}^{m}\big([\mathbf{I}_m]_{ik} + c[\mathbf{E}_{qp}]_{ik}\big)[\mathbf{A}]_{kj} = \sum_{k=1}^{m}[\mathbf{I}_m]_{ik}[\mathbf{A}]_{kj} + c\sum_{k=1}^{m}[\mathbf{E}_{qp}]_{ik}[\mathbf{A}]_{kj} \\ &= [\mathbf{I}_m\mathbf{A}]_{ij} + c\sum_{k=1}^{m}\delta_{iq}\delta_{pk}[\mathbf{A}]_{kj} = [\mathbf{A}]_{ij} + c\delta_{iq}[\mathbf{A}]_{pj},\end{aligned}$$

where the last equality holds since $\delta_{pk} = 0$ for all $k \neq p$.

Now, if $i \neq q$, then $\delta_{iq} = 0$ and we obtain

$$\big[\mathbf{M}_{p,q}(c)\mathbf{A}\big]_{ij} = [\mathbf{A}]_{ij}$$

for all $1 \leq j \leq n$, which shows that the $i$th row vector of $\mathbf{M}_{p,q}(c)\mathbf{A}$ equals the $i$th row vector $\mathbf{a}_i$ of $\mathbf{A}$ whenever $i \neq q$. On the other hand if $i = q$, then $\delta_{iq} = \delta_{qq} = 1$ and we obtain

$$\big[\mathbf{M}_{p,q}(c)\mathbf{A}\big]_{qj} = [\mathbf{A}]_{qj} + c[\mathbf{A}]_{pj}$$

for all $1 \leq j \leq n$, which shows that the $q$th row vector of $\mathbf{M}_{p,q}(c)\mathbf{A}$ equals the $q$th row vector of $\mathbf{A}$ plus $c$ times the $p$th row vector: $\mathbf{a}_q + c\mathbf{a}_p$.

*Proof of Part (2).* For $1 \leq i \leq m$ and $1 \leq j \leq n$,

$$\begin{aligned}[\mathbf{M}_{p,q}\mathbf{A}]_{ij} &= \sum_{k=1}^{m}[\mathbf{M}_{p,q}]_{ik}[\mathbf{A}]_{kj} = \sum_{k=1}^{m}[\mathbf{I}_m - \mathbf{E}_{pp} - \mathbf{E}_{qq} + \mathbf{E}_{pq} + \mathbf{E}_{qp}]_{ik}[\mathbf{A}]_{kj} \\ &= \sum_{k=1}^{m}\big([\mathbf{I}_m]_{ik} - [\mathbf{E}_{pp}]_{ik} - [\mathbf{E}_{qq}]_{ik} + [\mathbf{E}_{pq}]_{ik} + [\mathbf{E}_{qp}]_{ik}\big)[\mathbf{A}]_{kj} \\ &= \sum_{k=1}^{m}[\mathbf{I}_m]_{ik}[\mathbf{A}]_{kj} - \sum_{k=1}^{m}[\mathbf{E}_{pp}]_{ik}[\mathbf{A}]_{kj} - \sum_{k=1}^{m}[\mathbf{E}_{qq}]_{ik}[\mathbf{A}]_{kj} + \sum_{k=1}^{m}[\mathbf{E}_{pq}]_{ik}[\mathbf{A}]_{kj} \\ &\quad + \sum_{k=1}^{m}[\mathbf{E}_{qp}]_{ik}[\mathbf{A}]_{kj} \\ &= [\mathbf{I}_m\mathbf{A}]_{ij} - \sum_{k=1}^{m}\delta_{ip}\delta_{pk}[\mathbf{A}]_{kj} - \sum_{k=1}^{m}\delta_{iq}\delta_{qk}[\mathbf{A}]_{kj} + \sum_{k=1}^{m}\delta_{ip}\delta_{qk}[\mathbf{A}]_{kj}\end{aligned}$$

$$+\sum_{k=1}^{m}\delta_{iq}\delta_{pk}[\mathbf{A}]_{kj}$$
$$= [\mathbf{A}]_{ij} - \delta_{ip}[\mathbf{A}]_{pj} - \delta_{iq}[\mathbf{A}]_{qj} + \delta_{ip}[\mathbf{A}]_{qj} + \delta_{iq}[\mathbf{A}]_{pj}. \tag{2.15}$$

Now, if $i \neq p, q$, then $\delta_{ip} = \delta_{iq} = 0$, and so for any $1 \leq j \leq n$ we find from (2.15) that $[\mathbf{M}_{p,q}\mathbf{A}]_{ij} = [\mathbf{A}]_{ij}$, which shows the $i$th row vector of $\mathbf{M}_{p,q}\mathbf{A}$ equals the $i$th row vector of $\mathbf{A}$.

If $i = p$, then from (2.15) we obtain

$$[\mathbf{M}_{p,q}\mathbf{A}]_{pj} = [\mathbf{A}]_{pj} - \delta_{pp}[\mathbf{A}]_{pj} - \delta_{pq}[\mathbf{A}]_{qj} + \delta_{pp}[\mathbf{A}]_{qj} + \delta_{pq}[\mathbf{A}]_{pj} = [\mathbf{A}]_{qj}$$

for all $1 \leq j \leq n$, so that

$$\begin{bmatrix}[\mathbf{M}_{p,q}\mathbf{A}]_{p1} & \cdots & [\mathbf{M}_{p,q}\mathbf{A}]_{pn}\end{bmatrix} = \begin{bmatrix}[\mathbf{A}]_{q1} & \cdots & [\mathbf{A}]_{qn}\end{bmatrix} = \mathbf{a}_q,$$

and it's seen that the $p$th row vector of $\mathbf{M}_{p,q}\mathbf{A}$ is the $q$th row vector of $\mathbf{A}$.

Finally, if $i = q$, then from (2.15) we obtain

$$[\mathbf{M}_{p,q}\mathbf{A}]_{qj} = [\mathbf{A}]_{qj} - \delta_{qp}[\mathbf{A}]_{pj} - \delta_{qq}[\mathbf{A}]_{qj} + \delta_{qp}[\mathbf{A}]_{qj} + \delta_{qq}[\mathbf{A}]_{pj} = [\mathbf{A}]_{pj}$$

for all $1 \leq j \leq n$, so that

$$\begin{bmatrix}[\mathbf{M}_{p,q}\mathbf{A}]_{q1} & \cdots & [\mathbf{M}_{p,q}\mathbf{A}]_{qn}\end{bmatrix} = \begin{bmatrix}[\mathbf{A}]_{p1} & \cdots & [\mathbf{A}]_{pn}\end{bmatrix} = \mathbf{a}_p,$$

and it's seen that the $q$th row vector of $\mathbf{M}_{p,q}\mathbf{A}$ is the $p$th row vector of $\mathbf{A}$.

We now see that $\mathbf{M}_{p,q}\mathbf{A}$ is identical to $\mathbf{A}$ save for a swap of the $p$th and $q$th row vectors, as was to be shown. ■

**Proposition 2.17.** *Suppose* $\mathbf{A} \in \mathbb{F}^{m\times n}$ *has column vectors* $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{F}^m$*. Let* $c \neq 0$*, and let* $1 \leq p, q \leq n$ *with* $p \neq q$*.*

1. $\mathbf{A}\mathbf{M}_{p,q}^\top(c)$ *is the matrix obtained from* $\mathbf{A}$ *by replacing the column vector* $\mathbf{a}_q$ *by* $\mathbf{a}_q + c\mathbf{a}_p$*:*

$$\begin{bmatrix}\cdots & \mathbf{a}_q & \cdots\end{bmatrix}\mathbf{M}_{p,q}^\top(c) = \begin{bmatrix}\cdots & \mathbf{a}_q + c\mathbf{a}_p & \cdots\end{bmatrix}.$$

2. $\mathbf{A}\mathbf{M}_{p,q}^\top$ *is the matrix obtained from* $\mathbf{A}$ *by interchanging* $\mathbf{a}_p$ *and* $\mathbf{a}_q$*:*

$$\begin{bmatrix}\cdots & \mathbf{a}_{\min\{p,q\}} & \cdots & \mathbf{a}_{\max\{p,q\}} & \cdots\end{bmatrix}\mathbf{M}_{p,q}^\top = \begin{bmatrix}\cdots & \mathbf{a}_{\max\{p,q\}} & \cdots & \mathbf{a}_{\min\{p,q\}} & \cdots\end{bmatrix}.$$

3. $\mathbf{A}\mathbf{M}_{p}^\top(c)$ *is the matrix obtained from* $\mathbf{A}$ *by replacing* $\mathbf{a}_p$ *by* $c\mathbf{a}_p$*:*

$$\begin{bmatrix}\cdots & \mathbf{a}_p & \cdots\end{bmatrix}\mathbf{M}_{p}^\top(c) = \begin{bmatrix}\cdots & c\mathbf{a}_p & \cdots\end{bmatrix}.$$

**Proof.**

*Proof of Part (1).* Observing that the row vectors of $\mathbf{A}^\top \in \mathbb{F}^{n\times m}$ are $\mathbf{a}_1^\top, \ldots, \mathbf{a}_n^\top$, by Proposition 2.16(1) we have,

$$\mathbf{M}_{p,q}(c)\mathbf{A}^\top = \mathbf{M}_{p,q}(c)\begin{bmatrix}\vdots \\ \mathbf{a}_q^\top \\ \vdots\end{bmatrix} = \begin{bmatrix}\vdots \\ \mathbf{a}_q^\top + c\mathbf{a}_p^\top \\ \vdots\end{bmatrix},$$

and so by Proposition 2.13,

$$\mathbf{A}\mathbf{M}_{p,q}^{\top}(c) = \left(\mathbf{M}_{p,q}(c)\mathbf{A}^{\top}\right)^{\top} = \begin{bmatrix} \vdots \\ \mathbf{a}_q^{\top} + c\mathbf{a}_p^{\top} \\ \vdots \end{bmatrix}^{\top} = \begin{bmatrix} \cdots & \mathbf{a}_q + c\mathbf{a}_p & \cdots \end{bmatrix}.$$

*Proof of Part (2).* By Propositions 2.13 and 2.16(2),

$$\begin{aligned}\mathbf{A}\mathbf{M}_{p,q}^{\top} = \left(\mathbf{M}_{p,q}\mathbf{A}^{\top}\right)^{\top} &= \left(\mathbf{M}_{p,q}\begin{bmatrix} \vdots \\ \mathbf{a}_{\min\{p,q\}}^{\top} \\ \vdots \\ \mathbf{a}_{\max\{p,q\}}^{\top} \\ \vdots \end{bmatrix}\right)^{\top} = \begin{bmatrix} \vdots \\ \mathbf{a}_{\max\{p,q\}}^{\top} \\ \vdots \\ \mathbf{a}_{\min\{p,q\}}^{\top} \\ \vdots \end{bmatrix}^{\top} \\ &= \begin{bmatrix} \cdots & \mathbf{a}_{\max\{p,q\}} & \cdots & \mathbf{a}_{\min\{p,q\}} & \cdots \end{bmatrix},\end{aligned}$$

and we're done. ∎

The proof of part (3) of Proposition 2.17 is left as a problem.

**Definition 2.18.** *Let $\mathbf{A} = [a_{ij}]_{m,n}$. The **ith pivot** of $\mathbf{A}$, $p_i$, is the first nonzero entry (from the left) in the $i$th row of $\mathbf{A}$:*

$$p_i = a_{ir_i}, \quad \textit{where } r_i = \min\{j : a_{ij} \neq 0\}$$

A **zero row** of a matrix $\mathbf{A}$, which is a row with all entries equal to 0, is said to have no pivot.

**Definition 2.19.** *A matrix is a **row-echelon matrix** (or has **row-echlon form**) if the following conditions are satisfied:*

1. *No zero row lies above a nonzero row.*
2. *Given two pivots $p_{i_1} = a_{i_1 j_1}$ and $p_{i_2} = a_{i_2 j_2}$, $j_2 > j_1$ whenever $i_2 > i_1$.*

*In a row-echelon matrix, a **pivot column** is a column that has a pivot. An **upper-triangular matrix** is a square matrix having row-echelon form. A **lower-triangular matrix** is a square matrix $\mathbf{A}$ for which $\mathbf{A}^{\top}$ has row-echelon form.*

The first condition requires that all zero rows be at the bottom of a matrix in row-echelon form. The second condition requires that if the first $k$ entries of the row $i$ are zeros, then at least the first $k+1$ entries of row $i+1$ must be zeros. Thus, all entries that lie below a pivot in a given column must be zero. Examples of matrices in reduced-echelon form are the following, with $p_i$ entries indicating pivots (i.e. nonzero entries) and asterisks indicating entries whose values may be zero or nonzero:

$$\begin{bmatrix} 0 & p_1 & * & * & * & * & * & * & * \\ 0 & 0 & p_2 & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & p_3 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_4 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} p_1 & * & * & * & * \\ 0 & p_2 & * & * & * \\ 0 & 0 & p_3 & * & * \\ 0 & 0 & 0 & p_4 & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} p_1 & * & * & * & * \\ 0 & p_2 & * & * & * \\ 0 & 0 & p_3 & * & * \\ 0 & 0 & 0 & p_4 & * \\ 0 & 0 & 0 & 0 & p_5 \end{bmatrix}.$$

The rightmost matrix is a square matrix and therefore happens to be in upper-triangular form. Its transpose,

$$\begin{bmatrix} p_1 & 0 & 0 & 0 & 0 \\ * & p_2 & 0 & 0 & 0 \\ * & * & p_3 & 0 & 0 \\ * & * & * & p_4 & 0 \\ * & * & * & * & p_5 \end{bmatrix},$$

is an example of a matrix in lower-triangular form. The diagonal entries of a square matrix need not be nonzero in order to have upper-triangular or lower-triangular form, however, so even

$$\begin{bmatrix} * & * & * & * & * \\ 0 & * & * & * & * \\ 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} * & 0 & 0 & 0 & 0 \\ * & * & 0 & 0 & 0 \\ * & * & * & 0 & 0 \\ * & * & * & * & 0 \\ * & * & * & * & * \end{bmatrix}$$

represent $5 \times 5$ triangular matrices regardless of what values we substitute for the asterisks.

Another way to define an upper-triangular matrix is to say it is a square matrix with all entries below the diagonal equal to 0. Similarly, a lower-triangular matrix is a square matrix with all entries above the diagonal equal to 0. A **diagonal matrix** is a square matrix $[a_{ij}]_n$ that is both upper-triangular and lower-triangular, so that $a_{ij} = 0$ whenever $i \neq j$. Any identity matrix $\mathbf{I}_n$ or square zero matrix $\mathbf{O}_n$ is a diagonal matrix, and (trivially) so too is any $1 \times 1$ matrix $[a]$.

**Proposition 2.20.** *Every matrix is row-equivalent to a matrix in row-echelon form. Thus if* $\mathbf{A}$ *is a square matrix, then it is row-equivalent to an upper-triangular matrix.*

**Proof.** We start by observing that any $1 \times n$ matrix is trivially in row-echelon form for any $n$. Let $m \in \mathbb{N}$ be arbitrary, and suppose that an $m \times n$ matrix is row-equivalent to a matrix in row-echelon form for any $n$. It remains to show that any $(m+1) \times n$ matrix is row-equivalent to a matrix in row-echelon form for any $n$, whereupon the proof will be finished by the Principle of Induction.

Let $n$ be arbitrary. Fix $\mathbf{A} = [a_{ij}]_{m+1,n}$. We may express $\mathbf{A}$ as a partitioned matrix,

$$\left[\begin{array}{c|c} \mathbf{B} & \mathbf{a} \\ \hline \mathbf{b} & b_n \end{array}\right],$$

where $\mathbf{B} = [a_{ij}]_{m,n-1}$. Observing that $[\,\mathbf{B}\,|\,\mathbf{a}\,]$ is an $m \times n$ matrix, by our inductive hypothesis it is row-equivalent to a matrix in row-echelon form $[\,\mathbf{R}\,|\,\mathbf{c}\,]$, and thus

$$\left[\begin{array}{c|c} \mathbf{B} & \mathbf{a} \\ \hline \mathbf{b} & b_n \end{array}\right] \sim \left[\begin{array}{c|c} \mathbf{R} & \mathbf{r} \\ \hline \mathbf{b} & b_n \end{array}\right] \tag{2.16}$$

Now, if

$$[\,\mathbf{b}\,|\,b_n\,] = [\,b_1 \ \cdots \ b_n\,]$$

consists of all zeros, or the pivot has column number greater than the pivot in the $m$th row, then the matrix at right in (2.16) is in row-echelon form and we are done. Supposing neither is the case, let $b_k$ be the pivot for $[\,\mathbf{b}\,|\,b_n\,]$, and let row $\ell$ be the lowest row in $[\,\mathbf{R}\,|\,\mathbf{r}\,]$ that does not have a pivot which lies to the right of column $k$. (If $k = 1$ then set $\ell = 0$.) We now effect a succession of R2 row operations,

$$\mathbf{A}' = \mathbf{M}_{\ell+2,\ell+1} \cdots \mathbf{M}_{m,m-1}\mathbf{M}_{m+1,m}\left[\begin{array}{c|c} \mathbf{R} & \mathbf{r} \\ \hline \mathbf{b} & b_n \end{array}\right],$$

which have the effect of moving $[\,\mathbf{b}\,|\,b_n\,]$ to just below row $\ell$ without altering the order of the other rows. (If $[\,\mathbf{b}\,|\,b_n\,]$ has pivot in the first column it will become the top row since $\ell = 0$.) We now have a matrix that either is in row-echelon form, or else rows $\ell$ and $\ell + 1$ have pivots in the same column.

Suppose the latter is the case. If $\ell = 0$, then the first entries of the first and second rows are nonzero scalars $x_1$ and $x_2$, respectively, and performing the R1 operation $\mathbf{M}_{1,2}(-x_2/x_1)$ of adding $-x_2/x_1$ times the first row to the second row will put a 0 at the beginning of the second row. If $\ell > 0$ we need do nothing, and proceed to partition $\mathbf{A}'$ as follows:

$$\left[\begin{array}{c|c} c_1 & \mathbf{c} \\ \hline \mathbf{0} & \mathbf{C} \end{array}\right]$$

Now, $[\,\mathbf{0}\,|\,\mathbf{C}\,]$ is an $m \times n$ matrix, so by our inductive hypothesis it is row-equivalent to a matrix $[\,\mathbf{0}\,|\,\mathbf{R}'\,]$ in row-echelon form. The resultant $(m + 1) \times n$ matrix,

$$\left[\begin{array}{c|c} c_1 & \mathbf{c} \\ \hline \mathbf{0} & \mathbf{R}' \end{array}\right],$$

is in row-echelon form, and since

$$\mathbf{A} = \left[\begin{array}{c|c} \mathbf{B} & \mathbf{a} \\ \hline \mathbf{b} & b_n \end{array}\right] \sim \left[\begin{array}{c|c} \mathbf{R} & \mathbf{r} \\ \hline \mathbf{b} & b_n \end{array}\right] \sim \left[\begin{array}{c|c} c_1 & \mathbf{c} \\ \hline \mathbf{0} & \mathbf{C} \end{array}\right] \sim \left[\begin{array}{c|c} c_1 & \mathbf{c} \\ \hline \mathbf{0} & \mathbf{R}' \end{array}\right]$$

we conclude that $\mathbf{A}$ is row-equivalent to a matrix in row-echelon form. ■

In the example to follow, and frequently throughout the remainder of the text, we will indicate the R1 elementary row operation of left-multiplying a matrix by $\mathbf{M}_{i,j}(c)$ by writing

$$cr_i + r_j \to r_j,$$

which may be read as "$c$ times row $i$ is added to row $j$ to yield a new row $j$" (see Prop-osition 2.16(1)). Similarly an R2 operation, which occurs when left-multiplying by $\mathbf{M}_{i,j}$, will be indicated by

$$r_i \leftrightarrow r_j,$$

which may be read as "interchange rows $i$ and $j$" (see Proposition 2.16(2)). Finally an R3 operation, which is the operation of left-multiplying by $\mathbf{M}_i(c)$, will be indicated by

$$cr_i \to r_i,$$

which may be read as "$c$ times row $i$ to yield a new row $i$" (see Proposition 2.16(3)).

**Example 2.21.** Using elementary row operations, find a row-equivalent matrix for

$$\begin{bmatrix} 0 & 1 & 3 & -2 \\ 2 & 1 & -4 & 3 \\ 2 & 3 & 2 & -1 \end{bmatrix}$$

that is in row-echelon form.

**Solution.** Call the matrix $\mathbf{A}$. Then,

$$\mathbf{A} \xrightarrow{r_1 \leftrightarrow r_2} \begin{bmatrix} 2 & 1 & -4 & 3 \\ 0 & 1 & 3 & -2 \\ 2 & 3 & 2 & -1 \end{bmatrix} \xrightarrow{-r_1+r_3 \to r_3} \begin{bmatrix} 2 & 1 & -4 & 3 \\ 0 & 1 & 3 & -2 \\ 0 & 2 & 6 & -4 \end{bmatrix} \xrightarrow{-2r_2+r_3 \to r_3} \begin{bmatrix} 2 & 1 & -4 & 3 \\ 0 & 1 & 3 & -2 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

In terms of elementary matrices we computed

$$\mathbf{M}_{2,3}(-2)\mathbf{M}_{1,3}(-1)\mathbf{M}_{1,2}\mathbf{A},$$

multiplying from right to left. ■

**Example 2.22.** A **permutation matrix** is a square matrix $\mathbf{P}$ with exactly one entry equal to 1 in each row and in each column, and all other entries equal to 0. Any such matrix may be obtained by rearranging (i.e. permuting) the rows of the identity matrix. Of course, $\mathbf{I}_n$ itself is a permutation matrix for any $n \in \mathbb{N}$, as is the $n \times n$ elementary matrix $\mathbf{M}_{i,j}$ that results from interchanging the $i$th and $j$th rows of $\mathbf{I}_n$.

The matrix

$$\mathbf{P} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

is a $3 \times 3$ permutation matrix that is obtained from $\mathbf{I}_3$ by performing the R2 operation $r_1 \leftrightarrow r_2$ followed by $r_2 \leftrightarrow r_3$. By Proposition 2.16(2), $\mathbf{P} = \mathbf{M}_{2,3}\mathbf{M}_{1,2}\mathbf{I}_3$, or simply $\mathbf{P} = \mathbf{M}_{2,3}\mathbf{M}_{1,2}$. Thus for any $3 \times n$ matrix $\mathbf{A}$ we have

$$\mathbf{PA} = (\mathbf{M}_{2,3}\mathbf{M}_{1,2})\mathbf{A} = \mathbf{M}_{2,3}(\mathbf{M}_{1,2}\mathbf{A}),$$

which shows that left-multiplication of $\mathbf{A}$ by $\mathbf{P}$ is equivalent to performing the following operations: first, the top and middle rows of $\mathbf{A}$ will be swapped to give a new matrix $\mathbf{A}'$; and second, the middle and bottom rows of $\mathbf{A}'$ will be swapped to give the final product. If $\mathbf{a}_1$, $\mathbf{a}_2$, and $\mathbf{a}_3$ are the row vectors of $\mathbf{A}$, then left-multiplication of $\mathbf{A}$ by $\mathbf{P}$ may be characterized as the action of assigning new positions to the row vectors of $\mathbf{A}$. Namely, $\mathbf{PA}$ sends $\mathbf{a}_1$ to row 3, $\mathbf{a}_2$ to row 1, and $\mathbf{a}_3$ to row 2. Note how these three placement operations correspond to the placement of the three entries equaling 1 in $\mathbf{P}$: column 1, row 3; column 2, row 1; and column 3, row 2. ■

## Problems

1. Show that, for any $1 \leq i \leq n$, the matrix $\mathbf{E}_{n,ii}$ is symmetric: $\mathbf{E}_{n,ii}^{\top} = \mathbf{E}_{n,ii}$.

2. What matrix results from right-multiplication $\mathbf{BP}$ of an $m \times 3$ matrix $\mathbf{B}$ by the $3 \times 3$ matrix $\mathbf{P}$ in Example 2.22? What permutation matrix $\mathbf{Q}$ should be used so that $\mathbf{BQ}$ permutes the columns of $\mathbf{B}$ the same way that $\mathbf{PA}$ permutes the rows of a $3 \times n$ matrix $\mathbf{A}$?

3. Prove part (3) of Proposition 2.16.

4. Prove part (3) of Proposition 2.17.

## 2.4 – The Inverse of a Matrix

**Definition 2.23.** *An $n \times n$ matrix $\mathbf{A}$ is **invertible** if there exists a matrix $\mathbf{B}$ such that*

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}_n,$$

*in which case we call $\mathbf{B}$ the **inverse** of $\mathbf{A}$ and denote it by the symbol $\mathbf{A}^{-1}$. A matrix that is not invertible is said to be **noninvertible** or **nonsingular**.*

From the definition we see that

$$\mathbf{AA}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_n,$$

provided that $\mathbf{A}^{-1}$ exists. Observe that $\mathbf{O}_n$ does not have an inverse since $\mathbf{AO}_n = \mathbf{O}_n$ for any $n \times n$ matrix $\mathbf{A}$. Also observe that, of necessity, if $\mathbf{A}$ is an $n \times n$ matrix, then $\mathbf{A}^{-1}$ must also be $n \times n$.

**Proposition 2.24.** *The inverse of a matrix $\mathbf{A}$ is unique.*

**Proof.** Let $\mathbf{A}$ be an invertible $n \times n$ matrix and suppose that $\mathbf{B}$ and $\mathbf{C}$ are such that

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}_n \quad \text{and} \quad \mathbf{AC} = \mathbf{CA} = \mathbf{I}_n.$$

From $\mathbf{BA} = \mathbf{I}_n$ we obtain

$$(\mathbf{BA})\mathbf{C} = \mathbf{I}_n\mathbf{C} = \mathbf{C},$$

and since matrix multiplication is associative by Theorem 2.7,

$$\mathbf{C} = (\mathbf{BA})\mathbf{C} = \mathbf{B}(\mathbf{AC}) = \mathbf{BI}_n = \mathbf{B}.$$

That is, $\mathbf{B} = \mathbf{C}$, and so $\mathbf{A}$ can have only one inverse. ∎

**Proposition 2.25.** *If $\mathbf{A}$ has $\mathbf{0}$ as a row or column vector, then $\mathbf{A}$ is not invertible.*

**Proof.** Let $\mathbf{A}$ be an $n \times n$ matrix with row vectors $\mathbf{a}_1, \dots, \mathbf{a}_n$. Suppose $\mathbf{a}_i = \mathbf{0}$ for some $1 \le i \le n$. Let

$$\mathbf{B} = \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_n \end{bmatrix}$$

be any $n \times n$ matrix. Since the $ii$-entry of $\mathbf{AB}$ is

$$\mathbf{a}_i \cdot \mathbf{b}_i = \mathbf{0} \cdot \mathbf{b}_i = 0,$$

it is seen that $\mathbf{AB} \neq \mathbf{I}_n$. Since $\mathbf{B}$ is arbitrary, we conclude that $\mathbf{A}$ has no inverse. That is, $\mathbf{A}$ is not invertible.

The proof that $\mathbf{A}$ is not invertible if it has $\mathbf{0}$ among its column vectors is similar. ∎

**Theorem 2.26.** *Let $k \in \mathbb{N}$. If $\mathbf{A}_1, \dots, \mathbf{A}_k \in \mathbb{F}^{n \times n}$ are invertible, then $\mathbf{A}_1 \cdots \mathbf{A}_k$ is invertible and*

$$(\mathbf{A}_1 \cdots \mathbf{A}_k)^{-1} = \mathbf{A}_k^{-1} \cdots \mathbf{A}_1^{-1}.$$

**Proof.** An inductive argument is suitable. The case when $k = 1$ is trivially true. Let $k \in \mathbb{N}$ be arbitrary, and suppose that the invertibility of $k$ matrices $\mathbf{A}_1, \ldots, \mathbf{A}_k \in \mathbb{F}^{n\times n}$ implies $\mathbf{A}_1 \cdots \mathbf{A}_k$ is invertible and $(\mathbf{A}_1 \cdots \mathbf{A}_k)^{-1} = \mathbf{A}_k^{-1} \cdots \mathbf{A}_1^{-1}$.

Suppose that $\mathbf{A}_1, \ldots, \mathbf{A}_{k+1}$ are invertible $n \times n$ matrices. Let

$$\mathbf{B} = \mathbf{A}_2 \cdots \mathbf{A}_{k+1} \quad \text{and} \quad \mathbf{C} = \mathbf{A}_{k+1}^{-1} \cdots \mathbf{A}_2^{-1}.$$

By the inductive hypothesis $\mathbf{B}$ is invertible, with

$$\mathbf{B}^{-1} = (\mathbf{A}_2 \cdots \mathbf{A}_{k+1})^{-1} = \mathbf{A}_{k+1}^{-1} \cdots \mathbf{A}_2^{-1} = \mathbf{C},$$

and so by Proposition 2.8

$$\begin{aligned}(\mathbf{A}_1 \cdots \mathbf{A}_{k+1})(\mathbf{A}_{k+1}^{-1} \cdots \mathbf{A}_1^{-1}) &= (\mathbf{A}_1\mathbf{B})(\mathbf{B}^{-1}\mathbf{A}_1^{-1}) = \mathbf{A}_1(\mathbf{B}\mathbf{B}^{-1})\mathbf{A}_1^{-1} \\ &= \mathbf{A}_1\mathbf{I}_n\mathbf{A}_1^{-1} = \mathbf{A}_1\mathbf{A}_1^{-1} = \mathbf{I}_n. \end{aligned} \tag{2.17}$$

(The associativity of matrix multiplication is implicitly used to justify the penultimate equality.)

Next, let

$$\mathbf{P} = \mathbf{A}_1 \cdots \mathbf{A}_k \quad \text{and} \quad \mathbf{Q} = \mathbf{A}_k^{-1} \cdots \mathbf{A}_1^{-1}.$$

By the inductive hypothesis $\mathbf{Q}$ is invertible, with

$$\mathbf{P}^{-1} = (\mathbf{A}_1 \cdots \mathbf{A}_k)^{-1} = \mathbf{A}_k^{-1} \cdots \mathbf{A}_1^{-1} = \mathbf{Q},$$

and so by Proposition 2.8

$$\begin{aligned}(\mathbf{A}_{k+1}^{-1} \cdots \mathbf{A}_1^{-1})(\mathbf{A}_1 \cdots \mathbf{A}_{k+1}) &= (\mathbf{A}_{k+1}^{-1}\mathbf{Q})(\mathbf{Q}^{-1}\mathbf{A}_{k+1}) = \mathbf{A}_{k+1}^{-1}(\mathbf{Q}\mathbf{Q}^{-1})\mathbf{A}_{k+1} \\ &= \mathbf{A}_{k+1}^{-1}\mathbf{I}_n\mathbf{A}_{k+1} = \mathbf{A}_{k+1}^{-1}\mathbf{A}_{k+1} = \mathbf{I}_n. \end{aligned} \tag{2.18}$$

From (2.17) and (2.18) we conclude that $\mathbf{A}_{k+1}^{-1} \cdots \mathbf{A}_1^{-1}$ is the inverse for $\mathbf{A}_1 \cdots \mathbf{A}_{k+1}$. That is, $\mathbf{A}_1 \cdots \mathbf{A}_{k+1}$ is invertible and

$$(\mathbf{A}_1 \cdots \mathbf{A}_{k+1})^{-1} = \mathbf{A}_{k+1}^{-1} \cdots \mathbf{A}_1^{-1}.$$

Therefore the statement of the theorem holds for all $k \in \mathbb{N}$ by the Principle of Induction. ■

We now proceed to establish some results that will help us determine whether a matrix has an inverse, and then develop an algorithm for computing the inverse of any invertible matrix. We start by examining elementary matrices, since the calculations involved are much simpler.

**Proposition 2.27.** *An elementary matrix is invertible, with*

$$\mathbf{M}_{i,j}^{-1}(c) = \mathbf{M}_{i,j}(-c), \quad \mathbf{M}_{i,j}^{-1} = \mathbf{M}_{i,j}, \quad \mathbf{M}_i^{-1}(c) = \mathbf{M}_i(c^{-1}).$$

**Proof.** Let $n \in \mathbb{N}$ be arbitrary, let $c \neq 0$, and let $i, j \in \{1, \ldots, n\}$ with $i \neq j$. Using the fact that $\mathbf{E}_{ji}^2 = \mathbf{O}_n$ by Proposition 2.14(2), we have

$$\begin{aligned}\mathbf{M}_{i,j}(-c)\mathbf{M}_{i,j}(c) &= (\mathbf{I}_n - c\mathbf{E}_{ji})(\mathbf{I}_n + c\mathbf{E}_{ji}) = \mathbf{I}_n^2 + c\mathbf{I}_n\mathbf{E}_{ji} - c\mathbf{E}_{ji}\mathbf{I}_n - c^2\mathbf{E}_{ji}^2 \\ &= \mathbf{I}_n + c\mathbf{E}_{ji} - c\mathbf{E}_{ji} - c^2\mathbf{O}_n = \mathbf{I}_n,\end{aligned}$$

and

$$\mathbf{M}_{i,j}(c)\mathbf{M}_{i,j}(-c) = (\mathbf{I}_n + c\mathbf{E}_{ji})(\mathbf{I}_n - c\mathbf{E}_{ji}) = \mathbf{I}_n^2 - c\mathbf{I}_n\mathbf{E}_{ji} + c\mathbf{E}_{ji}\mathbf{I}_n - c^2\mathbf{E}_{ji}^2$$
$$= \mathbf{I}_n - c\mathbf{E}_{ji} + c\mathbf{E}_{ji} - c^2\mathbf{O}_n = \mathbf{I}_n,$$

and therefore $\mathbf{M}_{i,j}^{-1}(-c)$ is the inverse for $\mathbf{M}_{i,j}(c)$.

Next we have

$$\begin{aligned}\mathbf{M}_{i,j}^2 &= (\mathbf{I}_n - \mathbf{E}_{ii} - \mathbf{E}_{jj} + \mathbf{E}_{ij} + \mathbf{E}_{ji})^2 \\ &= \mathbf{I}_n - \mathbf{E}_{ii} - \mathbf{E}_{jj} + \mathbf{E}_{ij} + \mathbf{E}_{ji} - \mathbf{E}_{ii} + \mathbf{E}_{ii}\mathbf{E}_{ii} + \mathbf{E}_{ii}\mathbf{E}_{jj} - \mathbf{E}_{ii}\mathbf{E}_{ij} - \mathbf{E}_{ii}\mathbf{E}_{ji} \\ &\quad - \mathbf{E}_{jj} + \mathbf{E}_{jj}\mathbf{E}_{ii} + \mathbf{E}_{jj}\mathbf{E}_{jj} - \mathbf{E}_{jj}\mathbf{E}_{ij} - \mathbf{E}_{jj}\mathbf{E}_{ji} + \mathbf{E}_{ij} - \mathbf{E}_{ij}\mathbf{E}_{ii} - \mathbf{E}_{ij}\mathbf{E}_{jj} \\ &\quad + \mathbf{E}_{ij}\mathbf{E}_{ij} + \mathbf{E}_{ij}\mathbf{E}_{ji} + \mathbf{E}_{ji} - \mathbf{E}_{ji}\mathbf{E}_{ii} - \mathbf{E}_{ji}\mathbf{E}_{jj} + \mathbf{E}_{ji}\mathbf{E}_{ij} + \mathbf{E}_{ji}\mathbf{E}_{ji} \\ &= \mathbf{I}_n - \mathbf{E}_{ii} - \mathbf{E}_{jj} + \mathbf{E}_{ij} + \mathbf{E}_{ji} - \mathbf{E}_{ii} + \mathbf{E}_{ii} - \mathbf{E}_{ij} - \mathbf{E}_{jj} + \mathbf{E}_{jj} - \mathbf{E}_{ji} + \mathbf{E}_{ij} \\ &\quad - \mathbf{E}_{ij} + \mathbf{E}_{ii} + \mathbf{E}_{ji} - \mathbf{E}_{ji} + \mathbf{E}_{jj} = \mathbf{I}_n,\end{aligned}$$

where the third equality owes itself to Proposition 2.14 and the understanding that $i \neq j$, and so for instance $\mathbf{E}_{ii}\mathbf{E}_{jj} = \mathbf{O}_n$, $\mathbf{E}_{ij}\mathbf{E}_{ij} = \mathbf{O}_n$, $\mathbf{E}_{ii}\mathbf{E}_{ii} = \mathbf{E}_{ii}$, $\mathbf{E}_{ij}\mathbf{E}_{ji} = \mathbf{E}_{ii}$, and so on. Therefore $\mathbf{M}_{i,j}$ is its own inverse.

Finally we show that the inverse for $\mathbf{M}_i(c)$ is $\mathbf{M}_i(c^{-1})$ for any fixed $1 \leq i \leq n$ and $c \neq 0$. Since $\mathbf{E}_{ii}^2 = \mathbf{E}_{ii}$ by Proposition 2.14(1), we have

$$\begin{aligned}\mathbf{M}_i(c)\mathbf{M}_i(c^{-1}) &= \big(\mathbf{I}_n + (c-1)\mathbf{E}_{ii}\big)\big(\mathbf{I}_n + (c^{-1}-1)\mathbf{E}_{ii}\big) \\ &= \mathbf{I}_n + (c^{-1}-1)\mathbf{E}_{ii} + (c-1)\mathbf{E}_{ii} + (c-1)(c^{-1}-1)\mathbf{E}_{ii}^2 \\ &= \mathbf{I}_n + (c^{-1}-1)\mathbf{E}_{ii} + (c-1)\mathbf{E}_{ii} - (c-1)\mathbf{E}_{ii} - (c^{-1}-1)\mathbf{E}_{ii} = \mathbf{I}_n,\end{aligned}$$

and similarly $\mathbf{M}_i(c^{-1})\mathbf{M}_i(c) = \mathbf{I}_n$. ■

**Proposition 2.28.** *Suppose* $\mathbf{A}$ *is row-equivalent to* $\mathbf{B}$*. Then* $\mathbf{A}$ *is invertible if and only if* $\mathbf{B}$ *is invertible.*

**Proof.** Since $\mathbf{A}$ is row-equivalent to $\mathbf{B}$, there exist elementary matrices $\mathbf{M}_1, \ldots, \mathbf{M}_k$ such that

$$\mathbf{M}_k \cdots \mathbf{M}_1\mathbf{A} = \mathbf{B}. \tag{2.19}$$

Now, suppose $\mathbf{A}$ invertible. The matrices $\mathbf{M}_1, \ldots, \mathbf{M}_k$ are invertible by Proposition 2.27, and since $\mathbf{A}$ is invertible by hypothesis, by Theorem 2.26 we conclude that $\mathbf{B}$ is invertible.

Next, suppose $\mathbf{B}$ is invertible. From (2.19) we have

$$\mathbf{A} = (\mathbf{M}_k \cdots \mathbf{M}_1)^{-1}\mathbf{B} = \mathbf{M}_1^{-1} \cdots \mathbf{M}_k^{-1}\mathbf{B},$$

where $\mathbf{M}_1^{-1}, \ldots, \mathbf{M}_k^{-1}$ are all elementary matrices by Proposition 2.27. Thus $\mathbf{B}$ is row-equivalent to $\mathbf{A}$, and since $\mathbf{B}$ is invertible, the conclusion that $\mathbf{A}$ is invertible follows from the first part of the proof. ■

**Proposition 2.29.** *If* $\mathbf{A}$ *is invertible, then* $\mathbf{A}$ *is row-equivalent to an upper-triangular matrix with nonzero diagonal elements.*

**Proof.** Let $\mathbf{A}$ be an $n \times n$ matrix. Then $\mathbf{A}$ is row-equivalent to an upper-triangular matrix $\mathbf{U} = [u_{ij}]_n$ by Proposition 2.20. Suppose that $u_{ii} = 0$ for some $1 \leq i \leq n$. Then $u_{kk} = 0$ for all $i \leq k \leq n$, and in particular $u_{nn} = 0$ so that the $n$th row vector of $\mathbf{U}$ is $\mathbf{0}$. Hence $\mathbf{U}$ is not invertible by Proposition 2.25, and since $\mathbf{A} \sim \mathbf{U}$ it follows that $\mathbf{A}$ is not invertible by Proposition 2.28. We have now proven that if $\mathbf{A}$ is row-equivalent to an upper-triangular matrix with a diagonal element equalling 0, then $\mathbf{A}$ is not invertible. This is equivalent to the statement of the proposition. ■

**Theorem 2.30.** *An* $n \times n$ *matrix* $\mathbf{A}$ *is invertible if and only if* $\mathbf{A}$ *is row-equivalent to* $\mathbf{I}_n$*.*

**Proof.** Suppose $\mathbf{A} \in \mathbb{F}^{n\times n}$ is invertible. By Proposition 2.29 $\mathbf{A}$ is row-equivalent to an upper triangular matrix $\mathbf{U} = [u_{ij}]_n$ with nonzero diagonal elements. We multiply each row $i$ of $\mathbf{U}$ by $u_{ii}^{-1}$ (which of course is defined since $u_{ii} \neq 0$) to obtain a row-equivalent upper-triangular matrix $\mathbf{U}_1$ with diagonal entries all equal to 1:

$$\mathbf{M}_1(u_{11}^{-1}) \cdots \mathbf{M}_n(u_{nn}^{-1})\mathbf{U} = \mathbf{U}_1. \tag{2.20}$$

In particular the first column of $\mathbf{U}'$ is $\mathbf{e}_1$ as desired, recalling that $\mathbf{I}_n = [\,\mathbf{e}_1 \ \cdots \ \mathbf{e}_n\,]$. If we add $-u_{12}$ times the second row of $\mathbf{U}_1$ to the first row to obtain a row-equivalent matrix $\mathbf{U}_2$,

$$\mathbf{M}_{2,1}(-u_{12})\mathbf{U}_1 = \mathbf{U}_2,$$

we find in particular that $\mathbf{U}_2$ is upper-triangular with first column $\mathbf{e}_1$ and second column $\mathbf{e}_2$. Proceeding in this fashion to the $j$th column, we have an upper-triangular matrix

$$\mathbf{U}_{j-1} = \left[\,\mathbf{e}_1 \ \cdots \ \mathbf{e}_{j-1} \ \ \mathbf{u}_j \ \cdots \ \mathbf{u}_n\,\right]$$

on which we perform a sequence of R1 row operations to obtain a row-equivalent matrix $\mathbf{U}_j$:

$$\left(\prod_{i=1}^{j-1}\mathbf{M}_{j,i}(-u_{ij})\right)\mathbf{U}_{j-1} = \mathbf{M}_{j,1}(-u_{1j})\cdots\mathbf{M}_{j,j-1}(-u_{j-1,j})\mathbf{U}_{j-1} = \mathbf{U}_j, \tag{2.21}$$

where

$$\mathbf{U}_j = \left[\,\mathbf{e}_1 \ \cdots \ \mathbf{e}_j \ \ \mathbf{u}_{j+1} \ \cdots \ \mathbf{u}_n\,\right]$$

Equation (2.21) holds for $j = 2, \ldots, n$, and gives $\mathbf{U}_n$ as

$$\mathbf{U}_n = \left(\prod_{i=1}^{n-1}\mathbf{M}_{n,i}(-u_{in})\right)\left(\prod_{i=1}^{n-2}\mathbf{M}_{n-1,i}(-u_{i,n-1})\right)\cdots\left(\prod_{i=1}^{1}\mathbf{M}_{2,i}(-u_{i2})\right)\mathbf{U}_1.$$

Observing that $\mathbf{U}_n = \mathbf{I}_n$, and recalling (2.20), we finally obtain

$$\mathbf{I}_n = \left(\prod_{i=1}^{n-1}\mathbf{M}_{n,i}(-u_{in})\right)\left(\prod_{i=1}^{n-2}\mathbf{M}_{n-1,i}(-u_{i,n-1})\right)\cdots\left(\prod_{i=1}^{1}\mathbf{M}_{2,i}(-u_{i2})\right)\left(\prod_{i=1}^{n}\mathbf{M}_i(u_{ii}^{-1})\right)\mathbf{U},$$

which demonstrates in explicit terms that $\mathbf{U}$ is row-equivalent to $\mathbf{I}_n$. Now, $\mathbf{A} \sim \mathbf{U}$ and $\mathbf{U} \sim \mathbf{I}_n$ imply that $\mathbf{A} \sim \mathbf{I}_n$ and the first part of the proof is finished.

The converse is much easier to prove. Suppose that $\mathbf{A}$ is row-equivalent to $\mathbf{I}_n$. Since $\mathbf{I}_n$ is invertible, by Proposition 2.28 we conclude that $\mathbf{A}$ is invertible. ■

This theorem gives rise to a sure method for finding the inverse of any invertible matrix $\mathbf{A}$. If $\mathbf{A} \in \mathbb{F}^{n\times n}$ is invertible, then $\mathbf{A} \sim \mathbf{I}_n$, which is to say there exist elementary matrices $\mathbf{M}_1, \dots, \mathbf{M}_k$ such that $\mathbf{M}_k \cdots \mathbf{M}_1\mathbf{A} = \mathbf{I}_n$. Now,

$$\begin{aligned}
\mathbf{M}_k \cdots \mathbf{M}_1\mathbf{A} = \mathbf{I}_n \;&\Leftrightarrow\; (\mathbf{M}_k \cdots \mathbf{M}_1\mathbf{A})\mathbf{A}^{-1} = \mathbf{I}_n\mathbf{A}^{-1} \\
&\Leftrightarrow\; \mathbf{M}_k \cdots \mathbf{M}_1(\mathbf{A}\mathbf{A}^{-1}) = \mathbf{A}^{-1} \\
&\Leftrightarrow\; \mathbf{A}^{-1} = \mathbf{M}_k \cdots \mathbf{M}_1\mathbf{I}_n,
\end{aligned}$$

which demonstrates that the selfsame elementary row operations $\mathbf{M}_1, \dots, \mathbf{M}_k$ that transform $\mathbf{A}$ into $\mathbf{I}_n$ will transform $\mathbf{I}_n$ into $\mathbf{A}^{-1}$. In practice we set up a partitioned matrix $[\,\mathbf{A}\,|\,\mathbf{I}_n\,]$, and apply identical sequences of elementary row operations to each submatrix until the submatrix that started as $\mathbf{A}$ has become $\mathbf{I}_n$. At that point the submatrix that started as $\mathbf{I}_n$ will be $\mathbf{A}^{-1}$:

$$[\,\mathbf{A}\,|\,\mathbf{I}_n\,] \;\sim\; [\,\mathbf{M}_1\mathbf{A}\,|\,\mathbf{M}_1\mathbf{I}_n\,] \;\sim\; \cdots \;\sim\; [\,\mathbf{M}_k \cdots \mathbf{M}_1\mathbf{A}\,|\,\mathbf{M}_k \cdots \mathbf{M}_1\mathbf{I}_n\,] = [\,\mathbf{I}_n\,|\,\mathbf{A}^{-1}\,].$$

The next example illustrates the procedure.

**Example 2.31.** Find the inverse of the matrix

$$\begin{bmatrix} 2 & 4 & 3 \\ -1 & 3 & 0 \\ 0 & 2 & 1 \end{bmatrix}$$

**Solution.** We employ the same sequence of elementary row operations on both $\mathbf{A}$ and $\mathbf{I}_3$, as follows.

$$\left[\begin{array}{ccc|ccc} 2 & 4 & 3 & 1 & 0 & 0 \\ -1 & 3 & 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & 0 & 1 \end{array}\right] \xrightarrow[-r_1 \to r_1]{r_2 \leftrightarrow r_1} \left[\begin{array}{ccc|ccc} 1 & -3 & 0 & 0 & -1 & 0 \\ 2 & 4 & 3 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 1 \end{array}\right] \xrightarrow{-2r_1 + r_2 \to r_2}$$

$$\left[\begin{array}{ccc|ccc} 1 & -3 & 0 & 0 & -1 & 0 \\ 0 & 10 & 3 & 1 & 2 & 0 \\ 0 & 2 & 1 & 0 & 0 & 1 \end{array}\right] \xrightarrow{r_2 \leftrightarrow r_3} \left[\begin{array}{ccc|ccc} 1 & -3 & 0 & 0 & -1 & 0 \\ 0 & 2 & 1 & 0 & 0 & 1 \\ 0 & 10 & 3 & 1 & 2 & 0 \end{array}\right] \xrightarrow{-5r_2 + r_3 \to r_3}$$

$$\left[\begin{array}{ccc|ccc} 1 & -3 & 0 & 0 & -1 & 0 \\ 0 & 2 & 1 & 0 & 0 & 1 \\ 0 & 0 & -2 & 1 & 2 & -5 \end{array}\right] \xrightarrow{\frac{1}{2}r_2 \to r_2} \left[\begin{array}{ccc|ccc} 1 & -3 & 0 & 0 & -1 & 0 \\ 0 & 1 & 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & -2 & 1 & 2 & -5 \end{array}\right] \xrightarrow{3r_2 + r_1 \to r_1}$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 3/2 & 0 & -1 & 3/2 \\ 0 & 1 & 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & -2 & 1 & 2 & -5 \end{array}\right] \xrightarrow[\frac{3}{4}r_3 + r_1 \to r_1]{\frac{1}{4}r_3 + r_2 \to r_2} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 3/4 & 1/2 & -9/4 \\ 0 & 1 & 0 & 1/4 & 1/2 & -3/4 \\ 0 & 0 & -2 & 1 & 2 & -5 \end{array}\right] \xrightarrow{-\frac{1}{2}r_3 \to r_3}$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 3/4 & 1/2 & -9/4 \\ 0 & 1 & 0 & 1/4 & 1/2 & -3/4 \\ 0 & 0 & 1 & -1/2 & -1 & 5/2 \end{array}\right].$$

Therefore

$$\mathbf{A}^{-1} = \begin{bmatrix} \frac{3}{4} & \frac{1}{2} & -\frac{9}{4} \\ \frac{1}{4} & \frac{1}{2} & -\frac{3}{4} \\ -\frac{1}{2} & -1 & \frac{5}{2} \end{bmatrix}$$

is the inverse of $\mathbf{A}$. ■

**Proposition 2.32.** *If $\mathbf{A} \in \mathbb{F}^{n\times n}$ is invertible, then $\mathbf{A}^\top$ is invertible and*

$$(\mathbf{A}^\top)^{-1} = (\mathbf{A}^{-1})^\top.$$

**Proof.** Suppose that $\mathbf{A} \in \mathbb{F}^{n\times n}$ is invertible, so that $\mathbf{A}^{-1}$ exists. Now, by Proposition 2.13,

$$\mathbf{A}\mathbf{A}^{-1} = \mathbf{I}_n \;\;\Rightarrow\;\; (\mathbf{A}\mathbf{A}^{-1})^\top = \mathbf{I}_n^\top \;\;\Rightarrow\;\; (\mathbf{A}^{-1})^\top\mathbf{A}^\top = \mathbf{I}_n$$

and

$$\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_n \;\;\Rightarrow\;\; (\mathbf{A}^{-1}\mathbf{A})^\top = \mathbf{I}_n^\top \;\;\Rightarrow\;\; \mathbf{A}^\top(\mathbf{A}^{-1})^\top = \mathbf{I}_n.$$

Now,

$$(\mathbf{A}^{-1})^\top\mathbf{A}^\top = \mathbf{A}^\top(\mathbf{A}^{-1})^\top = \mathbf{I}_n$$

shows that $(\mathbf{A}^{-1})^\top$ is the inverse of $\mathbf{A}^\top$. Therefore $\mathbf{A}^\top$ is invertible, and moreover $(\mathbf{A}^\top)^{-1} = (\mathbf{A}^{-1})^\top$. ■

**Example 2.33.** If $\mathbf{P} \in \mathbb{F}^{n\times n}$ is a permutation matrix (see Example 2.22), then $\mathbf{P}^{-1} = \mathbf{P}^\top$. To see this, first observe that $\mathbf{P}$ may be obtained by permuting the rows of $\mathbf{I}_n$, and since any permutation of $n$ objects may be accomplished by performing at most $n$ transpositions (i.e. the operation of swapping two objects), we may write $\mathbf{P} = \mathbf{M}_1\mathbf{M}_2\cdots\mathbf{M}_m$, where $m \le n$, and for each $1 \le k \le m$ the matrix $\mathbf{M}_k$ is an elementary matrix of the form $\mathbf{M}_{i,j}$ for some $i, j \in \{1, \dots, n\}$ with $i \ne j$.

Next, we claim that any elementary matrix $\mathbf{M}_{i,j}$ is symmetric: $\mathbf{M}_{i,j}^\top = \mathbf{M}_{i,j}$. To show this, since

$$\mathbf{M}_{i,j} = \mathbf{I}_n - \mathbf{E}_{ii} - \mathbf{E}_{jj} + \mathbf{E}_{ij} + \mathbf{E}_{ji},$$

we need to show that, generally, $\mathbf{E}_{pp}^\top = \mathbf{E}_{pp}$, and $\mathbf{E}_{pq}^\top = \mathbf{E}_{qp}$. The former is a problem in §2.3, so we'll show the latter. Let $i, j \in \{1, \dots, n\}$ with $i \ne j$. By Definition 2.2 and equation (2.14),

$$[\mathbf{E}_{pq}^\top]_{ij} = [\mathbf{E}_{pq}]_{ji} = \delta_{jp}\delta_{qi},$$

whereas by (2.14),

$$[\mathbf{E}_{qp}]_{ij} = \delta_{iq}\delta_{pj} = \delta_{qi}\delta_{jp} = \delta_{jp}\delta_{qi}.$$

Hence $[\mathbf{E}_{pq}^\top]_{ij} = [\mathbf{E}_{qp}]_{ij}$, and therefore $\mathbf{E}_{pq}^\top = \mathbf{E}_{qp}$. It is clear that $\mathbf{I}_n$ is symmetric, so that $\mathbf{I}_n^\top = \mathbf{I}_n$. Now, by Proposition 2.3(2) and the foregoing findings,

$$\begin{aligned}\mathbf{M}_{i,j}^\top &= (\mathbf{I}_n - \mathbf{E}_{ii} - \mathbf{E}_{jj} + \mathbf{E}_{ij} + \mathbf{E}_{ji})^\top = \mathbf{I}_n^\top - \mathbf{E}_{ii}^\top - \mathbf{E}_{jj}^\top + \mathbf{E}_{ij}^\top + \mathbf{E}_{ji}^\top \\ &= \mathbf{I}_n - \mathbf{E}_{ii} - \mathbf{E}_{jj} + \mathbf{E}_{ji} + \mathbf{E}_{ij} = \mathbf{M}_{i,j}.\end{aligned}$$

Finally, we have

$$\mathbf{P}^\top = (\mathbf{M}_1\mathbf{M}_2\cdots\mathbf{M}_m)^\top = \mathbf{M}_m^\top\cdots\mathbf{M}_2^\top\mathbf{M}_1^\top \qquad \text{(Proposition 2.13)}$$

$$
\begin{aligned}
&= \mathbf{M}_m \cdots \mathbf{M}_2 \mathbf{M}_1 = \mathbf{M}_m^{-1} \cdots \mathbf{M}_2^{-1} \mathbf{M}_1^{-1} && \text{(Proposition 2.27)} \\
&= (\mathbf{M}_1 \mathbf{M}_2 \cdots \mathbf{M}_m)^{-1} = \mathbf{P}^{-1}, && \text{(Theorem 2.26)}
\end{aligned}
$$

as was to be shown. ■

## 2.5 – Systems of Linear Equations

As usual let $\mathbb{F}$ denote a field. A **system** over $\mathbb{F}$ of $m$ linear equations in $n$ unknowns $x_1, \ldots, x_n$ is a set of equations of the form

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \quad\vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad\quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{2.22}$$

for which $a_{ij} \in \mathbb{F}$ and $b_i \in \mathbb{F}$ for all integers $1 \le i \le m$ and $1 \le j \le n$. The scalars $a_{ij}$ are the **coefficients** of the system, and $b_1, \ldots, b_m$ are the **constant terms**. If $S_i$ is the solution set of the $i$th equation, which is to say

$$S_i = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{F}^n \ : \ a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i \right\},$$

then the **solution set** of the system (2.22) is

$$S = S_1 \cap \cdots \cap S_m = \bigcap_{i=1}^m S_i,$$

or equivalently

$$S = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{F}^n \ : \ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in S_i \text{ for all } 1 \le i \le m \right\}.$$

A system is **consistent** if its solution set $S$ is nonempty (i.e. the system has at least one solution), and **inconsistent** if $S = \varnothing$ (i.e. the system has no solution). A consistent system is **dependent** if $S$ has an infinite number of elements, and **independent** if $S$ has precisely one element. As we will see later, a system of linear equations has either no solution, precisely one solution, or an infinite number of solutions. There are no other possibilities.

If we define

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \quad \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \quad \text{and} \quad \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}, \tag{2.23}$$

then the system (2.22) may be written as the matrix equation $\mathbf{Ax} = \mathbf{b}$,

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}. \tag{2.24}$$

In this representation of the system, all solutions $\mathbf{x}$ are expressed as column vectors

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \tag{2.25}$$

so that the solution set $S$ is given as

$$S = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{F}^n \;\middle|\; \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in S_i \text{ for all } 1 \le i \le m \right\}.$$

As a further notational convenience we may express the matrix equation (2.24) as an **augmented matrix** featuring only the coefficients and constant terms of the system,

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right]. \tag{2.26}$$

We see the augmented matrix is just the partitioned matrix $[\,\mathbf{A}\,|\,\mathbf{b}\,]$. The fact that there are $n$ columns of coefficients (understood to be the columns to the left of the vertical line) informs us that there are $n$ variables, and since an $n$-variable system of equations is fully determined by its coefficients and constant terms, no information is lost in doing this.

We now consider how the system (2.22) is affected if we left-multiply the corresponding augmented matrix $[\,\mathbf{A}\,|\,\mathbf{b}\,]$ by any one of the three elementary matrices $\mathbf{M}_{i,j}(c)$, $\mathbf{M}_{i,j}$, or $\mathbf{M}_i(c)$.

By Proposition 2.16 we know that

$$\mathbf{M}_{i,j}(c)[\,\mathbf{A}\,|\,\mathbf{b}\,]$$

will effect an R1 operation, specifically adding $c \neq 0$ times the $i$th row of $[\,\mathbf{A}\,|\,\mathbf{b}\,]$ to the $j$th row. What results is a new augmented matrix $[\,\mathbf{A}'\,|\,\mathbf{b}'\,]$ corresponding to a new system of equations in which $c$ times the $i$th equation has been added to the $j$th equation. But is the solution set $S'$ of the new system $[\,\mathbf{A}'\,|\,\mathbf{b}'\,]$ any different from the solution set $S$ of the original system $[\,\mathbf{A}\,|\,\mathbf{b}\,]$? In the system $[\,\mathbf{A}\,|\,\mathbf{b}\,]$ the $i$th and $j$th equations are

$$\sum_{k=1}^{n} a_{ik}x_k = b_i \quad \text{and} \quad \sum_{k=1}^{n} a_{jk}x_k = b_j, \tag{2.27}$$

which have solution sets $S_i$ and $S_j$, respectively; and in the system $[\,\mathbf{A}'\,|\,\mathbf{b}'\,]$ the $i$th and $j$th equations are

$$\sum_{k=1}^{n} a_{ik}x_k = b_i \quad \text{and} \quad \sum_{k=1}^{n}(ca_{ik} + a_{jk})x_k = cb_i + b_j, \tag{2.28}$$

which have solution sets $S_i'$ and $S_j'$, respectively. We will show that $S_i \cap S_j = S_i' \cap S_j'$. To start, we first observe that the $i$th equation of $[\,\mathbf{A}'\,|\,\mathbf{b}'\,]$ is the same as the $i$th equation of $[\,\mathbf{A}\,|\,\mathbf{b}\,]$, so $S_i' = S_i$ and our task becomes that of showing $S_i \cap S_j = S_i \cap S_j'$.

Let $\mathbf{x} \in S_i \cap S_j$ be given by (2.25). Thus the scalars $x_1, \ldots, x_n$ are such that the equations in (2.27) are satisfied. We have, using (2.27),

$$\sum_{k=1}^{n}(ca_{ik} + a_{jk})x_k = c\sum_{k=1}^{n} a_{ik} + \sum_{k=1}^{n} a_{jk}x_k = cb_i + b_j,$$

which shows that $x_1, \ldots, x_n$ satisfy the second equation in (2.28) and so $\mathbf{x} \in S'_j$. From $\mathbf{x} \in S_i$ and $\mathbf{x} \in S'_j$ we have $\mathbf{x} \in S_i \cap S'_j$, and therefore $S_i \cap S_j \subseteq S_i \cap S'_j$.

Now suppose $\mathbf{x} \in S_i \cap S'_j$, so that the scalars $x_1, \ldots, x_n$ are assumed to satisfy the equations in (2.28). Multiplying the first equation by $c$ yields

$$\sum_{k=1}^{n} ca_{ik}x_k = cb_i,$$

so that

$$\sum_{k=1}^{n}(ca_{ik} + a_{jk})x_k - \sum_{k=1}^{n} ca_{ik}x_k = (cb_i + b_j) - cb_i$$

obtains from the second equation in (2.28), which in turn implies that

$$\sum_{k=1}^{n} a_{jk}x_k = b_j$$

and so $\mathbf{x} \in S_j$. Since $\mathbf{x} \in S_i$ also, we conclude that $\mathbf{x} \in S_i \cap S_j$ and therefore $S_i \cap S'_j \subseteq S_i \cap S_j$. We have now shown that $S_i \cap S'_j = S_i \cap S_j$, so that

$$S' = (S_i \cap S'_j) \cap \left(\bigcap_{k \neq i,j} S_k\right) = (S_i \cap S_j) \cap \left(\bigcap_{k \neq i,j} S_k\right) = \bigcap_{k=1}^{m} S_k = S.$$

Thus, performing an $\mathsf{R1}$ operation

$$\mathbf{M}_{i,j}(c)[\,\mathbf{A} \,|\, \mathbf{b}\,] = [\,\mathbf{A}' \,|\, \mathbf{b}'\,]$$

on the augmented matrix $[\,\mathbf{A} \,|\, \mathbf{b}\,]$ corresponding to a system of equations results in a new augmented matrix $[\,\mathbf{A}' \,|\, \mathbf{b}'\,]$ that corresponds to a new system of equations *that has the same solution set as the original system.* This is clearly also the case whenever performing an $\mathsf{R2}$ operation $\mathbf{M}_{i,j}[\,\mathbf{A} \,|\, \mathbf{b}\,]$, since the outcome yields an augmented matrix corresponding to a system of equations that is identical to the original system except that the $i$th and $j$th equations have traded places. (Again, a system of equations is a set of equations, and sets are blind to order.) Finally, an $\mathsf{R3}$ operation $\mathbf{M}_i(c)[\,\mathbf{A} \,|\, \mathbf{b}\,]$ results in an augmented matrix corresponding to a system of equations that is identical to the original system except that the $i$th equation has been multiplied by a nonzero scalar $c$, which does not alter the solution set of the $i$th equation and therefore does not alter the solution set of the system as a whole. We have proven the following.

**Proposition 2.34.** *Any elementary row operation performed on the augmented matrix* $[\,\mathbf{A} \,|\, \mathbf{b}\,]$ *of a system of linear equations results in an augmented matrix* $[\,\mathbf{A}' \,|\, \mathbf{b}'\,]$ *whose corresponding system has the same solution set.*

**Definition 2.35.** *Two systems of linear equations are* ***equivalent*** *if their corresponding augmented matrices are row-equivalent.*

In light of Proposition 2.34 it is immediate that equivalent systems of linear equations have the same solution set. Thus, to solve a system of linear equations such as (2.22), one fairly efficient approach is to perform elementary row operations on its corresponding augmented matrix until it is in row-echelon form, at which point it is easy to determine the system's solution set. The process is known as **Gaussian elimination.**

**Example 2.36.** Apply Gaussian elimination to determine the solution set of the system

$$\begin{cases} 3x + y + 4z + \phantom{4}w = \phantom{1}6 \\ 2x \phantom{{}+y} + 3z + 4w = 13 \\ \phantom{3x+{}} y - 2z - \phantom{4}w = \phantom{1}0 \\ \phantom{3}x - y + \phantom{4}z + \phantom{4}w = \phantom{1}3 \end{cases}$$

**Solution.** The corresponding augmented matrix for the system is

$$\left[\begin{array}{cccc|c} 3 & 1 & 4 & 1 & 6 \\ 2 & 0 & 3 & 4 & 13 \\ 0 & 1 & -2 & -1 & 0 \\ 1 & -1 & 1 & 1 & 3 \end{array}\right].$$

We'll start by interchanging the 1st and 4th rows, since it will be convenient having a 1 at the top of the 1st column. Also we'll interchange the 2nd and 3rd rows so as to move the 0 in the 2nd column down to a position where row-echelon form requires a 0 entry.

$$\left[\begin{array}{cccc|c} 3 & 1 & 4 & 1 & 6 \\ 2 & 0 & 3 & 4 & 13 \\ 0 & 1 & -2 & -1 & 0 \\ 1 & -1 & 1 & 1 & 3 \end{array}\right] \xrightarrow[r_2 \leftrightarrow r_3]{r_1 \leftrightarrow r_4} \left[\begin{array}{cccc|c} 1 & -1 & 1 & 1 & 3 \\ 0 & 1 & -2 & -1 & 0 \\ 2 & 0 & 3 & 4 & 13 \\ 3 & 1 & 4 & 1 & 6 \end{array}\right] \xrightarrow[-3r_1 + r_4 \to r_4]{-2r_1 + r_3 \to r_3}$$

$$\left[\begin{array}{cccc|c} 1 & -1 & 1 & 1 & 3 \\ 0 & 1 & -2 & -1 & 0 \\ 0 & 2 & 1 & 2 & 7 \\ 0 & 4 & 1 & -2 & -3 \end{array}\right] \xrightarrow[-4r_2 + r_4 \to r_4]{-2r_2 + r_3 \to r_3} \left[\begin{array}{cccc|c} 1 & -1 & 1 & 1 & 3 \\ 0 & 1 & -2 & -1 & 0 \\ 0 & 0 & 5 & 4 & 7 \\ 0 & 0 & 9 & 2 & -3 \end{array}\right] \xrightarrow{-\frac{9}{5}r_3 + r_4 \to r_4}$$

$$\left[\begin{array}{cccc|c} 1 & -1 & 1 & 1 & 3 \\ 0 & 1 & -2 & -1 & 0 \\ 0 & 0 & 5 & 4 & 7 \\ 0 & 0 & 0 & -\frac{26}{5} & -\frac{78}{5} \end{array}\right] \xrightarrow{-\frac{5}{26}r_4 \to r_4} \left[\begin{array}{cccc|c} 1 & -1 & 1 & 1 & 3 \\ 0 & 1 & -2 & -1 & 0 \\ 0 & 0 & 5 & 4 & 7 \\ 0 & 0 & 0 & 1 & 3 \end{array}\right]$$

The fifth matrix above is in row-echelon form, so technically the last row operation is not required. On the other hand it certainly is desirable to eliminate any fractions if there's an easy way to do it. We have obtained the following equivalent system of equations:

$$\begin{cases} x - y + \phantom{2}z + \phantom{4}w = 3 \\ \phantom{x-{}} y - 2z - \phantom{4}w = 0 \\ \phantom{x-y-{}} 5z + 4w = 7 \\ \phantom{x-y-5z+4} w = 3 \end{cases}$$

We may now determine the solution to the system by employing so-called "backward substitution." Taking $w = 3$ from the 4th equation and substituting into the 3rd equation yields

$$5z + 4(3) = 7 \quad\Rightarrow\quad 5z = -5 \quad\Rightarrow\quad z = -1.$$

Taking $w = 3$ and $z = -1$ and substituting into the 2nd equation yields

$$y - 2(-1) - 3 = 0 \quad\Rightarrow\quad y = 1.$$

Finally, substituting $w = 3$, $z = -1$, and $y = 1$ into the 1st equation yields

$$x - 1 + (-1) + 3 = 3 \quad\Rightarrow\quad x = 2.$$

Therefore the only solution to the system is $(x, y, z, w) = (2, 1, -1, 3)$, which is to say the solution set is $\{(2, 1, -1, 3)\}$. ■

**Example 2.37.** Apply Gaussian elimination to determine the solution set of the system

$$\begin{cases} -3x - 5y + 36z = 10 \\ -x \phantom{{}-5y} + 7z = 5 \\ x + y - 10z = -4 \end{cases} \tag{2.29}$$

Write the solution set in terms of column vectors.

**Solution.** The corresponding augmented matrix for the system is

$$\left[\begin{array}{rrr|r} -3 & -5 & 36 & 10 \\ -1 & 0 & 7 & 5 \\ 1 & 1 & -10 & -4 \end{array}\right].$$

We transform this matrix into row-echelon form:

$$\left[\begin{array}{rrr|r} -3 & -5 & 36 & 10 \\ -1 & 0 & 7 & 5 \\ 1 & 1 & -10 & -4 \end{array}\right] \xrightarrow{r_1 \leftrightarrow r_3} \left[\begin{array}{rrr|r} 1 & 1 & -10 & -4 \\ -1 & 0 & 7 & 5 \\ -3 & -5 & 36 & 10 \end{array}\right] \xrightarrow[3r_1 + r_3 \to r_3]{r_1 + r_2 \to r_2} \left[\begin{array}{rrr|r} 1 & 1 & -10 & -4 \\ 0 & 1 & -3 & 1 \\ 0 & -2 & 6 & -2 \end{array}\right]$$

$$\xrightarrow{2r_2 + r_3 \to r_3} \left[\begin{array}{rrr|r} 1 & 1 & -10 & -4 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

We have obtained the equivalent system of equations

$$\begin{cases} x + y - 10z = -4 \\ \phantom{x+{}} y - 3z = 1 \end{cases}$$

From the second equation we have

$$y = 3z + 1,$$

which, when substituted into the first equation, yields

$$x = 10z - y - 4 = 10z - (3z + 1) - 4 = 7z - 5.$$

That is, we have $x = 7z - 5$ and $y = 3z + 1$, and $z$ is free to assume any scalar value whatsoever.

Any ordered triple $[x, y, z]^\top$ that satisfies (2.29) must be of the form

$$[7z - 5, 3z + 1, z]^\top$$

for some $z \in \mathbb{F}$, and therefore the solution set is

$$S = \big\{[7z - 5, 3z + 1, z]^\top : z \in \mathbb{F}\big\}.$$

Since

$$\begin{bmatrix} 7z-5 \\ 3z+1 \\ z \end{bmatrix} = \begin{bmatrix} -5 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 7z \\ 3z \\ z \end{bmatrix} = \begin{bmatrix} -5 \\ 1 \\ 0 \end{bmatrix} + z\begin{bmatrix} 7 \\ 3 \\ 1 \end{bmatrix},$$

we may write

$$S = \left\{ \begin{bmatrix} -5 \\ 1 \\ 0 \end{bmatrix} + t\begin{bmatrix} 7 \\ 3 \\ 1 \end{bmatrix} \ : \ t \in \mathbb{F} \right\}.$$

■

The solution set $S$ in Example 2.37 is called a one-parameter solution set, meaning all elements of $S$ may be specified by designating a value in the field $\mathbb{F}$ for a single parameter (namely $z$). The solution set of the system in Example 2.36 is a zero-parameter solution set. In general an ***n*-parameter set** is a set $S$ whose elements are determined by the values of $n$ independent variables $x_1, \ldots, x_n$ called **parameters** . If the values of $x_1, \ldots, x_n$ derive from a set $I$ (sometimes called the **index set**), then $S$ has the form

$$S = \{f(x_1, \ldots, x_n) : x_i \in I \text{ for each } 1 \leq i \leq n\}.$$

Here $f$ is a function that pairs each $n$-tuple $(x_1, \ldots, x_n)$ with a single element of $S$.

## Problems

In Exercises 1–4 use Gaussian elimination to determine the solution set of the system of linear equations. Write all solution sets in terms of column vectors.

1. $$\begin{cases} x + 2y - z = 9 \\ 2x - z = -2 \\ 3x + 5y + 2z = 22 \end{cases}$$

2. $$\begin{cases} x - z = 1 \\ -2x + 3y - z = 0 \\ -6x + 6y = -2 \end{cases}$$

3. $$\begin{cases} x + z + w = 4 \\ y - z = -4 \\ x - 2y + 3z + w = 12 \\ 2x - 2z + 5w = -1 \end{cases}$$

4. $$\begin{cases} 3x - 6y - z + w = 7 \\ -x + 2y + 2z + 3w = 1 \\ 4x - 8y - 3z - 2w = 6 \end{cases}$$

5. Consider the system of equations
$$\begin{cases} 2x + y + z = 3 \\ x - y + 2z = 3 \\ x - 2y + \lambda z = 4 \end{cases}$$
Determine for which values of $\lambda$, if any, the system has:
(a) No solution.
(b) A unique solution, in which case give the solution.
(c) Infinitely many solutions, in which case give the solution.

6. Find conditions on the general vector $\mathbf{b}$ that would make the equation $\mathbf{A}\mathbf{x} = \mathbf{b}$ consistent, where
$$\mathbf{A} = \begin{bmatrix} 1 & 0 & -1 \\ -2 & 3 & -1 \\ 3 & -3 & 0 \\ 2 & 0 & -2 \end{bmatrix}.$$

## 2.6 – Homogeneous Systems

A system of linear equations in which all constant terms are equal to 0 is said to be **homogeneous**:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \quad\vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases} \tag{2.30}$$

If we define $\mathbf{A}$ and $\mathbf{x}$ as in (2.23), which is to say $\mathbf{A} = [a_{ij}]_{m,n}$ and $\mathbf{x} = [x_i]_{n,1}$, then we may write (2.30) as the matrix equation $\mathbf{Ax} = \mathbf{0}$. At a glance it is clear that setting

$$x_1 = \cdots = x_n = 0$$

will satisfy the system. This is called the **trivial solution**, and it may be represented as an $n$-tuple $(0, \ldots, 0)$, an $n \times 1$ zero vector $\mathbf{0}$, or some analogous construct.

**Theorem 2.38.** *Let* $\mathbf{A} = [a_{ij}]_{m,n}$ *and* $\mathbf{x} = [x_i]_{n,1}$. *If* $n > m$, *then the homogeneous system* $\mathbf{Ax} = \mathbf{0}$ *has a nontrivial solution.*

**Proof.** The theorem states that, for each $m \in \mathbb{N}$, the system (2.30) has a nontrivial solution whenever $n > m$. The proof will be accomplished using induction.

We consider the base case, when $m = 1$. For any $n > 1$ the "system" consists of a single equation

$$a_{11}x_1 + \cdots + a_{1n}x_n = 0. \tag{2.31}$$

Now, if $a_{1j} = 0$ for all $1 \leq j \leq n$, then *any* choice of scalars for $x_1, \ldots, x_n$ will satisfy this equation, and so in particular there exists a nontrivial solution. On the other hand if $a_{1k} \neq 0$ for some $1 \leq k \leq n$, then we may choose any scalar values for $x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n$, and set

$$x_k = -\frac{1}{a_{1k}} \sum_{j \neq k} a_{ij}x_j$$

so as to satisfy (2.31). Since there again exists a nontrivial solution, we see that the theorem is true in the case when $m = 1$.

Let $m \in \mathbb{N}$ be arbitrary and suppose that the theorem is true for this $m$ value. Consider the system

$$\begin{cases} a_{11}x_1 \quad + \quad a_{12}x_2 \quad + \cdots + \quad a_{1n}x_n \quad = 0 \\ \quad\vdots \qquad\qquad\quad \vdots \qquad\qquad\qquad\quad \vdots \qquad\quad \vdots \\ a_{m+1,1}x_1 + a_{m+1,2}x_2 + \cdots + a_{m+1,n}x_n = 0 \end{cases} \tag{2.32}$$

where $n > m + 1$. Assume that $a_{11} \neq 0$. If $[\,\mathbf{A} \,|\, \mathbf{0}\,]$ is the corresponding augmented matrix, then the sequence of elementary row operations

$$\mathbf{M}_{1,m+1}(-a_{m+1,1}/a_{11}) \cdots \mathbf{M}_{1,2}(-a_{21}/a_{11})[\,\mathbf{A} \,|\, \mathbf{0}\,]$$

will yield a new augmented matrix $[\,\mathbf{A}'\,|\,\mathbf{0}\,]$ that has zero entries under $a_{11}$ in the first column, which is to say we have attained an equivalent system of the form

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ \qquad\quad a'_{22}x_2 + \cdots + a'_{2n}x_n = 0 \\ \qquad\qquad \vdots \qquad\qquad\quad \vdots \qquad \vdots \\ \qquad a'_{m+1,2}x_2 + \cdots + a'_{m+1,n}x_n = 0 \end{cases} \tag{2.33}$$

Contained within this system is the system

$$\begin{cases} a'_{22}x_2 + \cdots + a'_{2n}x_n = 0 \\ \quad \vdots \qquad\qquad\quad \vdots \qquad \vdots \\ a'_{m+1,2}x_2 + \cdots + a'_{m+1,n}x_n = 0 \end{cases}$$

which has $m$ equations and $n$ variables, where $n > m$. By our inductive hypothesis this smaller system has a nontrivial solution $(\hat{x}_2, \ldots, \hat{x}_n)$, so that there is some $2 \le k \le n$ for which $\hat{x}_k \neq 0$. Now, if we let

$$\hat{x}_1 = -\frac{1}{a_{11}} \sum_{j=2}^{n} a_{1j}\hat{x}_j,$$

then $(\hat{x}_1, \ldots, \hat{x}_n)$ will satisfy all the equations in the system (2.33). Since (2.32) is equivalent to (2.33) it follows that $(\hat{x}_1, \ldots, \hat{x}_n)$ is a solution to (2.32), and moreover it is a nontrivial solution since $\hat{x}_k \neq 0$. We conclude that the theorem is true for $m+1$ at least when $a_{11} \neq 0$.

If $a_{11} = 0$ but there exists some $2 \le k \le n$ for which $a_{1k} \neq 0$, we relabel our variables thus: $y_1 = x_k$, $y_k = x_1$, and $y_j = x_j$ for $j \neq 1, k$. We thereby obtain a system of the form

$$\begin{cases} a_{1k}y_1 + a_{12}y_2 + \cdots + a_{11}y_k \cdots + a_{1n}y_n = 0 \\ \quad \vdots \qquad\qquad \vdots \qquad\qquad\quad \vdots \qquad\qquad \vdots \qquad \vdots \\ a_{m+1,k}y_1 + a_{m+1,2}y_2 + \cdots + a_{m+1,1}y_k \cdots + a_{m+1,n}y_n = 0 \end{cases} \tag{2.34}$$

From this, much like before, we obtain an equivalent system in which the variable $y_1$ has been eliminated from all equations save the first one. By our inductive hypothesis there exists a nontrivial solution $(\hat{y}_2, \ldots, \hat{y}_n)$ to the system consisting of the 2nd through $(m+1)$st equations of the equivalent system, whereupon setting

$$\hat{y}_1 = -\frac{1}{a_{1k}}(a_{12}\hat{y}_2 + \cdots + a_{11}\hat{y}_k + \cdots + a_{1n}\hat{y}_n)$$

gives an $n$-tuple $(\hat{y}_1, \ldots, \hat{y}_n)$ that is nontrivial and satisfies (2.34). It is then a routine matter to verify that $(\hat{x}_1, \ldots, \hat{x}_n)$ with $\hat{x}_1 = \hat{y}_k$, $\hat{x}_k = \hat{y}_1$, and $\hat{x}_j = \hat{y}_j$ for $j \neq 1, k$ is a nontrivial solution to (2.32).

If $a_{1j} = 0$ for all $1 \le j \le n$, then by our inductive hypothesis we may find a nontrivial solution to the other $m$ equations of (2.32), and this solution must necessarily satisfy the first equation.

We have now verified that the theorem is true for $m+1$ in all possible cases. By the Principle of Induction, therefore, the theorem is proven. ■

A system of equations $\mathbf{Ax} = \mathbf{b}$ for which $\mathbf{b} \neq \mathbf{0}$ is **nonhomogeneous**. The next example shows the first of many intimate connections between a nonhomogeneous system $\mathbf{Ax} = \mathbf{b}$ and the corresponding homogeneous system $\mathbf{Ax} = \mathbf{0}$ (i.e. the homogeneous system having the same coefficient matrix $\mathbf{A}$).

**Example 2.39.** Let $\mathbf{Ax} = \mathbf{b}$ be a nonhomogeneous system of equations, and let $\mathbf{x}'$ be a solution. Show that if $\mathbf{x}_0$ is a solution to the corresponding homogeneous system $\mathbf{Ax} = \mathbf{0}$, then $\mathbf{x}' + \mathbf{x}_0$ is another solution to $\mathbf{Ax} = \mathbf{b}$.

**Solution.** We have $\mathbf{Ax}' = \mathbf{b}$ and $\mathbf{Ax}_0 = \mathbf{0}$. Let $\mathbf{y} = \mathbf{x}' + \mathbf{x}_0$. We must show that $\mathbf{Ay} = \mathbf{b}$. But this is immediate:

$$\mathbf{Ay} = \mathbf{A}(\mathbf{x}' + \mathbf{x}_0) = \mathbf{Ax}' + \mathbf{Ax}_0 = \mathbf{b} + \mathbf{0} = \mathbf{b},$$

using the Distributive Law of matrix multiplication established in §2.2. ■

Given any nonempty $S \subseteq \mathbb{F}^n$ and nonzero $\mathbf{x} \in \mathbb{F}^n$, we define a new set

$$\mathbf{x} + S = \{\mathbf{x} + \mathbf{y} : \mathbf{y} \in S\}$$

called a **coset** of $S$. We now improve on Example 2.39 with the following more general result.

**Theorem 2.40.** *Let $\mathbf{Ax} = \mathbf{b}$ be a nonhomogeneous system of linear equations with solution set $S$, and let $S_h$ be the solution set of the corresponding homogeneous system $\mathbf{Ax} = \mathbf{0}$. If $\mathbf{x}_p$ is any particular solution to $\mathbf{Ax} = \mathbf{b}$, then $S = \mathbf{x}_p + S_h$.*

**Proof.** Suppose that $\mathbf{x}_p$ is a particular solution to $\mathbf{Ax} = \mathbf{b}$. Let $\mathbf{x}' \in S$ be arbitrary. Then

$$\mathbf{A}(\mathbf{x}' - \mathbf{x}_p) = \mathbf{Ax}' - \mathbf{Ax}_p = \mathbf{b} - \mathbf{b} = \mathbf{0}$$

shows that $\mathbf{x}' - \mathbf{x}_p$ is a solution to $\mathbf{Ax} = \mathbf{0}$ and hence $\mathbf{x}' - \mathbf{x}_P \in S_h$. Since

$$\mathbf{x}' = \mathbf{x}_p + (\mathbf{x}' - \mathbf{x}_p) \in \{\mathbf{x}_p + \mathbf{x}_h : \mathbf{x}_h \in S_h\} = \mathbf{x}_p + S_h,$$

we conclude that $S \subseteq \mathbf{x}_p + S_h$.

Next, suppose that $\mathbf{x}' \in \mathbf{x}_p + S_h$, so $\mathbf{x}' = \mathbf{x}_p + \mathbf{x}_h$ for some $\mathbf{x}_h \in S_h$. Since

$$\mathbf{Ax}' = \mathbf{A}(\mathbf{x}_p + \mathbf{x}_h) = \mathbf{Ax}_p + \mathbf{Ax}_h = \mathbf{b} + \mathbf{0} = \mathbf{b},$$

we conclude that $\mathbf{x}' \in S$ and hence $\mathbf{x}_p + S_h \subseteq S$.

Therefore $S = \mathbf{x}_p + S_h$. ■

To fully determine the solution set of any nonhomogeneous system $\mathbf{Ax} = \mathbf{b}$, according to Theorem 2.40 it suffices to find just one solution to $\mathbf{Ax} = \mathbf{b}$ (called a **particular solution**) along with the complete solution set of $\mathbf{Ax} = \mathbf{0}$.

We close this chapter with a final result that will later become bound up in the Inverse Matrix Theorem, which is a theorem that will bring together over a dozen seemingly disparate statements that all turn out to be equivalent.

**Proposition 2.41.** *If $\mathbf{A} \in \mathbb{F}^{n\times n}$ is invertible, then the homogeneous system $\mathbf{Ax} = \mathbf{0}$ has only the trivial solution.*

**Proof.** Suppose $\mathbf{A} \in \mathbb{F}^{n\times n}$ is invertible. Clearly $\mathbf{0}$ is a solution to $\mathbf{A}\mathbf{x} = \mathbf{0}$, and it only remains to show it is a unique solution. Suppose that $\mathbf{x}_0$ is a solution to the system, so that $\mathbf{A}\mathbf{x}_0 = \mathbf{0}$. Since $\mathbf{A}^{-1}$ exists, we have

$$\mathbf{A}\mathbf{x}_0 = \mathbf{0} \;\Rightarrow\; \mathbf{A}^{-1}(\mathbf{A}\mathbf{x}_0) = \mathbf{A}^{-1}\mathbf{0} \;\Rightarrow\; (\mathbf{A}^{-1}\mathbf{A})\mathbf{x}_0 = \mathbf{0} \;\Rightarrow\; \mathbf{I}_n\mathbf{x}_0 = \mathbf{0} \;\Rightarrow\; \mathbf{x}_0 = \mathbf{0}.$$

Thus any $\mathbf{x}_0$ given to be a solution to the system must in fact be $\mathbf{0}$, proving uniqueness. ■

# 3

# Vector Spaces

## 3.1 – The Vector Space Axioms

Let $\mathbb{F}$ be a field. In practice $\mathbb{F}$ is usually either the real number system $\mathbb{R}$ or the complex number system $\mathbb{C}$, but in any case it is a set of objects that obey the field axioms given in §1.1.

**Definition 3.1.** *A* ***vector space*** *over* $\mathbb{F}$ *is a set* $V$ *of objects, along with operations* ***vector addition*** $V \times V \to V$ *(denoted by* $+$*) and* ***scalar multiplication*** $\mathbb{F} \times V \to V$ *(denoted by* $\cdot$ *or juxtaposition) subject to the following axioms:*

VS1. $\mathbf{u}+\mathbf{v}=\mathbf{v}+\mathbf{u}$ *for any* $\mathbf{u},\mathbf{v}\in V$
VS2. $\mathbf{u}+(\mathbf{v}+\mathbf{w})=(\mathbf{u}+\mathbf{v})+\mathbf{w}$ *for any* $\mathbf{u},\mathbf{v},\mathbf{w}\in V$
VS3. *There exists some* $\mathbf{0}\in V$ *such that* $\mathbf{u}+\mathbf{0}=\mathbf{u}$ *for any* $\mathbf{u}\in V$
VS4. *For each* $\mathbf{u}\in V$ *there exists some* $-\mathbf{u}\in V$ *such that* $\mathbf{u}+(-\mathbf{u})=\mathbf{0}$
VS5. *For any* $a\in\mathbb{F}$ *and* $\mathbf{u},\mathbf{v}\in V$*,* $a(\mathbf{u}+\mathbf{v})=a\mathbf{u}+a\mathbf{v}$
VS6. *For any* $a,b\in\mathbb{F}$ *and* $\mathbf{u}\in V$*,* $(a+b)\mathbf{u}=a\mathbf{u}+b\mathbf{u}$
VS7. *For any* $a,b\in\mathbb{F}$ *and* $\mathbf{u}\in V$*,* $a(b\mathbf{u})=(ab)\mathbf{u}$
VS8. *For all* $\mathbf{u}\in V$*,* $1\mathbf{u}=\mathbf{u}$

*The elements of* $V$ *are called* ***vectors*** *and the elements of the underlying field* $\mathbb{F}$ *are called* ***scalars****.*

A **real vector space** is a vector space over $\mathbb{R}$, and a **complex vector space** is a vector space over $\mathbb{C}$. A **Euclidean *n*-space over** $\mathbb{F}$ is specifically a vector space consisting of $n$-tuples $[x_1,\dots,x_n]$, where $x_k\in\mathbb{F}$ for all $1\le k\le n$. In general a **Euclidean space** is any Euclidean $n$-space over $\mathbb{F}$ for some unspecified $n\in\mathbb{N}$ and field $\mathbb{F}$. If $\mathbb{F}=\mathbb{R}$, we obtain a **real Euclidean space**; and if $\mathbb{F}=\mathbb{C}$, we obtain a **complex Euclidean space**.

The object $\mathbf{0}$ mentioned in Axiom VS3 is called the **zero vector**, and the vector $-\mathbf{u}$ mentioned in Axiom VS4 is the **additive inverse** of $\mathbf{u}$.

We have in the statement of the definition that $+:V\times V\to V$. That is, the vector addition operation $+$ takes any ordered pair $(\mathbf{u},\mathbf{v})\in V\times V$ and returns an object $\mathbf{u}+\mathbf{v}\in V$. Thus $\mathbf{u}+\mathbf{v}$ *must* be an object that belong to the set $V$! Similarly the scalar multiplication operation is given to be a map $\cdot:\mathbb{F}\times V\to V$, which means scalar multiplication takes any ordered pair $(a,\mathbf{u})\in\mathbb{F}\times V$ and returns an object $a\cdot\mathbf{u}=a\mathbf{u}\in V$. Thus $a\mathbf{u}$ must also belong to $V$! Some books state these facets of the definition of a vector space as two additional axioms:

$$\mathbf{u} + \mathbf{v} \in V \text{ for any } \mathbf{u}, \mathbf{v} \in V \tag{3.1}$$

and

$$a\mathbf{u} \in V \text{ for any } a \in \mathbb{F} \text{ and } \mathbf{u} \in V. \tag{3.2}$$

We call (3.1) the **closure property of scalar multiplication**, and (3.2) the **closure property of addition**. When property (3.1) holds for a set $V$, we say that $V$ is **closed under addition**; and when property (3.2) holds we say $V$ is **closed under scalar multiplication**.

**Remark.** A set $V$ together with given operations $+$ and $\cdot$ defined on $V \times V$ and $\mathbb{F} \times V$, respectively, is a vector space if and only if the eight axioms VS1–VS8 and the two closure properties (3.1) and (3.2) are all satisfied!

Some seemingly "obvious" results actually require careful reasoning to prove their validity in the context of vector spaces, as the next two propositions show.

**Proposition 3.2.** *Let $V$ be a vector space, $\mathbf{u} \in V$, and $a \in \mathbb{F}$. Then the following properties hold.*

1. $0\mathbf{u} = \mathbf{0}$
2. $a\mathbf{0} = \mathbf{0}$
3. *If $a\mathbf{u} = \mathbf{0}$, then $a = 0$ or $\mathbf{u} = \mathbf{0}$*

**Proof.**

*Proof of Part (1).* Since $\mathbf{u} \in V$ and $0 \in \mathbb{F}$, we have $0\mathbf{u} \in V$ by the closure property (3.2). Now,

$$\begin{aligned}
0\mathbf{u} &= 0\mathbf{u} + \mathbf{0} && \text{Axiom VS3} \\
&= 0\mathbf{u} + [\mathbf{u} + (-\mathbf{u})] && \text{Axiom VS4} \\
&= (0\mathbf{u} + \mathbf{u}) + (-\mathbf{u}) && \text{Axiom VS2} \\
&= (0\mathbf{u} + 1\mathbf{u}) + (-\mathbf{u}) && \text{Axiom VS8} \\
&= (0 + 1)\mathbf{u} + (-\mathbf{u}) && \text{Axiom VS6} \\
&= 1\mathbf{u} + (-\mathbf{u}) && \text{Axiom F3} \\
&= \mathbf{u} + (-\mathbf{u}) && \text{Axiom VS8} \\
&= \mathbf{0}. && \text{Axiom VS4}
\end{aligned}$$

The proofs of parts (2) and (3) are left to the exercises. ■

**Proposition 3.3.** *If $V$ is a vector space and $\mathbf{u} \in V$, then $(-1)\mathbf{u} = -\mathbf{u}$.*

**Proof.** Suppose that $V$ is a vector space and $\mathbf{u} \in V$. Then $(-1)\mathbf{u} \in V$, and

$$\begin{aligned}
(-1)\mathbf{u} &= (-1)\mathbf{u} + \mathbf{0} && \text{Axiom VS3} \\
&= (-1)\mathbf{u} + [\mathbf{u} + (-\mathbf{u})] && \text{Axiom VS4} \\
&= [(-1)\mathbf{u} + \mathbf{u}] + (-\mathbf{u}) && \text{Axiom VS2} \\
&= [(-1)\mathbf{u} + 1\mathbf{u}] + (-\mathbf{u}) && \text{Axiom VS8}
\end{aligned}$$

| | |
|---|---|
| $= (-1+1)\mathbf{u} + (-\mathbf{u})$ | Axiom VS6 |
| $= 0\mathbf{u} + (-\mathbf{u})$ | Axiom F4 |
| $= \mathbf{0} + (-\mathbf{u}),$ | Proposition 3.2(1) |
| $= -\mathbf{u}.$ | Axiom VS3 |

■

As with Euclidean vectors we define **vector subtraction** by

$$\mathbf{u} - \mathbf{v} = \mathbf{u} + (-\mathbf{v})$$

for any $\mathbf{u}, \mathbf{v} \in V$.

The objects belonging to a vector space are invariably called vectors, but they could be any kind of mathematical entity either concrete or abstract. They often are the Euclidean vectors encountered in Chapter 1, but they could also be matrices, polynomials, functions, or other objects. This is part of the power of linear algebra.

**Example 3.4.** The set of coordinate vectors

$$\mathbb{R}^n = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \middle| \; x_1, \ldots, x_n \in \mathbb{R} \right\},$$

together with the definitions of vector addition and real scalar multiplication as given in §1.2, is easily verified to be a vector space over $\mathbb{R}$. Similarly, the set of coordinate vectors

$$\mathbb{C}^n = \left\{ \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \middle| \; z_1, \ldots, z_n \in \mathbb{C} \right\},$$

with vector addition and complex scalar multiplication defined in analogous fashion to $\mathbb{R}^n$, is a vector space over $\mathbb{C}$. Important: the underlying fields of $\mathbb{R}^n$ and $\mathbb{C}^n$ are always taken to be $\mathbb{R}$ and $\mathbb{C}$, respectively, unless otherwise specified! ■

**Example 3.5.** The set $\mathbb{F}^{m\times n}$ of all $m \times n$ matrices with entries in $\mathbb{F}$ is a vector space under the standard operations of matrix addition and scalar multiplication given by Definition 2.1. In particular the set $\mathbb{R}^{m\times n}$ of $m \times n$ matrices with real-valued entries is a real vector space, and the set $\mathbb{C}^{m\times n}$ of $m \times n$ matrices with complex-valued entries is a complex vector space. ■

**Example 3.6.** Given an integer $n \geq 0$, let $\mathcal{P}_n(\mathbb{F})$ be the set of all polynomials of a single variable $x$ with coefficients in $\mathbb{F}$ and degree at most $n$; that is,

$$\mathcal{P}_n(\mathbb{F}) = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n : a_i \in \mathbb{F} \text{ for } 0 \leq i \leq n\}.$$

By definition the polynomial 0 has degree $-\infty$, and so $0 \in \mathcal{P}_n(\mathbb{F})$ in particular. We have

$$\mathcal{P}_0(\mathbb{R}) = \{a : a \in \mathbb{R}\} = \mathbb{R},$$

$$\mathcal{P}_1(\mathbb{R}) = \{a + bx : a, b \in \mathbb{R}\},$$

$$\mathcal{P}_2(\mathbb{R}) = \{a + bx + cx^2 : a, b, c \in \mathbb{R}\}.$$

If we define polynomial addition and scalar multiplication in the customary fashion by

$$(a_0 + a_1x + \cdots + a_nx^n) + (b_0 + b_1x + \cdots + b_nx^n)$$
$$= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n,$$

and

$$c\,(a_0 + a_1x + \cdots + a_nx^n) = ca_0 + ca_1x + \cdots + ca_nx^n,$$

then it is straightforward to verify that $\mathcal{P}_n(\mathbb{F})$ is a vector space. ■

**Example 3.7.** Let $S \subseteq \mathbb{F}$, where as usual $\mathbb{F}$ is some field. Let $\mathcal{F}(S, \mathbb{F})$ denote the set of all functions $S \to \mathbb{F}$. Given $f \in \mathcal{F}(S, \mathbb{F})$ and $c \in \mathbb{F}$, we define scalar multiplication of $c$ with $f$ as yielding a new function $cf \in \mathcal{F}(S, \mathbb{F})$ given by

$$(cf)(x) = cf(x)$$

for all $x \in S$. If $f, g \in \mathcal{F}(S, \mathbb{F})$, we define addition of $f$ with $g$ as yielding a new function $f + g \in \mathcal{F}(S, \mathbb{F})$ given by

$$(f + g)(x) = f(x) + g(x)$$

for all $x \in S$. These operations are consonant with conventions established in elementary algebra, and it is straightforward to verify that $\mathcal{F}(S, \mathbb{F})$ is in fact a vector space. The zero vector is the function 0 given by $0(x) = 0$ for all $x \in S$. The additive inverse of any $f \in \mathcal{F}(S, \mathbb{F})$ is the function $-f$ given by $(-f)(x) = -f(x)$, since

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) + (-f(x)) = 0 = 0(x)$$

for all $x \in S$, and hence $f + (-f) = 0$.

If a set $S$ is not specified at the outset of an analysis involving functions $f_1, f_2, \ldots, f_n$, then we take

$$S = \bigcap_{i=1}^{n} \mathrm{Dom}(f_i) = \mathrm{Dom}(f_1) \cap \mathrm{Dom}(f_2) \cap \cdots \cap \mathrm{Dom}(f_n)$$

and carry out the analysis in the vector space $\mathcal{F}(S, \mathbb{F})$ provided that $S \neq \varnothing$. ■

**Example 3.8.** Show that the collection of functions[4]

$$\mathcal{C} = \{f : \mathbb{R} \to \mathbb{R} \mid f(2) = 0\}$$

is a vector space over $\mathbb{R}$ under the usual operations of function addition and scalar multiplication (see Example 3.7).

**Solution.** First, it's worth noting that since $\mathcal{F}(\mathbb{R}, \mathbb{R})$ is the set of all real-valued functions with domain $\mathbb{R}$, we have $\mathcal{C} \subseteq \mathcal{F}(\mathbb{R}, \mathbb{R})$.

Let $f, g, h \in \mathcal{C}$ and $a, b \in \mathbb{R}$. Let $x \in \mathbb{R}$ be arbitrary. We have $f + g \in \mathcal{C}$ and $af \in \mathcal{C}$ since

$$(f + g)(2) = f(2) + g(2) = 0 + 0 = 0 \quad \text{and} \quad (af)(2) = af(2) = a(0) = 0,$$

[4]Sets of functions (as well as sets of sets) are often referred to as "collections" or "families" in the mathematical literature.

and so there is closure under addition and scalar multiplication. In what follows we make frequent use of the field axioms of the real number system (see §1.1).

By the Commutative Property of Addition we have

$$(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x),$$

so that $f + g = g + f$. Axiom VS1 holds.

We have

$$f(x) + [g(x) + h(x)] = [f(x) + g(x)] + h(x)$$

by the Associative Property of Addition, and thus $f + (g + h) = (f + g) + h$. Axiom VS2 holds.

Let $o$ be the zero function. That is, $o(x) = 0$ for all $x \in \mathbb{R}$. Since $o(2) = 0$ we see that $o \in \mathcal{C}$. Now,

$$(o + f)(x) = o(x) + f(x) = 0 + f(x) = f(x)$$

and

$$(f + o)(x) = f(x) + o(x) = f(x) + 0 = f(x),$$

and so $o + f = f + o = f$. Axiom VS3 holds.

As usual $-f$ is the function given by $(-f)(x) = -f(x)$, so in particular $(-f)(2) = -f(2) = 0$ implies that $-f \in \mathcal{C}$. Now,

$$(-f + f)(x) = (-f)(x) + f(x) = -f(x) + f(x) = 0 = o(x)$$

shows that $-f + f = o$. Similarly $f + (-f) = o$. Axiom VS4 holds.

By the Distributive Property,

$$\begin{aligned}\big(a(f+g)\big)(x) &= a(f+g)(x) = a[f(x) + g(x)] = af(x) + ag(x)\\ &= (af)(x) + (ag)(x) = (af + ag)(x),\end{aligned}$$

which shows that $a(f + g) = af + ag$. Axiom VS5 holds.

Again by the Distributive Property,

$$\big((a+b)f\big)(x) = (a+b)f(x) = af(x) + bf(x) = (af)(x) + (bf)(x) = (af + bf)(x),$$

so $(a + b)f = af + bf$. Axiom VS6 holds.

By the Associative Property of Multiplication,

$$\big(a(bf)\big)(x) = a(bf)(x) = a(bf(x)) = (ab)f(x) = \big((ab)f\big)(x),$$

so $a(bf) = (ab)f$. Axiom VS7 holds.

Finally, since $1 \in \mathbb{R}$ is the multiplicative identity, we have $(1f)(x) = 1f(x) = f(x)$. This shows that $1f = f$, and Axiom VS8 holds. ∎

## Problems

In Exercises 1–4 a set of objects $V$ is given, along with definitions for operations of vector addition and scalar multiplication. Determine whether or not $V$ is a vector space under the given operations. If it is not, indicate which axioms and closure properties fail to hold.

1. $V = \mathbb{R}^2$, with vector addition and scalar multiplication defined by
$$\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} u_1 + v_1 \\ u_2 + v_2 \end{bmatrix} \quad \text{and} \quad c\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} 9cu_1 \\ 9cu_2 \end{bmatrix}.$$

2. $V = \mathbb{R}^2$, with vector addition and scalar multiplication defined by
$$\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} u_1 + v_1 + 3 \\ u_2 + v_2 + 3 \end{bmatrix} \quad \text{and} \quad c\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} cu_1 \\ cu_2 \end{bmatrix}.$$

3. $V$ is the set of $2 \times 2$ matrices of the form
$$\begin{bmatrix} a & 0 \\ 1 & b \end{bmatrix}$$
with the standard operations of matrix addition and scalar multiplication.

4. $V$ is the set of real-valued one-to-one functions with domain $(-\infty, \infty)$, together with the zero function $x \mapsto 0$. For any $f, g \in V$ and $c \in \mathbb{R}$, the sum $f + g$ and scalar product $cf$ are defined in the standard way.

5. Prove part (2) of Proposition 3.2.

6. Prove part (3) of Proposition 3.2.

## 3.2 – Subspaces

**Definition 3.9.** *Let $V$ be a vector space. If $W \subseteq V$ is a vector space under the vector addition and scalar multiplication operations defined on $V \times V$ and $\mathbb{F} \times V$, respectively, then $W$ is a **subspace** of $V$.*

In order for $W \subseteq V$ to be a vector space it must satisfy the statement of Definition 3.1 *to the letter*, except that the symbol $W$ is substituted for $V$. Straightaway this means we must have $W \neq \varnothing$ since Axiom VS3 requires that $\mathbf{0} \in W$. Moreover, vector addition must map $W \times W \to W$ and scalar multiplication must map $\mathbb{F} \times W \to W$, which is to say for any $\mathbf{u}, \mathbf{v} \in W$ and $a \in \mathbb{F}$ we must have $\mathbf{u} + \mathbf{v} \in W$ and $a\mathbf{u} \in W$. These observations prove the forward implication in the following theorem.

**Theorem 3.10.** *Let $V$ be a vector space and $\varnothing \neq W \subseteq V$. Then $W$ is a subspace of $V$ if and only if $a\mathbf{u} \in W$ and $\mathbf{u} + \mathbf{v} \in W$ for all $a \in \mathbb{F}$ and $\mathbf{u}, \mathbf{v} \in W$.*

**Proof.** We need only prove the reverse implication. So, suppose that for any $a \in \mathbb{F}$ and $\mathbf{u}, \mathbf{v} \in W$, it is true that $a\mathbf{u} \in W$ and $\mathbf{u} + \mathbf{v} \in W$. Then vector addition maps $W \times W \to W$ and scalar multiplication maps $\mathbb{F} \times W \to W$, and it remains to confirm that $W$ satisfies the eight axioms in Definition 3.1. But it is clear that Axioms VS1, VS2, VS5, VS6, VS7, and VS8 must hold. For instance if $\mathbf{u}, \mathbf{v} \in W$, then $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ since $\mathbf{u}, \mathbf{v} \in V$ and $V$ is given to be a vector space, and so Axiom VS1 is confirmed.

Let $\mathbf{u} \in W$. Since $a\mathbf{u} \in W$ for any $a \in \mathbb{F}$, it follows that $(-1)\mathbf{u} \in W$ in particular. Now, $(-1)\mathbf{u} = -\mathbf{u}$ by Proposition 3.3, and so $-\mathbf{u} \in W$. That is, for every $\mathbf{u} \in W$ we find that $-\mathbf{u} \in W$ as well, where $\mathbf{u} + (-\mathbf{u}) = -\mathbf{u} + \mathbf{u} = \mathbf{0}$. This shows that Axiom VS4 holds for $W$.

Finally, since $a\mathbf{u} \in W$ for any $a \in \mathbb{F}$, it follows that $0\mathbf{u} \in W$. By Proposition 3.2 we have $0\mathbf{u} = \mathbf{0}$, so $\mathbf{0} \in W$ and Axiom VS3 holds for $W$.

We conclude that $W \subseteq V$ is a vector space under the vector addition and scalar multiplication operations defined on $V \times V$ and $\mathbb{F} \times V$, respectively. Therefore $W$ is a subspace of $V$ by Definition 3.9. ■

The following result is immediate, and provides a checklist that commonly is employed to quickly determine whether a subset of a vector space is a subspace.

**Corollary 3.11.** *Let $V$ be a vector space, and let $W \subseteq V$. Then $W$ is a subspace of $V$ if the following conditions hold:*

1. $\mathbf{0} \in W$.
2. $a\mathbf{u} \in W$ *for all* $\mathbf{u} \in W$ *and* $a \in \mathbb{F}$.
3. $\mathbf{u} + \mathbf{v} \in W$ *for all* $\mathbf{u}, \mathbf{v} \in W$.

In practice, to determine whether any given subset of a vector space $V$ is a subspace the first thing one usually checks is whether or not it contains the zero vector $\mathbf{0}$. If $W \subseteq V$ does not contain $\mathbf{0}$, then it is not a subspace.

**Example 3.12.** Consider the set

$$U = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3 \,:\, xyz = 0 \right\}.$$

Certainly $U$ is a subset of $\mathbb{R}^3$, but is it a subspace of $\mathbb{R}^3$? Two vectors belonging to $U$ are

$$\mathbf{u}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad \text{and} \quad \mathbf{u}_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix},$$

since $(1)(0)(0) = 0$ and $(0)(1)(1) = 0$. However, the vector

$$\mathbf{u}_1 + \mathbf{u}_2 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

does not belong to $U$ since $(1)(1)(1) \neq 0$. Since $U$ is not closed under vector addition, it is not a subspace of $\mathbb{R}^3$. ■

**Example 3.13.** Consider the set $\text{Skw}_n(\mathbb{R})$ of $n \times n$ skew-symmetric matrices with entries in $\mathbb{R}$:

$$\text{Skw}_n(\mathbb{R}) = \{\mathbf{A} \in \mathbb{R}^{n\times n} : \mathbf{A}^\top = -\mathbf{A}\}.$$

Clearly $\text{Skw}_n(\mathbb{R})$ is a subset of the vector space $\mathbb{R}^{n\times n}$, and since $\mathbf{O}_n^\top = -\mathbf{O}_n$ we see that $\text{Skw}_n(\mathbb{R})$ contains the "zero vector" of $\mathbb{R}^{n\times n}$. Let $\mathbf{A}, \mathbf{B} \in \text{Skw}_n(\mathbb{R})$ and $c \in \mathbb{R}$. By Proposition 2.3,

$$(c\mathbf{A})^\top = c\mathbf{A}^\top = c(-\mathbf{A}) = -(c\mathbf{A})$$

and

$$(\mathbf{A}+\mathbf{B})^\top = \mathbf{A}^\top + \mathbf{B}^\top = -\mathbf{A} + (-\mathbf{B}) = -(\mathbf{A}+\mathbf{B}),$$

which shows that $c\mathbf{A} \in \text{Skw}_n(\mathbb{R})$ and $\mathbf{A}+\mathbf{B} \in \text{Skw}_n(\mathbb{R})$. Therefore $\text{Skw}_n(\mathbb{R})$ is a subspace by Corollary 3.11. ■

**Example 3.14.** As we saw in §2.5, a system of $m$ linear equations in $n$ unknowns

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \quad \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad\; \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{3.3}$$

may be written as a matrix equation $\mathbf{Ax} = \mathbf{b}$, where

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \quad \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \quad \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}. \tag{3.4}$$

Here each vector $\mathbf{x}$ in $\mathbb{F}^n$ is represented by a column matrix as in (3.4), so that

$$\mathbb{F}^n = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \,\middle|\, x_1, \ldots, x_n \in \mathbb{F} \right\}.$$

As previously established, a vector

$$\mathbf{s} = \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}$$

is a **solution** to $\mathbf{Ax} = \mathbf{b}$ if and only if substituting $\mathbf{s}$ for $\mathbf{x}$ in $\mathbf{Ax} = \mathbf{b}$ makes the equation true, and this will be the case if and only if the $n$-tuple $(s_1, \ldots, s_n)$ is a solution to the system of equations (3.3).

Now, if we set $\mathbf{b} = \mathbf{0}$, we obtain the matrix equation $\mathbf{Ax} = \mathbf{0}$ representing the *homogeneous* system in which the right-hand side of every equation in (3.3) is 0. The solution set for $\mathbf{Ax} = \mathbf{0}$ is the set

$$S = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{Ax} = \mathbf{0}\},$$

so clearly $S \subseteq \mathbb{F}^n$. But is $S$ a *subspace* of $\mathbb{F}^n$? Certainly $\mathbf{A0} = \mathbf{0}$ is true, so $\mathbf{0} \in S$ and $S \neq \varnothing$. To determine definitively whether $S$ is a subspace we use Corollary 3.11.

Let $\mathbf{s} \in S$ and $a \in \mathbb{F}$. Since $\mathbf{s}$ is in $S$ we have $\mathbf{As} = \mathbf{0}$, and then

$$\mathbf{A}(a\mathbf{s}) = a(\mathbf{As}) = a\mathbf{0} = \mathbf{0}$$

shows that $a\mathbf{s} \in S$. Next, if $\mathbf{s}, \mathbf{s}' \in S$, so that $\mathbf{As} = \mathbf{0}$ and $\mathbf{As}' = \mathbf{0}$ both hold, then

$$\mathbf{A}(\mathbf{s} + \mathbf{s}') = \mathbf{As} + \mathbf{As}' = \mathbf{0} + \mathbf{0} = \mathbf{0}$$

shows that $\mathbf{s} + \mathbf{s}' \in S$ also.

Therefore $S$ is a subspace of $\mathbb{F}^n$ by Corollary 3.11. We call $S$ the **solution space** of the system $\mathbf{Ax} = \mathbf{0}$. ■

**Definition 3.15.** *The* ***null space*** *of* $\mathbf{A} \in \mathbb{F}^{m\times n}$ *is the set*

$$\text{Nul}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{Ax} = \mathbf{0}\}.$$

**Proposition 3.16.** *If* $\mathbf{A} \in \mathbb{F}^{m\times n}$*, then* $\text{Nul}(\mathbf{A})$ *is a subspace of* $\mathbb{F}^n$*.*

**Proof.** This follows easily from the proceedings of Example 3.14 since the null space of a matrix $\mathbf{A}$ corresponds to the solution space of the homogeneous system of linear equations $\mathbf{Ax} = \mathbf{0}$. ■

**Definition 3.17.** *Let* $V$ *be a subspace of* $\mathbb{R}^n$*. The* ***orthogonal complement*** *of* $V$ *is the set*

$$V^\perp = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{v} \in V\}.$$

**Proposition 3.18.** *If* $V$ *is a subspace of* $\mathbb{R}^n$*, then* $V^\perp$ *is also a subspace of* $\mathbb{R}^n$*.*

**Proof.** Let $V$ be a subspace of $\mathbb{R}^n$. Suppose $\mathbf{x}, \mathbf{y} \in V^\perp$. Then for any $\mathbf{v} \in V$ we have

$$(\mathbf{x}+\mathbf{y}) \cdot \mathbf{v} = \mathbf{x} \cdot \mathbf{v} + \mathbf{y} \cdot \mathbf{v} = 0 + 0 = 0,$$

which shows that $\mathbf{x}+\mathbf{y} \in V^\perp$. Moreover, for any $c \in \mathbb{R}$ we have

$$(c\mathbf{x}) \cdot \mathbf{v} = c(\mathbf{x} \cdot \mathbf{v}) = c(0) = 0$$

for any $\mathbf{v} \in V$, which shows that $c\mathbf{x} \in V^\perp$. Since $V^\perp \subseteq \mathbb{R}^n$ is closed under scalar multiplication and vector addition, we conclude that it is a subspace of $\mathbb{R}^n$. ■

## Problems

1. Determine whether the set
$$W = \left\{ [x, y, z]^\top : y = 2x - z \right\}$$
is a subspace of $\mathbb{R}^3$. If it is, prove it; otherwise show how it fails to be a subspace.

2. Prove or disprove that the set is a subspace of the vector space $\mathbb{R}^{2\times 2}$ of all $2 \times 2$ matrices with real entries.
   (a) $\left\{ \mathbf{A} \in \mathbb{R}^{2\times 2} : \mathbf{A}^\top = \mathbf{A} \right\}$
   (b) $\left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\}$
   (c) $\left\{ \begin{bmatrix} a & 0 \\ 0 & a^2 \end{bmatrix} : a \in \mathbb{R} \right\}$
   (d) $\left\{ \begin{bmatrix} a^2 & 0 \\ 0 & b^2 \end{bmatrix} : a, b \in \mathbb{R} \right\}$

3. Determine whether $\mathrm{Sym}_n(\mathbb{R})$, the set of $n \times n$ symmetric matrices with real entries, is a subspace of $\mathbb{R}^{n\times n}$. If it is, prove it; otherwise show how it fails to be a subspace.

4. Prove or disprove that the set is a subspace of the vector space $\mathcal{F}(\mathbb{R}, \mathbb{R})$ of all real-valued functions $f$ with domain $\mathbb{R}$.
   (a) $\{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f(x) \leq 0 \text{ for all } x \in \mathbb{R}\}$
   (b) $\{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f(0) = 0\}$
   (c) $\{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f(0) = 9\}$
   (d) $\{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f \text{ is a constant function}\}$
   (e) $\{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) : f(x) = a\cos x + b\sin x \text{ for some } a, b \in \mathbb{R}\}$

## 3.3 – Subspace Sums and Direct Sums

**Definition 3.19.** *Let $U$ and $W$ be subspaces of a vector space $V$. The* ***sum*** *of $U$ and $W$ is the set of vectors*

$$U + W = \{\mathbf{v} \in V : \mathbf{v} = \mathbf{u} + \mathbf{w} \text{ for some } \mathbf{u} \in U \text{ and } \mathbf{w} \in W\}.$$

*More generally, if $U_1, \dots, U_n$ are subspaces of $V$, then the* ***sum*** *of $U_1, \dots, U_n$ is the set of vectors*

$$\sum_{k=1}^{n} U_k = \left\{ \mathbf{v} \in V : \mathbf{v} = \sum_{k=1}^{n} \mathbf{u}_k \text{ for some } \mathbf{u}_k \in U_k \right\}.$$

Equivalently we may write

$$U + W = \{\mathbf{u} + \mathbf{w} : \mathbf{u} \in U \text{ and } \mathbf{w} \in W\}$$

for subspaces $U$ and $W$ of $V$, and

$$\sum_{k=1}^{n} U_k = \left\{ \sum_{k=1}^{n} \mathbf{u}_k : \mathbf{u}_k \in U_k \right\}$$

for subspaces $U_1, \dots, U_k$ of $V$.

**Proposition 3.20.** *If $U_1, \dots, U_n$ are subspaces of a vector space $V$ over $\mathbb{F}$, then $U_1 + \cdots + U_n$ is also a subspace of $V$.*

**Proof.** Suppose $U_1, \dots, U_n$ are subspaces of a vector space $V$, and let $U = U_1 + \cdots + U_n$. Clearly $\mathbf{0} \in U$, so $U \neq \varnothing$. Let $\mathbf{u}, \mathbf{v} \in U$, so that

$$\mathbf{u} = \sum_{k=1}^{n} \mathbf{u}_k \quad \text{and} \quad \mathbf{v} = \sum_{k=1}^{n} \mathbf{v}_k$$

for vectors $\mathbf{u}_k, \mathbf{v}_k \in U_k$, $1 \leq k \leq n$. Now, $\mathbf{u}_k + \mathbf{v}_k \in U_k$ since each $U_k$ is closed under vector addition, and hence

$$\mathbf{u} + \mathbf{v} = \sum_{k=1}^{n} (\mathbf{u}_k + \mathbf{v}_k) \in \sum_{k=1}^{n} U_k = U$$

and we conclude that $U$ is closed under vector addition. Also, for any $c \in \mathbb{F}$ we have $c\mathbf{u}_k \in U_k$ since each $U_k$ is closed under scalar multiplication, and hence

$$c\mathbf{u} = \sum_{k=1}^{n} c\mathbf{u}_k \in \sum_{k=1}^{n} U_k = U$$

and we conclude that $U$ is closed under scalar multiplication. Therefore $U$ is a subspace of $V$ by Corollary 3.11. ■

**Definition 3.21.** *Let $U$ and $W$ be subspaces of a vector space $V$. We say $V$ is the* ***direct sum*** *of $U$ and $W$, written $V = U \oplus W$, if $V = U + W$ and $U \cap W = \{\mathbf{0}\}$.*

*More generally, let $U_1, \ldots, U_n$ be subspaces of $V$. Then $V$ is the* ***direct sum*** *of $U_1, \ldots, U_n$, written*

$$V = \bigoplus_{k=1}^{n} U_k,$$

*if $V = \sum_{k=1}^{n} U_k$ and*

$$U_i \cap \sum_{k \neq i} U_k = \{\mathbf{0}\} \tag{3.5}$$

*for each $i = 1, \ldots, n$.*

In (3.5) it's understood that the sum is taken over all $1 \leq k \leq n$ not equal to $i$; that is,

$$\sum_{k \neq i} U_k = U_1 + \cdots + U_{i-1} + U_{i+1} + \cdots + U_n.$$

Thus, in particular, if $U_1$, $U_2$, and $U_3$ are subspaces of $V$, then

$$V = \bigoplus_{k=1}^{3} U_k = U_1 \oplus U_2 \oplus U_3$$

if and only if

$$V = U_1 + U_2 + U_3$$

and

$$U_1 \cap (U_2 + U_3) = U_2 \cap (U_1 + U_3) = U_3 \cap (U_1 + U_2) = \{\mathbf{0}\}.$$

**Proposition 3.22.** *Let $U$ and $W$ be subspaces of $V$. Then $V = U \oplus W$ if and only if for each $\mathbf{v} \in V$ there exist unique vectors $\mathbf{u} \in U$ and $\mathbf{w} \in W$ such that $\mathbf{v} = \mathbf{u} + \mathbf{w}$.*

To say there exist unique vectors $\mathbf{u} \in U$ and $\mathbf{w} \in W$ such that $\mathbf{v} = \mathbf{u} + \mathbf{w}$ means, specifically, that if $\mathbf{u}, \mathbf{u}' \in U$ and $\mathbf{w}, \mathbf{w}' \in W$ are such that $\mathbf{v} = \mathbf{u} + \mathbf{w}$ and $\mathbf{v} = \mathbf{u}' + \mathbf{w}'$, then we must have $\mathbf{u} = \mathbf{u}'$ and $\mathbf{w} = \mathbf{w}'$. We now prove the proposition.

**Proof.** Suppose that $V = U \oplus W$, and let $\mathbf{v} \in V$. Since $V = U + W$ there exist some $\mathbf{u} \in U$ and $\mathbf{w} \in W$ such that $\mathbf{v} = \mathbf{u} + \mathbf{w}$. Suppose $\mathbf{u}' \in U$ and $\mathbf{w}' \in W$ are such that $\mathbf{v} = \mathbf{u}' + \mathbf{w}'$. Then

$$\mathbf{0} = \mathbf{v} - \mathbf{v} = (\mathbf{u} + \mathbf{w}) - (\mathbf{u}' + \mathbf{w}') = (\mathbf{u} - \mathbf{u}') + (\mathbf{w} - \mathbf{w}'),$$

which implies that

$$\mathbf{u} - \mathbf{u}' = \mathbf{w}' - \mathbf{w}$$

and hence $\mathbf{u} - \mathbf{u}', \mathbf{w}' - \mathbf{w} \in U \cap W$ since $\mathbf{u} - \mathbf{u}' \in U$ and $\mathbf{w}' - \mathbf{w} \in W$. However, from $V = U \oplus W$ we have $U \cap W = \{\mathbf{0}\}$, leading to

$$\mathbf{u} - \mathbf{u}' = \mathbf{w}' - \mathbf{w} = \mathbf{0}$$

and therefore $\mathbf{u}' = \mathbf{u}$ and $\mathbf{w}' = \mathbf{w}$.

Conversely, suppose that for each $\mathbf{v} \in V$ there exists unique vectors $\mathbf{u} \in U$ and $\mathbf{w} \in W$ such that $\mathbf{v} = \mathbf{u} + \mathbf{w}$. Then $\mathbf{v} \in U + W$, so clearly $V = U + W$. Suppose that $\mathbf{v} \in U \cap W$. Then we may take $\mathbf{u} \in U$ to be $\mathbf{v}$, and $\mathbf{w} \in W$ to be $\mathbf{0}$, so that

$$\mathbf{u} + \mathbf{w} = \mathbf{v} + \mathbf{0} = \mathbf{v};$$

on the other hand if we let $\mathbf{u}' = \mathbf{0}$ and $\mathbf{w}' = \mathbf{v}$, then $\mathbf{u}' \in U$ and $\mathbf{w}' \in W$ are such that $\mathbf{v} = \mathbf{u}' + \mathbf{w}'$. By our uniqueness hypothesis we must have $\mathbf{u} = \mathbf{u}'$ and $\mathbf{w} = \mathbf{w}'$. That is, $\mathbf{u} = \mathbf{0}$ and $\mathbf{w} = \mathbf{0}$, so that $\mathbf{v} = \mathbf{0}$ and we obtain $\mathbf{v} \in \{\mathbf{0}\}$. From this we conclude that $U \cap W \subseteq \{\mathbf{0}\}$, and since the reverse containment is obvious, we find that both $U \cap W = \{\mathbf{0}\}$ and $V = U + W$ are true. Therefore $V = U \oplus W$. ∎

Proposition 3.22 and its proof are presented largely for pedagogical reasons. The more general result is given next, though it takes a bit more work to prove and will have limited applicability in the next few chapters.

**Theorem 3.23.** *Let $U_1, \ldots, U_n$ be subspaces of $V$. Then $V = U_1 \oplus \cdots \oplus U_n$ if and only if for each $\mathbf{v} \in V$ there exist unique vectors $\mathbf{u}_1 \in U_1, \ldots, \mathbf{u}_n \in U_n$ such that $\mathbf{v} = \mathbf{u}_1 + \cdots + \mathbf{u}_n$.*

**Proof.** Suppose that $V = U_1 \oplus \cdots \oplus U_n$. Let $\mathbf{v} \in V$, so for each $1 \leq k \leq n$ there exists some $\mathbf{u}_k \in U_k$ such that $\mathbf{v} = \sum_{k=1}^n \mathbf{u}_k$. Now, suppose that $\mathbf{v} = \sum_{k=1}^n \mathbf{u}_k'$, where $\mathbf{u}_k' \in U_k$ for each $k$. Fix $1 \leq i \leq n$. We have $\mathbf{u}_i' - \mathbf{u}_i \in U_i$, and from

$$\sum_{k=1}^n (\mathbf{u}_k - \mathbf{u}_k') = \sum_{k=1}^n \mathbf{u}_k - \sum_{k=1}^n \mathbf{u}_k' = \mathbf{v} - \mathbf{v} = \mathbf{0}$$

we obtain

$$\mathbf{u}_i' - \mathbf{u}_i = \sum_{k \neq i} (\mathbf{u}_k - \mathbf{u}_k') \in \sum_{k \neq i} U_k.$$

That is,

$$\mathbf{u}_i' - \mathbf{u}_i \in U_i \cap \sum_{k \neq i} U_k = \{\mathbf{0}\},$$

so that $\mathbf{u}_i' - \mathbf{u}_i = \mathbf{0}$ and hence $\mathbf{u}_i' = \mathbf{u}_i$. Since $1 \leq i \leq n$ is arbitrary we conclude that $\mathbf{u}_1' = \mathbf{u}_1, \ldots, \mathbf{u}_n' = \mathbf{u}_n$, and therefore the vectors $\mathbf{u}_1 \in U_1, \ldots, \mathbf{u}_n \in U_n$ for which $\mathbf{v} = \sum_{k=1}^n \mathbf{u}_k$ are unique.

Next, suppose that for each $\mathbf{v} \in V$ there exist unique vectors $\mathbf{u}_1 \in U_1, \ldots, \mathbf{u}_n \in U_n$ such that $\mathbf{v} = \sum_{k=1}^n \mathbf{u}_k$. Then it is clear that

$$V = \sum_{k=1}^n U_k. \tag{3.6}$$

Fix $1 \leq i \leq n$, and suppose that

$$\mathbf{v} \in U_i \cap \sum_{k \neq i} U_k.$$

Thus $\mathbf{v} \in U_i$ implies we have $\mathbf{u} = \sum_{k=1}^n \mathbf{u}_k$, where $\mathbf{u}_k \in U_k$ is $\mathbf{0}$ for $k \neq i$, and $\mathbf{u}_i = \mathbf{v} \in U_i$. On the other hand $\mathbf{v} \in \sum_{k \neq i} U_k$ implies that, for each $k \neq i$ there exists some $\mathbf{u}_k' \in U_k$ such that

$\mathbf{v} = \sum_{k \neq i} \mathbf{u}'_k$, and so if we let $\mathbf{u}'_i \in U_i$ be $\mathbf{0}$, we obtain $\mathbf{v} = \sum_{k=1}^{n} \mathbf{u}'_k$. Now, by our uniqueness hypothesis it must be that $\mathbf{u}_k = \mathbf{u}'_k$ for each $1 \leq k \leq n$. In particular,

$$\mathbf{v} = \mathbf{u}_i = \mathbf{u}'_i = \mathbf{0},$$

and so $\mathbf{v} \in \{\mathbf{0}\}$. This shows that $U_i \cap \sum_{k \neq i} U_k \subseteq \{\mathbf{0}\}$, and since the reverse containment is obvious, we conclude that

$$U_i \cap \sum_{k \neq i} U_k = \{\mathbf{0}\}. \tag{3.7}$$

Now, the equations (3.6) and (3.7) imply that $V = U_1 \oplus \cdots \oplus U_n$. ■

## 3.4 – Linear Combinations and Spans

**Definition 3.24.** *A vector* $\mathbf{v}$ *is called a* ***linear combination*** *of the vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *if there exist scalars* $c_1, \ldots, c_n$ *such that*

$$\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = \sum_{i=1}^{n} c_i\mathbf{v}_i.$$

**Example 3.25.** Define $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^3$ by

$$\mathbf{u} = \begin{bmatrix} 2 \\ -3 \\ 5 \end{bmatrix}, \quad \mathbf{v} = \begin{bmatrix} 0 \\ 7 \\ -1 \end{bmatrix}, \quad \text{and} \quad \mathbf{w} = \begin{bmatrix} 4 \\ 1 \\ 9 \end{bmatrix}.$$

Show that $\mathbf{w}$ is a linear combination of $\mathbf{u}$ and $\mathbf{v}$.

**Solution.** We must find scalars $a$ and $b$ such that

$$\mathbf{w} = a\mathbf{u} + b\mathbf{v} = \begin{bmatrix} 2a \\ -3a \\ 5a \end{bmatrix} + \begin{bmatrix} 0 \\ 7b \\ -b \end{bmatrix} = \begin{bmatrix} 2a \\ -3a + 7b \\ 5a - b \end{bmatrix}.$$

That is, we need $a$ and $b$ to satisfy

$$\begin{bmatrix} 2a \\ -3a + 7b \\ 5a - b \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \\ 9 \end{bmatrix},$$

which is the system of equations

$$\begin{cases} 2a \phantom{+7b} = 4 \\ -3a + 7b = 1 \\ 5a - \phantom{7}b = 9 \end{cases}$$

From the first equation we have $a = 2$. Substituting this into the second equation yields $-6 + 7b = 1$, or $b = 1$. Now we must determine whether $(a, b) = (2, 1)$ satisfies the third equation, in which general is unlikely but in this case works:

$$5a - b = 9 \quad \Rightarrow \quad 5(2) - 1 = 9 \quad \Rightarrow \quad 9 = 9.$$

So $\mathbf{w} = 2\mathbf{u} + \mathbf{v}$, and therefore $\mathbf{w}$ is a linear combination of $\mathbf{u}$ and $\mathbf{v}$. ■

**Example 3.26.** Define $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^3$ by

$$\mathbf{u} = \begin{bmatrix} 2 \\ -3 \\ 5 \end{bmatrix}, \quad \mathbf{v} = \begin{bmatrix} 0 \\ 7 \\ -1 \end{bmatrix}, \quad \text{and} \quad \mathbf{w} = \begin{bmatrix} 4 \\ -13 \\ 9 \end{bmatrix}.$$

Show that $\mathbf{w}$ is not a linear combination of $\mathbf{u}$ and $\mathbf{v}$.

**Solution.** We must show that there exist no scalars $a$ and $b$ such that

$$\begin{bmatrix} 4 \\ -13 \\ 9 \end{bmatrix} = \mathbf{w} = a\mathbf{u} + b\mathbf{v} = \begin{bmatrix} 2a \\ -3a + 7b \\ 5a - b \end{bmatrix},$$

which sets up the system of equations

$$\begin{cases} 2a \phantom{+7b} = 4 \\ -3a + 7b = -13 \\ 5a - \phantom{7}b = 9 \end{cases}$$

The first equation gives $a = 2$. Substituting this into the second equation yields $-6 + 7b = -13$, or $b = -1$. However, putting $(a, b) = (2, -1)$ into the third equation yields a contradiction:

$$5a - b = 9 \quad \Rightarrow \quad 5(2) - (-1) = 9 \quad \Rightarrow \quad 11 = 9.$$

Hence the system of equations has no solution, which is to say there are no scalars $a$ and $b$ for which $\mathbf{w} = a\mathbf{u} + b\mathbf{v}$. ■

**Definition 3.27.** *Let $V$ be a vector space and $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$. We say vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ **span** $V$, or $V$ is **spanned** by the set $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$, if for every $\mathbf{v} \in V$ there exist scalars $c_1, \dots, c_n$ such that $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n$.*[5]

Thus vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ span $V$ if and only if every vector in $V$ is expressible as a linear combination of $\mathbf{v}_1, \dots, \mathbf{v}_n$. Define the **span** of $\mathbf{v}_1, \dots, \mathbf{v}_n$ to be the set

$$\operatorname{Span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \left\{ \sum_{i=1}^{n} c_i\mathbf{v}_i : c_1, \dots, c_n \in \mathbb{F} \right\},$$

which is to say $\operatorname{Span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is the set of *all* possible linear combinations of the vectors $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$. It is easy to see in light of the closure properties (3.1) and (3.2) that $V$ is spanned by $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ if and only if

$$V = \operatorname{Span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}.$$

If $S$ is an arbitrary subset of a vector space $V$ over $\mathbb{F}$, then $\operatorname{Span}(S)$ is defined to be the set of all linear combinations of *finitely many* vectors belonging to $S$. Precisely put,

$$\operatorname{Span}(S) = \left\{ \sum_{k=1}^{n} c_k\mathbf{v}_k : n \in \mathbb{N},\ \mathbf{v}_1, \dots, \mathbf{v}_n \in S, \text{ and } c_1, \dots, c_n \in \mathbb{F} \right\}.$$

This definition allows us to speak meaningfully of the span of an infinite set, in particular.

**Example 3.28.** Determine whether the vectors

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 2 \\ 2 \\ 0 \end{bmatrix}, \quad \mathbf{v}_3 = \begin{bmatrix} 3 \\ 0 \\ 0 \end{bmatrix}$$

span $\mathbb{R}^3$.

[5]Some books say $\mathbf{v}_1, \dots, \mathbf{v}_n$ **generate** $V$, or $V$ is **generated** by the set $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$.

**Solution.** Let

$$\mathbf{x} = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3.$$

We attempt to find scalars $c_1, c_2, c_3 \in \mathbb{R}$ such that $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 = \mathbf{x}$; that is,

$$c_1 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + c_2 \begin{bmatrix} 2 \\ 2 \\ 0 \end{bmatrix} + c_3 \begin{bmatrix} 3 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

This yields the system

$$\begin{cases} c_1 + 2c_2 + 3c_3 = x \\ c_1 + 2c_2 \qquad\;\; = y \\ c_1 \qquad\qquad\quad\; = z \end{cases}$$

which indeed has a solution:

$$(c_1, c_2, c_3) = \left( z, \frac{y-z}{2}, \frac{x-y}{3} \right).$$

Thus every vector in $\mathbb{R}^3$ is expressible as a linear combination of $\mathbf{v}_1$, $\mathbf{v}_2$, and $\mathbf{v}_3$, which shows that the set $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ spans $\mathbb{R}^3$. ■

**Example 3.29.** Determine whether the vectors

$$\mathbf{v}_1 = \begin{bmatrix} 2 \\ -1 \\ 3 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 4 \\ 1 \\ 2 \end{bmatrix}, \quad \mathbf{v}_3 = \begin{bmatrix} 8 \\ -1 \\ 8 \end{bmatrix}$$

span $\mathbb{R}^3$.

**Solution.** Let

$$\mathbf{x} = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3.$$

We attempt to find scalars $c_1, c_2, c_3 \in \mathbb{R}$ such that $c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3 = \mathbf{x}$. This yields the system

$$\begin{cases} 2c_1 + 4c_2 + 8c_3 = x \\ -c_1 + \phantom{4}c_2 - \phantom{8}c_3 = y \\ 3c_1 + 2c_2 + 8c_3 = z \end{cases}$$

This can be cast as an augmented matrix and manipulated using elementary row operations:

$$\left[\begin{array}{rrr|c} 2 & 4 & 8 & x \\ -1 & 1 & -1 & y \\ 3 & 2 & 8 & z \end{array}\right] \sim \left[\begin{array}{rrr|c} -1 & 1 & -1 & y \\ 2 & 4 & 8 & x \\ 3 & 2 & 8 & z \end{array}\right] \sim \left[\begin{array}{rrr|c} -1 & 1 & -1 & y \\ 0 & 6 & 6 & 2y+x \\ 0 & 5 & 5 & 3y+z \end{array}\right]$$

$$\sim \left[\begin{array}{rrr|c} 1 & -1 & 1 & -y \\ 0 & 1 & 1 & \frac{2y+x}{6} \\ 0 & 5 & 5 & 3y+z \end{array}\right] \sim \left[\begin{array}{rrr|c} 1 & -1 & 1 & -y \\ 0 & 1 & 1 & \frac{2y+x}{6} \\ 0 & 0 & 0 & 3y+z-5\left(\frac{2y+x}{6}\right) \end{array}\right]$$

We see that in order for $\mathbf{x}$ to be expressed as a linear combination of $\mathbf{v}_1$, $\mathbf{v}_2$, and $\mathbf{v}_3$, we need $x$, $y$, and $z$ such that

$$3y + z - 5\left(\frac{2y + x}{6}\right) = 0,$$

or

$$5x - 8y - 6z = 0.$$

This leads to $1 = 0$ if we choose $x = 0$, $y = 0$, and $z = 1$, for instance. That is, we cannot express

$$\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

as a linear combination of $\mathbf{v}_1$, $\mathbf{v}_2$, and $\mathbf{v}_3$. We conclude that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ does not span $\mathbb{R}^3$. ■

**Proposition 3.30.** *Let $V$ be a vector space. If $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$, then $W = \operatorname{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a subspace of $V$.*

**Proof.** Suppose $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$. First we observe that

$$\mathbf{0} = 0\mathbf{v}_1 + \cdots + 0\mathbf{v}_n \in W.$$

Now, let $a \in \mathbb{F}$, and let $\mathbf{u} \in W$ so that there exist $c_1, \ldots, c_n \in \mathbb{F}$ such that

$$\mathbf{u} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n.$$

Since

$$a\mathbf{u} = a(c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n) = ac_1\mathbf{v}_1 + \cdots + ac_n\mathbf{v}_n$$

for $ac_1, \ldots, ac_n \in \mathbb{F}$, it follows that $a\mathbf{u} \in W$ also.

Next, let $\mathbf{u}, \mathbf{v} \in W$. Then there exist $c_1, \ldots, c_n, d_1, \ldots, d_n \in \mathbb{F}$ such that

$$\mathbf{u} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n \quad \text{and} \quad \mathbf{v} = d_1\mathbf{v}_1 + \cdots + d_n\mathbf{v}_n,$$

and then

$$\mathbf{u} + \mathbf{v} = (c_1 + d_1)\mathbf{v}_1 + \cdots + (c_n + d_n)\mathbf{v}_n$$

for $c_1 + d_1, \ldots, c_n + d_n \in \mathbb{F}$ shows that $\mathbf{u} + \mathbf{v} \in W$ also.

Therefore $W$ is a subspace of $V$ by Corollary 3.11. ■

**Proposition 3.31.** *Let $V$ be a vector space, and let $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subseteq V$. If $a \in \mathbb{F}$ is nonzero, then*

$$\operatorname{Span}(S) = \operatorname{Span}\big((S \setminus \{\mathbf{v}_i\}) \cup \{\mathbf{v}_i + a\mathbf{v}_j\}\big)$$

*for any $i, j \in \{1, \ldots, n\}$ with $i \neq j$.*

**Proof.** Suppose $a \in \mathbb{F} \setminus \{0\}$, and let $i, j \in \{1, \ldots, n\}$ with $i \neq j$. Let $T = (S \setminus \{\mathbf{v}_i\}) \cup \{\mathbf{v}_i + a\mathbf{v}_j\}$, and note that $T$ is the set obtained from $S$ by replacing $\mathbf{v}_i$ with $\mathbf{v}_i + a\mathbf{v}_j$. Suppose $\mathbf{v} \in \operatorname{Span}(S)$, so that $\mathbf{v} = \sum_{k=1}^n c_k\mathbf{v}_k$ for some $c_1, \ldots, c_n \in \mathbb{F}$. Now,

$$\mathbf{v} = c_i\mathbf{v}_i + c_j\mathbf{v}_j + \sum_{k \neq i,j} c_k\mathbf{v}_k = c_i(\mathbf{v}_i + a\mathbf{v}_j) + (c_j - ac_i)\mathbf{v}_j + \sum_{k \neq i,j} c_k\mathbf{v}_k,$$

which shows that $\mathbf{v}$ is a linear combination of the elements of $T$ and hence $\mathbf{v} \in \mathrm{Span}(T)$.

Next, suppose that $\mathbf{v} \in \mathrm{Span}(T)$, so there exists $c_1, \ldots, c_n \in \mathbb{F}$ such that

$$\mathbf{v} = c_i(\mathbf{v}_i + a\mathbf{v}_j) + \sum_{k \neq i} c_k \mathbf{v}_k,$$

and hence

$$\mathbf{v} = \sum_{k=1}^{n} c'_k \mathbf{v}_k$$

with $c'_k = c_k$ for $k \neq j$ and $c'_j = ac_i + c_j$, which shows that $\mathbf{v}$ is a linear combination of elements of $S$ and hence $\mathbf{v} \in \mathrm{Span}(S)$.

Since $\mathrm{Span}(S) \subseteq \mathrm{Span}(T)$ and $\mathrm{Span}(T) \subseteq \mathrm{Span}(S)$, we conclude that $\mathrm{Span}(S) = \mathrm{Span}(T)$ as was to be shown. ■

## Problems

1. Let
$$\mathbf{u}_1 = \begin{bmatrix} -1 \\ 3 \end{bmatrix} \quad \text{and} \quad \mathbf{u}_2 = \begin{bmatrix} 2 \\ -6 \end{bmatrix}.$$
Prove or disprove that $\text{Span}\{\mathbf{u}_1, \mathbf{u}_2\} = \mathbb{R}^2$.

2. Determine which of the following are linear combinations of vectors
$$\mathbf{u} = \begin{bmatrix} 1 \\ -1 \\ 3 \end{bmatrix} \quad \text{and} \quad \mathbf{v} = \begin{bmatrix} 2 \\ 4 \\ 0 \end{bmatrix}.$$
(a) $\mathbf{w} = [-1, -11, 9]^\top$
(b) $\mathbf{w} = [3, 7, -2]^\top$

3. Express each polynomial as linear combinations of
$$p_1 = 2 + x + 4x^2, \quad p_2 = 1 - x + 3x^2, \quad \text{and} \quad p_3 = 3 + 2x + 5x^2.$$
(a) $6$
(b) $2 + 6x^2$
(c) $5 + 9x + 5x^2$

4. Determine whether the given vectors span $\mathbb{R}^3$.
(a) $\mathbf{v}_1 = [3, 3, 3]^\top$, $\mathbf{v}_2 = [-2, -2, 0]^\top$, $\mathbf{v}_3 = [1, 0, 0]^\top$
(b) $\mathbf{v}_1 = [1, -1, 3]^\top$, $\mathbf{v}_2 = [4, 0, 2]^\top$, $\mathbf{v}_3 = [6, -1, 6]^\top$
(c) $\mathbf{v}_1 = [3, 1, 4]^\top$, $\mathbf{v}_2 = [2, -3, 5]^\top$, $\mathbf{v}_3 = [5, -2, 9]^\top$, $\mathbf{v}_4 = [1, 4, -1]^\top$
(d) $\mathbf{v}_1 = [1, 3, 3]^\top$, $\mathbf{v}_2 = [1, 3, 4]^\top$, $\mathbf{v}_3 = [1, 4, 3]^\top$, $\mathbf{v}_4 = [6, 2, 1]^\top$

5. Determine whether the polynomials
$$\begin{aligned} p_1 &= 1 + 2x - x^2 \qquad & p_2 &= 3 + x^2 \\ p_3 &= 5 + 4x - x^2 \qquad & p_4 &= -2 + 2x - 2x^2 \end{aligned}$$
span the vector space $\mathcal{P}_2(\mathbb{R}) = \{a + bx + cx^2 : a, b, c \in \mathbb{R}\}$.

## 3.5 – Linear Independence and Bases

**Definition 3.32.** *Let $V$ be a vector space and $A = \{\mathbf{v}_1, \dots, \mathbf{v}_n\} \subseteq V$ be nonempty. If the equation*

$$c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = \mathbf{0} \tag{3.8}$$

*admits only the trivial solution $c_1 = \cdots = c_n = 0$, then we call $A$ a **linearly independent set** and $\mathbf{v}_1, \dots, \mathbf{v}_n$ are **linearly independent vectors**. Otherwise we call $A$ a **linearly dependent set** and $\mathbf{v}_1, \dots, \mathbf{v}_n$ are **linearly dependent vectors**.*

*An arbitrary set $S \subseteq V$ is **linearly independent** if every finite subset of $S$ is linearly independent. Otherwise $S$ is **linearly dependent**.*

It is straightforward to show that the definition for linear independence of an arbitrary set $S$ is equivalent to the definition for linear independence of $A = \{\mathbf{v}_1, \dots, \mathbf{v}_n\} \neq \varnothing$ in the case when $S$ is a nonempty finite set. Thus, the second paragraph of Definition 3.32 is the more general definition of linear independence.

A careful reading of Definition 3.32 should make clear that vectors $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$ are linearly dependent if and only if there exist scalars $c_1, \dots, c_n$ *not all zero* such that (3.8) is satisfied. Also, an arbitrary set $S$ is linearly dependent if and only if there exists some finite set $\{\mathbf{v}_1, \dots, \mathbf{v}_n\} \subseteq S$ for which (3.8) has a *nontrivial* solution.

**Theorem 3.33.** *Let $\mathbf{A}$ be a row-echelon matrix. Then the nonzero row vectors of $\mathbf{A}$ are linearly independent, and the column vectors of $\mathbf{A}$ that contain a pivot are linearly independent.*

**Proof.** We shall prove the second statement concerning the column vectors using induction, and leave the proof of the first statement (which is quite similar) as a problem.

Let $m \in \mathbb{N}$ be arbitrary. It is clear that if $\mathbf{A} \in \mathbb{F}^m$ is a row-echelon matrix with a pivot, then its single column vector constitutes a linearly independent set. Let $n \in \mathbb{N}$ be arbitrary, and suppose that the pivot columns of any row-echelon matrix $\mathbf{A} \in \mathbb{F}^{m\times n}$ are linearly independent. Let $\mathbf{A} \in \mathbb{F}^{m\times(n+1)}$ be a row-echelon matrix. Then the matrix $\mathbf{B} \in \mathbb{F}^{m\times n}$ that results from deleting column $n+1$ from $\mathbf{A}$ is also a row-echelon matrix, and so its pivot columns $\mathbf{p}_1, \dots, \mathbf{p}_r$ are linearly independent by inductive hypothesis. Now, if column $n+1$ of $\mathbf{A}$ is not a pivot column, then the pivot columns of $\mathbf{A}$ are precisely $\mathbf{p}_1, \dots, \mathbf{p}_r$, and we conclude that the pivot columns of $\mathbf{A}$ are linearly independent.

Suppose rather that column $n+1$ of $\mathbf{A}$ is a pivot column. Then the pivot columns of $\mathbf{A}$ are precisely $\mathbf{p}_1, \dots, \mathbf{p}_r$ and $\mathbf{q}$, where $\mathbf{q} = [q_1 \cdots q_m]^\top$ denotes column $n+1$ of $\mathbf{A}$. For each $1 \leq j \leq r$ let

$$\mathbf{p}_j = \begin{bmatrix} p_{1j} \\ \vdots \\ p_{mj} \end{bmatrix}.$$

Since $\mathbf{q}$ is a pivot column, there exists some $1 \leq \ell \leq m$ such that $q_\ell$ is a pivot of $\mathbf{A}$, and then by the definition of a pivot we have $p_{\ell j} = 0$ for all $1 \leq j \leq r$. Suppose $c_1, \dots, c_r, a \in \mathbb{F}$ are such that

$$c_1\mathbf{p}_1 + \cdots + c_r\mathbf{p}_r + a\mathbf{q} = \mathbf{0}. \tag{3.9}$$

This yields

$$c_1 p_{\ell 1} + \cdots + c_r p_{\ell r} + a q_\ell = 0,$$

which reduces to $aq_\ell = 0$, and since $q_\ell \neq 0$ on account of being a pivot, we finally obtain $a = 0$. Hence

$$c_1 \mathbf{p}_1 + \cdots + c_r \mathbf{p}_r = \mathbf{0},$$

and since $\mathbf{p}_1, \ldots, \mathbf{p}_r$ are linearly independent, it follows that $c_j = 0$ for $1 \leq j \leq r$. This shows that (3.9) only admits the trivial solution, and therefore $\{\mathbf{p}_1, \ldots, \mathbf{p}_r, \mathbf{q}\}$ is a linearly independent set. That is, the pivot columns of $\mathbf{A} \in \mathbb{F}^{m \times (n+1)}$ are linearly independent, and we conclude by induction that the pivot columns of any row-echelon matrix are linearly independent. ■

Recall the vector space $\mathcal{F}(S, \mathbb{F})$ of functions $S \to \mathbb{F}$ introduced in Example 3.7. A linear combination of $f_1, f_2, \ldots, f_n \in \mathcal{F}(S, \mathbb{F})$ is an expression of the form

$$c_1 f_1 + c_2 f_2 + \cdots + c_n f_n$$

for some choice of constants $c_1, c_2, \ldots, c_n \in \mathbb{F}$, which of course is itself a function in $\mathcal{F}(S, \mathbb{F})$ given by

$$(c_1 f_1 + c_2 f_2 + \cdots + c_n f_n)(x) = c_1 f_1(x) + c_2 f_2(x) + \cdots + c_n f_n(x)$$

for all $x \in S$. To write

$$c_1 f_1 + c_2 f_2 + \cdots + c_n f_n = 0 \tag{3.10}$$

means

$$(c_1 f_1 + c_2 f_2 + \cdots + c_n f_n)(x) = 0$$

for all $x \in S$; that is, $c_1 f_1 + c_2 f_2 + \cdots + c_n f_n$ is the zero function $0 : S \to \{0\}$.

We say $f_1, f_2, \ldots, f_n \in \mathcal{F}(S, \mathbb{F})$ are **linearly independent on** $\boldsymbol{S}$ if (3.10) implies that

$$c_1 = c_2 = \cdots = c_n = 0.$$

Functions that are not linearly independent on $S$ are said to be **linearly dependent on** $\boldsymbol{S}$. Thus, $f_1, f_2, \ldots, f_n$ are linearly dependent on $S$ if there can be found constants $c_1, c_2, \ldots, c_n \in \mathbb{F}$, *not all zero*, such that $(c_1 f_1 + c_2 f_2 + \cdots + c_n f_n)(x) = 0$ for all (and it *must* be *all*) $x \in S$.

**Example 3.34.** Consider the functions $f, g : \mathbb{R} \to \mathbb{R}$ given by

$$f(t) = e^{at} \quad \text{and} \quad g(t) = e^{bt}$$

for $a, b \neq 0$ such that $a \neq b$. To show that $f$ and $g$ (as vectors in the vector space $\mathbb{R}^{\mathbb{R}}$) are linearly independent on $\mathbb{R}$, we start by supposing that $c_1, c_2 \in \mathbb{R}$ are such that

$$c_1 f + c_2 g = 0.$$

That is, the constants $c_1$ and $c_2$ are such that

$$c_1 e^{at} + c_2 e^{bt} = c_1 f(t) + c_2 g(t) = (c_1 f + c_2 g)(t) = 0$$

for all $t \in \mathbb{R}$. Thus, by choosing $t = 0$ and $t = 1$, we have in particular

$$c_1 + c_2 = 0 \quad \text{and} \quad c_1 e^a + c_2 e^b = 0.$$

From the first equation we have

$$c_2 = -c_1, \tag{3.11}$$

which, when put into the second equation, yields

$$c_1e^a - c_1e^b = 0,$$

and thus

$$c_1(e^a - e^b) = 0. \tag{3.12}$$

From $a \neq b$ we have

$$e^a = \exp(a) \neq \exp(b) = e^b$$

since the exponential function is one-to-one as established in §7.2 of the *Calculus Notes*, so $e^a - e^b \neq 0$ and from equations (3.12) and (3.11) we conclude that $c_1 = c_2 = 0$. Therefore the functions $f$ and $g$, which is to say $e^{at}$ and $e^{bt}$, are linearly independent on $\mathbb{R}$ for any distinct nonzero real numbers $a$ and $b$. ■

**Example 3.35.** Show that the functions 1, $x$, and $x^2$ are linearly independent on any open interval $I \subseteq (0, \infty)$.

**Solution.** Let $I$ be an interval in $(0, \infty)$, so that $I = (a, b)$ for some $0 < a < b \leq \infty$. From analysis we know there can be found some $\rho > 1$ such that $a < \rho a < 2\rho a < 3\rho a < b$. To show that the functions 1, $x$, and $x^2$ (as vectors in the space $\mathbb{R}^I$) are linearly independent on $I$, we suppose that $c_1, c_2, c_3 \in \mathbb{R}$ are such that

$$c_1 + c_2x + c_3x^2 = 0. \tag{3.13}$$

for all $x \in I$. Substituting $\rho a$, $2\rho a$, and $3\rho a$ for $x$ in (3.13) yields the system

$$\begin{cases} c_1 + \ \ (\rho a)c_2 + \ \ (\rho a)^2c_3 = 0 \\ c_1 + (2\rho a)c_2 + (2\rho a)^2c_3 = 0 \\ c_1 + (3\rho a)c_2 + (3\rho a)^2c_3 = 0 \end{cases}$$

We can employ Gaussian Elimination to help solve this system for $c_1$, $c_2$, and $c_3$:

$$\left[\begin{array}{ccc|c} 1 & \rho a & (\rho a)^2 & 0 \\ 1 & 2\rho a & 4(\rho a)^2 & 0 \\ 1 & 3\rho a & 9(\rho a)^2 & 0 \end{array}\right] \xrightarrow[-r_1+r_3\to r_3]{-r_1+r_2\to r_2} \left[\begin{array}{ccc|c} 1 & \rho a & (\rho a)^2 & 0 \\ 0 & \rho a & 3(\rho a)^2 & 0 \\ 0 & 2\rho a & 8(\rho a)^2 & 0 \end{array}\right] \xrightarrow{-2r_2+r_3\to r_3}$$

$$\left[\begin{array}{ccc|c} 1 & \rho a & (\rho a)^2 & 0 \\ 0 & \rho a & 3(\rho a)^2 & 0 \\ 0 & 0 & 2(\rho a)^2 & 0 \end{array}\right] \xrightarrow[r_3\div 2(\rho a)^2\to r_3]{r_2\div\rho a\to r_2} \left[\begin{array}{ccc|c} 1 & \rho a & (\rho a)^2 & 0 \\ 0 & 1 & 3\rho a & 0 \\ 0 & 0 & 1 & 0 \end{array}\right].$$

Thus we now have the system

$$\begin{cases} c_1 + (\rho a)c_2 + (\rho a)^2c_3 = 0 \\ \qquad\qquad c_2 + (3\rho a)c_3 = 0 \\ \qquad\qquad\qquad\qquad c_3 = 0 \end{cases}$$

from which it easily follows that $c_1 = c_2 = c_3 = 0$. This shows that the set $\{1, x, x^2\}$ is a linearly independent set of functions in $\mathbb{R}^I$ for any open interval $I \subseteq (0, \infty)$. ■

**Remark.** The basic approach exhibited in Example 3.35 can, with minor modifications, be used to show that

$$\{1, x, x^2, \dots, x^n\}$$

is linearly independent in $\mathbb{R}^I$ for *any* interval $I \subseteq \mathbb{R}$ and integer $n \geq 0$.

**Example 3.36.** Consider the functions

$$x \mapsto \cos 2x, \quad x \mapsto \cos^2 x, \quad x \mapsto \sin^2 x$$

with domain $\mathbb{R}$. Suppose $c_1, c_2, c_3 \in \mathbb{R}$ are such that

$$c_1 \cos 2x + c_2 \cos^2 x + c_3 \sin^2 x = 0 \tag{3.14}$$

for all $x \in \mathbb{R}$. The functions $\cos 2x$, $\cos^2 x$, and $\sin^2 x$ are linearly independent on $\mathbb{R}$ if and only if the only way to satisfy (3.14) for all $x \in \mathbb{R}$ is to have $c_1 = c_2 = c_3 = 0$. However, it is true that

$$\cos 2x = \cos^2 x - \sin^2 x$$

on $\mathbb{R}$, and hence (3.14) is equivalent to the equation

$$c_1(\cos^2 x - \sin^2 x) + c_2 \cos^2 x + c_3 \sin^2 x = 0.$$

Now notice that this equation, and subsequently (3.14), is satisfied for all $x \in \mathbb{R}$ if we let $c_1 = 1$, $c_2 = -1$, and $c_3 = 1$. So (3.14) has a nontrivial solution on $\mathbb{R}$, and therefore the functions $\cos 2x$, $\cos^2 x$, and $\sin^2 x$ are linearly dependent on $\mathbb{R}$. ■

**Proposition 3.37.** *Let $V$ be a vector space.*

1. *The set $\{\mathbf{0}\} \subseteq V$ is linearly dependent.*
2. *The empty set $\varnothing$ is linearly independent.*

**Proof.**
*Proof of Part (1).* The equation $c\mathbf{0} = \mathbf{0}$ is satisfied by letting $c = 1$. Since this is a nontrivial solution, it follows that $\{\mathbf{0}\}$ is linearly dependent.

*Proof of Part (2).* From Definition 3.32 an arbitrary set $S$ is linearly independent if and only if the following statement (P) is true: "If $\mathbf{v}_1, \dots, \mathbf{v}_n \in S$, then $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent." However if $S = \varnothing$, then the statement "$\mathbf{v}_1, \dots, \mathbf{v}_n \in S$" is necessarily false, and therefore (P) is vacuously true. We conclude that $\varnothing$ is linearly independent. ■

**Proposition 3.38.** *Let $V$ be a vector space. If $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$ are linearly independent and*

$$x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n = y_1\mathbf{v}_1 + \cdots + y_n\mathbf{v}_n$$

*for scalars $x_1, \dots, x_n$ and $y_1, \dots, y_n$, then $x_i = y_i$ for all $1 \leq i \leq n$.*

**Proof.** Suppose that $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ are linearly independent and

$$\sum_{i=1}^{n} x_i \mathbf{v}_i = \sum_{i=1}^{n} y_i \mathbf{v}_i$$

for scalars $x_i$ and $y_i$. Then

$$\sum_{i=1}^{n} (x_i - y_i)\mathbf{v}_i = \mathbf{0},$$

and since the vectors $\mathbf{v}_i$ are linearly independent, it follows that $x_i - y_i = 0$ for $1 \leq i \leq n$. That is, $x_i = y_i$ for $1 \leq i \leq n$. ■

**Proposition 3.39.** *Suppose $V$ is a vector space, and $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a linearly independent set in $V$. Given $\mathbf{w} \in V$, the set $S \cup \{\mathbf{w}\}$ is linearly dependent if and only if $\mathbf{w} \in \mathrm{Span}(S)$.*

**Proof.** Suppose that $S \cup \{\mathbf{w}\}$ is linearly dependent. Then the equation

$$x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n + x_{n+1}\mathbf{w} = 0$$

has a nontrivial solution, which is to say at least one of the coefficients $x_1, \ldots, x_{n+1}$ is nonzero. If $x_{n+1} = 0$, then $x_k \neq 0$ for some $1 \leq k \leq n$, in which case

$$x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n = 0$$

has a nontrivial solution and we conclude that $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly dependent—a contradiction. Hence $x_{n+1} \neq 0$, and we may write

$$\mathbf{w} = \sum_{k=1}^{n} -\frac{x_k}{x_{n+1}}\mathbf{v}_k,$$

which shows that $\mathbf{w} \in \mathrm{Span}(S)$.

Conversely, suppose that $\mathbf{w} \in \mathrm{Span}(S)$, so that

$$\mathbf{w} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$$

for some $a_1, \ldots, a_n \in \mathbb{F}$. If we choose $x_k = -a_k$ for each $1 \leq k \leq n$, and let $x_{n+1} = 1$, then

$$\begin{aligned} x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n + x_{n+1}\mathbf{w} &= -a_1\mathbf{v}_1 - \cdots - a_n\mathbf{v}_n + \mathbf{w} \\ &= -(a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) + (a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) \\ &= \mathbf{0}, \end{aligned}$$

and hence

$$x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n + x_{n+1}\mathbf{w} = \mathbf{0}.$$

has a nontrivial solution. Therefore $S \cup \{\mathbf{w}\}$ is a linearly dependent set. ■

**Definition 3.40.** *A **basis** for a vector space $V$ is a linearly independent set $\mathcal{B} \subseteq V$ such that $\mathrm{Span}(\mathcal{B}) = V$. In the case of the trivial vector space $\{\mathbf{0}\}$ we take the basis to be $\varnothing$, the empty set.*

A basis $\mathcal{B}$ is frequently **indexed**; that is, there exists an **index set** $I$ of positive integers together with a function $I \to \mathcal{B}$ that pairs each element of $\mathcal{B}$ with a unique $k \in I$. Typically $I$ is either $\{1, \dots, n\}$ for some $n \in \mathbb{N}$, or else $I = \mathbb{N}$. In this fashion the vectors in $\mathcal{B}$ are **ordered** according to the integers to which they are paired, with a symbol such as $\mathbf{v}_k$ being used to denote the vector that is paired with the integer $k \in I$. If $\mathcal{B}$ is an indexed set containing $n$ vectors that we wish to list explicitly, then the list is most properly presented as an $n$-tuple,

$$\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n),$$

rather than as a set $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$. We will adhere to this practice in all situations in which the order of the vectors in $\mathcal{B}$ is important.

**Theorem 3.41.** *If $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis for $V$, then for any $\mathbf{v} \in V$ there exist unique scalars $x_1, \dots, x_n$ for which $\mathbf{v} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n$.*

**Proof.** Suppose that $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis for $V$, and let $\mathbf{v} \in V$. Since $\mathbf{v}_1, \dots, \mathbf{v}_n$ span $V$, there exist scalars $x_1, \dots, x_n$ such that

$$\mathbf{v} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n.$$

Now, suppose

$$\mathbf{v} = y_1\mathbf{v}_1 + \cdots + y_n\mathbf{v}_n$$

for scalars $y_1, \dots, y_n$, so that

$$x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n = y_1\mathbf{v}_1 + \cdots + y_n\mathbf{v}_n.$$

Then since $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent we must have $y_i = x_i$ for all $1 \le i \le n$ by Proposition 3.38. Therefore the scalars $x_1, \dots, x_n$ for which $\mathbf{v} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n$ are unique. ■

The following proposition pertaining to $\mathbb{R}^2$ will be verified using only the most basic algebra. A more general result applying to $\mathbb{R}^n$ for all $n \ge 2$ must wait until later, when more sophisticated machinery will have been built to allow for a far more elegant proof.

**Proposition 3.42.** *Let $[a, b]^\top, [c, d]^\top \in \mathbb{R}^2$.*

1. *$[a, b]^\top$ and $[c, d]^\top$ are linearly dependent if and only if $ad - bc = 0$.*
2. *If $[a, b]^\top$ and $[c, d]^\top$ are linearly independent, then they form a basis for $\mathbb{R}^2$.*

**Proof.**

*Proof of Part (1).* Suppose that $[a, b]^\top$ and $[c, d]^\top$ are linearly dependent. Then there exist scalars $r$ and $s$, not both zero, such that

$$r\begin{bmatrix} a \\ b \end{bmatrix} + s\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

This vector equation gives rise to the system

$$\begin{cases} ar + cs = 0, & (\epsilon_1) \\ br + ds = 0, & (\epsilon_2) \end{cases}$$

If $r \neq 0$, then $d(\epsilon_1) - c(\epsilon_2)$ (i.e. $d$ times equation $(\epsilon_1)$ minus $c$ times equation $(\epsilon_2)$) yields $adr - bcr = 0$, or $(ad - bc)r = 0$. Since $r \neq 0$, we conclude that $ad - bc = 0$.

If $s \neq 0$, then $-b(\epsilon_1) + a(\epsilon_2)$ yields $-bcs + ads = 0$, or $(ad - bc)s = 0$. Since $s \neq 0$, we conclude that $ad - bc = 0$ once more.

Now, we have that either $r \neq 0$ or $s \neq 0$, both of which lead to the conclusion that $ad - bc = 0$ and so the forward implication of part (1) is proven.

Suppose next that $ad - bc = 0$. We must find scalars $x$ and $y$, not both 0, such that

$$x\begin{bmatrix} a \\ b \end{bmatrix} + y\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \tag{3.15}$$

This vector equation gives rise to the system

$$\begin{cases} ax + cy = 0, & (\epsilon_3) \\ bx + dy = 0, & (\epsilon_4) \end{cases}$$

Assume first that $a \neq 0$. Then from $(\epsilon_3)$ we have $x = -cy/a$, and from $-b(\epsilon_3) + a(\epsilon_4)$ we obtain $-bcy + ady = 0$ and then $(ad - bc)y = 0$. Since $ad - bc = 0$, we may satisfy $(ad - bc)y = 0$ by letting $y = a$, and then $x = -cy/a = -c$. It's easy to check that $x = -c$ and $y = a \neq 0$ will satisfy (3.15), and thus $[a, b]^\top$ and $[c, d]^\top$ are linearly dependent.

Now assume that $a = 0$. Then $ad - bc = 0$ implies that $bc = 0$, and so either $b = 0$ or $c = 0$. But $b = 0$ leads us to $[a, b]^\top = [0, 0]^\top$, in which case $[a, b]^\top$ and $[c, d]^\top$ are linearly dependent. Suppose that $c = 0$ and $b \neq 0$. Then equation $(\epsilon_3)$ in the system above vanishes, and only $(\epsilon_4)$ remains to give $x = -dy/b$. If we let $y = b$, then $x = -dy/b = -d$. It's easy to check that $x = -d$ and $y = b \neq 0$, together with our assumptions that $a = 0$ and $c = 0$, will satisfy (3.15).

Since either $a = 0$ or $a \neq 0$ must be the case, and both lead to the conclusion that $x$ and $y$ may be chosen such that both aren't zero and (3.15) is satisfied, it follows that $[a, b]^\top$ and $[c, d]^\top$ must be linearly dependent. The reverse implication of part (1) is proven.

*Proof of Part (2).* Suppose that $[a, b]^\top$ and $[c, d]^\top$ are linearly independent. To show that the vectors form a basis for $\mathbb{R}^2$, we need only verify that

$$\mathbb{R}^2 = \operatorname{Span}\left\{\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix}\right\}.$$

Let $[x_1, x_2]^\top \in \mathbb{R}^2$. Scalars $s_1$ and $s_2$ must be found so that

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = s_1\begin{bmatrix} a \\ b \end{bmatrix} + s_2\begin{bmatrix} c \\ d \end{bmatrix}. \tag{3.16}$$

This gives rise to the system

$$\begin{cases} as_1 + cs_2 = x_1, & (\epsilon_5) \\ bs_1 + ds_2 = x_2, & (\epsilon_6) \end{cases}$$

in which $s_1$ and $s_2$ are the unknowns. From $-b(\epsilon_5) + a(\epsilon_6)$ comes $(ad - bc)s_2 = ax_2 - bx_1$, and since by part (1) the linear independence of $[a, b]$ and $[c, d]^\top$ implies that $ad - bc \neq 0$, we obtain

$$s_2 = \frac{ax_2 - bx_1}{ad - bc}$$

Putting this into $(\epsilon_5)$ and solving for $s_1$ yields

$$s_1 = \frac{1}{a}\left(x_1 - \frac{ax_2 - bx_1}{ad - bc}c\right)$$

if we assume that $a \neq 0$, which shows that there exist scalars $s_1$ and $s_2$ that satisfy (3.16).

If $a = 0$, then $ad - bc \neq 0$ becomes $bc \neq 0$ and thus $b, c \neq 0$. Since $(\epsilon_5)$ is now just $cs_2 = x_1$ and $c \neq 0$, we obtain $s_2 = x_1/c$. Putting this into $(\epsilon_6)$ gives

$$bs_1 + \frac{dx_1}{c} = x_2 \quad \Rightarrow \quad s_1 = \frac{1}{b}\left(x_2 - \frac{dx_1}{c}\right),$$

since $b \neq 0$. Once again there exist scalars satisfying (3.16).

Therefore $[a, b]^\top$ and $[c, d]^\top$ span $\mathbb{R}^2$, and we conclude that the set $\{[a, b]^\top, [c, d]^\top\}$ forms a basis for $\mathbb{R}^2$. This proves part (2). ■

The two parts of Proposition 3.42, when combined, provide an easy test to determine whether two given vectors in $\mathbb{R}^2$ are linearly independent.

**Example 3.43.** Show that $[1, -3]^\top$ and $[5, 6]^\top$ form a basis for $\mathbb{R}^2$.

**Solution.** Here we have $[a, b]^\top = [1, -3]^\top$ and $[c, d]^\top = [5, 6]^\top$, and since

$$ad - bc = (1)(6) - (-3)(5) = 21 \neq 0$$

we conclude by part (1) of Proposition 3.42 that the vectors are linearly independent. Then, by part (2), it follows that the vectors do indeed form a basis for $\mathbb{R}^2$. ■

## Problems

1. Let

$$\mathbf{u}_1 = \begin{bmatrix} 2 \\ 0 \\ -1 \end{bmatrix}, \quad \mathbf{u}_2 = \begin{bmatrix} 3 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{u}_3 = \begin{bmatrix} -2 \\ 3 \\ 2 \end{bmatrix}.$$

   (a) Show that $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ is a linearly independent set.

   (b) The ordered set $\mathcal{B} = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ is a basis for $\mathbb{R}^3$. Given

$$\mathbf{v} = \begin{bmatrix} -6 \\ -10 \\ -5 \end{bmatrix},$$

   find $[\mathbf{v}]_{\mathcal{B}}$, the coordinates of $\mathbf{v}$ with respect to the basis $\mathcal{B}$.

2. Write down a basis for the $yz$-plane in $\mathbb{R}^3$.

3. The plane $P$ given by $x + 2y - 3z = 0$ is a subspace of $\mathbb{R}^3$. Find a basis for it.

## 3.6 – Dimension

The first proposition we consider is useful mainly for proving more momentous results in this section.

**Proposition 3.44.** *Let $V$ be a vector space such that $V = \text{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$. If $\mathbf{u}_1, \ldots, \mathbf{u}_n \in V$ for some $n > m$, then the vectors $\mathbf{u}_1, \ldots, \mathbf{u}_n$ are linearly dependent.*

**Proof.** Let $\mathbf{u}_1, \ldots, \mathbf{u}_n \in V$ for some $n > m$. Since the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m$ span $V$, there exist scalars $a_{ij}$ such that

$$\mathbf{u}_j = \sum_{i=1}^{m} a_{ij}\mathbf{v}_i = a_{1j}\mathbf{v}_1 + a_{2j}\mathbf{v}_2 + \cdots + a_{mj}\mathbf{v}_m \tag{3.17}$$

for each $1 \le j \le n$.

Now, by Theorem 2.38 the homogeneous system of equations

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \quad\vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases}$$

has a nontrivial solution since $n$ (the number of variables) is greater than $m$ (the number of equations). That is, there exists a solution $(x_1, \ldots, x_n) = (c_1, \ldots, c_n)$ such that not all the scalars $c_j$ are equal to 0.

We now have

$$\sum_{j=1}^{n} a_{ij}c_j = a_{i1}c_1 + \cdots + a_{in}c_n = 0$$

for each $1 \le i \le m$, which implies that

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}c_j\mathbf{v}_i = \sum_{j=1}^{n} a_{1j}c_j\mathbf{v}_1 + \cdots + \sum_{j=1}^{n} a_{mj}c_j\mathbf{v}_m = 0\mathbf{v}_1 + \cdots + 0\mathbf{v}_m = \mathbf{0}. \tag{3.18}$$

But, recalling (3.17), we may also write

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}c_j\mathbf{v}_i = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}c_j\mathbf{v}_i = \sum_{j=1}^{n}\left(c_j\sum_{i=1}^{m} a_{ij}\mathbf{v}_i\right) = \sum_{j=1}^{n} c_j\mathbf{u}_j. \tag{3.19}$$

Combining (3.18) and (3.19), we find that

$$\sum_{j=1}^{n} c_j\mathbf{u}_j = c_1\mathbf{u}_1 + \cdots + c_n\mathbf{u}_n = \mathbf{0}$$

for $c_1, \ldots, c_n$ not all equal to 0.

Therefore $\mathbf{u}_1, \ldots, \mathbf{u}_n$ are linearly dependent. ■

Theorem 3.57 at the end of this section states that every vector space $V$ has a basis, but it leaves open two mutually-exclusive possibilities: either $V$ has a finite basis (i.e. a basis containing a finite number of vectors), or it does not. If $V$ has a finite basis, then it is called a **finite-dimensional** vector space; otherwise it is an **infinite-dimensional** vector space. Note that the trivial vector space $\{\mathbf{0}\}$, which has basis $\varnothing$ by definition, is finite-dimensional.

**Remark.** If a vector space $V$ is finite-dimensional, so that it has a finite basis $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$, then it is an immediate consequence of Proposition 3.44 and the fact that $V = \text{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ that $V$ cannot possess any basis that is infinite. Indeed no set of more than $m$ vectors can even be linearly independent!

While it is usually the case that many different sets of vectors can serve as a basis for a finite-dimensional vector space $V$ (the trivial vector space being the sole exception), it turns out that every basis for a finite-dimensional vector space must contain the same *number* of vectors. In what follows we let $|S|$ denote the number of elements of a set $S$, also known as the **cardinality** of $S$.

**Theorem 3.45.** *If $\mathcal{B}_1$ and $\mathcal{B}_2$ are two bases for a finite-dimensional vector space $V$, then $|\mathcal{B}_1| = |\mathcal{B}_2|$.*

**Proof.** The remark made above makes clear that $\mathcal{B}_1$ and $\mathcal{B}_2$ must both be finite sets, so $\mathcal{B}_1 = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ and $\mathcal{B}_2 = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ for integers $m$ and $n$, and we have $|\mathcal{B}_1| = m$ and $|\mathcal{B}_2| = n$.

Since $\text{Span}(\mathcal{B}_1) = V$, if $n > m$ then $\mathbf{u}_1, \ldots, \mathbf{u}_n$ must be linearly dependent by Proposition 3.44, which contradicts the hypothesis that $\mathcal{B}_2$ is a basis for $V$. Hence $n \leq m$.

Since $\text{Span}(\mathcal{B}_2) = V$, if $n < m$ then $\mathbf{v}_1, \ldots, \mathbf{v}_m$ must be linearly dependent by Proposition 3.44, which contradicts the hypothesis that $\mathcal{B}_1$ is a basis for $V$. Hence $n \geq m$.

Therefore $m = n$, which is to say $|\mathcal{B}_1| = |\mathcal{B}_2|$. ■

Throughout these notes, if a vector space is not said to be finite-dimensional, then it can be assumed to be either finite- or infinite-dimensional. It is the fact that the cardinality of all the bases of a given finite-dimensional vector space is a constant that allows us to make the following definition.

**Definition 3.46.** *The **dimension** of a finite-dimensional vector space $V$, $\dim(V)$, is the number of elements in any basis for $V$. That is, if $\mathcal{B}$ is a basis for $V$, then $\dim(V) = |\mathcal{B}|$.*

**Remark.** Since the basis for the trivial vector space $\{\mathbf{0}\}$ is $\varnothing$ by Definition 3.40, it follows that the dimension of $\{\mathbf{0}\}$ is $|\varnothing| = 0$. If a vector space $V$ is infinite-dimensional then we might be tempted to write $\dim(V) = \infty$, but there is little use in doing this since there are in fact different "sizes" of infinity. We will not make a study of such matters in these notes, for it is more properly the domain of a book on the subject of functional analysis.

**Example 3.47.** A basis for the vector space $\mathbb{R}^2$ is $\mathcal{E}_2 = \{\mathbf{e}_1, \mathbf{e}_2\}$, where

$$\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Since there are two elements in the set we conclude that $\dim(\mathbb{R}^2) = 2$.

More generally, as we have seen, a basis for $\mathbb{R}^n$ is provided by the set

$$\mathcal{E}_n = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$$

of standard unit vectors. Since $|\mathcal{E}_n| = n$, we see that $\dim(\mathbb{R}^n) = n$.

**Example 3.48.** The vector space $\mathbb{R}^{m\times n}$ of $m \times n$ matrices with real-valued entries has as a basis the set

$$\mathcal{E}_{mn} = \{\mathbf{E}_{ij} : 1 \le i \le m, 1 \le j \le n\},$$

where $\mathbf{E}_{ij}$ is the $m \times n$ matrix with $ij$-entry 1 and all other entries 0. There are $mn$ elements in $\mathcal{E}_{mn}$, and thus $\dim(\mathbb{R}^{m\times n}) = mn$.

**Example 3.49.** Example 3.13 showed that $\text{Skw}_n(\mathbb{R})$ is a subspace of $\mathbb{R}^{n\times n}$, and thus is a vector space over $\mathbb{R}$ in its own right. The goal now is to find the dimension of $\text{Skw}_n(\mathbb{R})$. The first thing to notice is that the diagonal entries of any skew-symmetric matrix $\mathbf{A} = [a_{ij}]$ must all be zero:

$$\mathbf{A}^\top = -\mathbf{A} \quad\Rightarrow\quad a_{ii} = -a_{ii} \quad\Rightarrow\quad a_{ii} = 0.$$

So, in the case when $n = 2$, we must have

$$\mathbf{A} = \begin{bmatrix} 0 & a \\ -a & 0 \end{bmatrix}$$

for some $a \in \mathbb{R}$, which is to say

$$\text{Skw}_2(\mathbb{R}) = \left\{ \begin{bmatrix} 0 & a \\ -a & 0 \end{bmatrix} : a \in \mathbb{R} \right\} = \left\{ a\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} : a \in \mathbb{R} \right\} = \text{Span}\left( \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right).$$

Thus we see that the set

$$\mathcal{B}_2 = \left\{ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\} = \{\mathbf{E}_{2,12} - \mathbf{E}_{2,21}\}$$

spans $\text{Skw}_2(\mathbb{R})$, where the definitions of the matrices $\mathbf{E}_{2,12}$ and $\mathbf{E}_{2,21}$ are given by Equation (2.14). Since $\mathcal{B}_2$ is a linearly independent set it follows that $\mathcal{B}_2$ is a basis for $\text{Skw}_2(\mathbb{R})$, and therefore $\dim(\text{Skw}_2(\mathbb{R})) = |\mathcal{B}_2| = 1$.

When $n = 3$ we find that

$$\begin{aligned}
\text{Skw}_3(\mathbb{R}) &= \left\{ \begin{bmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{bmatrix} : a, b, c \in \mathbb{R} \right\} \\
&= \left\{ a\begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + b\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix} + c\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} : a, b, c \in \mathbb{R} \right\} \\
&= \text{Span}\left( \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} \right) \\
&= \text{Span}\left( \{\mathbf{E}_{3,12} - \mathbf{E}_{3,21},\ \mathbf{E}_{3,13} - \mathbf{E}_{3,31},\ \mathbf{E}_{3,23} - \mathbf{E}_{3,32}\} \right).
\end{aligned}$$

The set

$$\mathcal{B}_3 = \{\mathbf{E}_{3,12} - \mathbf{E}_{3,21},\ \mathbf{E}_{3,13} - \mathbf{E}_{3,31},\ \mathbf{E}_{3,23} - \mathbf{E}_{3,32}\}$$

is linearly independent, and so $\dim(\mathrm{Skw}_3(\mathbb{R})) = 3$.

More generally, for arbitrary $n \in \mathbb{N}$, we find $\mathbf{A} = [a_{ij}]_n$ is such that $a_{ii} = 0$ for $1 \leq i \leq n$, and $a_{ij} = -a_{ji}$ whenever $i \neq j$. Thus the entries of $\mathbf{A}$ are fully determined by just the entries above the main diagonal, since each entry below the diagonal must be the negative of the corresponding entry above the diagonal. The entries above the diagonal are $a_{ij}$ for $1 \leq i < j \leq n$, and it is straightforward to check that

$$\mathcal{B}_n = \{\mathbf{E}_{n,ij} - \mathbf{E}_{n,ji} : 1 \leq i < j \leq n\}$$

is a linearly independent set such that

$$\mathrm{Skw}_n(\mathbb{R}) = \mathrm{Span}\left(\{\mathbf{E}_{n,ij} - \mathbf{E}_{n,ji} : 1 \leq i < j \leq n\}\right),$$

and so

$$\dim(\mathrm{Skw}_n(\mathbb{R})) = |\mathcal{B}_n| = (n-1) + (n-2) + \cdots + 1 = \sum_{k=1}^{n-1} k = \frac{n(n-1)}{2}.$$

This is just the number of entries in an $n \times n$ matrix that are above the main diagonal. ■

**Definition 3.50.** *Let $V$ be a vector space and $A \subseteq V$ a nonempty set. We call $B \subseteq A$ a **maximal subset of linearly independent vectors** if the following are true:*

1. *$B$ is a linearly independent set.*
2. *For all $S \subseteq A$ with $|S| > |B|$, $S$ is a linearly dependent set.*

Thus if $B \subseteq A$ is a maximal subset of linearly independent vectors and $|B| = r$, then there exist $r$ linearly independent vectors in $A$, but there cannot be found $r + 1$ linearly independent vectors in $A$. It may be that only one combination of $r$ vectors in $A$ can be used to construct the set $B$, or there may be many different possible combinations.

**Theorem 3.51.** *Let $V$ be a vector space, and let $A = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subseteq V$ be such that $V = \mathrm{Span}(A)$. Then*

1. *The dimension of $V$ is at most $n$: $\dim(V) \leq n$.*
2. *If $B \subseteq A$ is a maximal subset of linearly independent vectors, then $B$ is a basis for $V$.*

**Proof.**

*Proof of Part (1).* By Proposition 3.44 any set containing more than $n$ vectors in $V$ must be linearly dependent, so if $\mathcal{B}$ is a basis for $V$, then we must have $\dim(V) = |\mathcal{B}| \leq n$.

*Proof of Part (2).* Suppose that $B \subseteq A$ is a maximal subset of linearly independent vectors. Reindexing the elements of $A$ if necessary, we may assume that $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$. If $r = n$, then $B = A$, and so $B$ spans $V$ and we straightaway conclude that $B$ is a basis for $V$ and we're done. Suppose, then, that $1 \leq r < n$. For each $1 \leq i \leq n - r$ let

$$B_i = B \cup \{\mathbf{v}_{r+i}\} = \{\mathbf{v}_1, \ldots, \mathbf{v}_r, \mathbf{v}_{r+i}\}.$$

The set $B_i$ is linearly dependent since $|B_i| > |B|$, and so there exist scalars $a_{i1}, \ldots, a_{ir}, b_i$, not all zero, such that

$$a_{i1}\mathbf{v}_1 + \cdots + a_{ir}\mathbf{v}_r + b_i\mathbf{v}_{r+i} = \mathbf{0}. \tag{3.20}$$

We must have $b_i \neq 0$, since otherwise (3.20) becomes

$$a_{i1}\mathbf{v}_1 + \cdots + a_{ir}\mathbf{v}_r = \mathbf{0},$$

whereupon the linear independence of $\mathbf{v}_1, \ldots, \mathbf{v}_r$ would imply that $a_{i1} = \cdots = a_{ir} = 0$ and so contradict the established fact that not all the scalars $a_{i1}, \ldots, a_{ir}, b_i$ are zero! From the knowledge that $b_i \neq 0$ we may write (3.20) as

$$\mathbf{v}_{r+i} = -\frac{a_{i1}}{b_i}\mathbf{v}_1 - \cdots - \frac{a_{ir}}{b_i}\mathbf{v}_r = \sum_{j=1}^{r} \frac{a_{ij}}{-b_i}\mathbf{v}_j = \sum_{j=1}^{r} d_{ij}\mathbf{v}_j, \tag{3.21}$$

where we define $d_{ij} = -a_{ij}/b_i$ for each $1 \leq i \leq n-r$ and $1 \leq j \leq r$. Hence the vectors $\mathbf{v}_{r+1}, \ldots, \mathbf{v}_n$ are each expressible as a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_r$.

Let $\mathbf{u} \in V$ be arbitrary. Since $\mathbf{v}_1, \ldots, \mathbf{v}_n$ span $V$ there exist scalars $c_1, \ldots, c_n$ such that

$$\mathbf{u} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n,$$

and then from (3.21) we have

$$\begin{aligned}
\mathbf{u} &= c_1\mathbf{v}_1 + \cdots + c_r\mathbf{v}_r + \sum_{i=1}^{n-r} c_{r+i}\mathbf{v}_{r+i} = \sum_{j=1}^{r} c_j\mathbf{v}_j + \sum_{i=1}^{n-r}\left(c_{r+i}\sum_{j=1}^{r} d_{ij}\mathbf{v}_j\right) \\
&= \sum_{j=1}^{r} c_j\mathbf{v}_j + \sum_{i=1}^{n-r}\sum_{j=1}^{r} c_{r+i}d_{ij}\mathbf{v}_j = \sum_{j=1}^{r} c_j\mathbf{v}_j + \sum_{j=1}^{r}\sum_{i=1}^{n-r} c_{r+i}d_{ij}\mathbf{v}_j \\
&= \sum_{j=1}^{r}\left(c_j\mathbf{v}_j + \sum_{i=1}^{n-r} c_{r+i}d_{ij}\mathbf{v}_j\right) = \sum_{j=1}^{r}\left(c_j + \sum_{i=1}^{n-r} c_{r+i}d_{ij}\right)\mathbf{v}_j.
\end{aligned}$$

Setting

$$\hat{c}_j = c_j + \sum_{i=1}^{n-r} c_{r+i}d_{ij}$$

for each $1 \leq j \leq r$, we finally obtain

$$\mathbf{u} = \hat{c}_1\mathbf{v}_1 + \cdots + \hat{c}_r\mathbf{v}_r$$

and so conclude that $\mathbf{u} \in \operatorname{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_r\} = \operatorname{Span}(B)$.

Therefore $V = \operatorname{Span}(B)$, and so $B$ is a basis for $V$. ∎

Closely related to the concept of a maximal subset of linearly independent vectors is the following.

**Definition 3.52.** *Let $V$ be a vector space. A set $B \subseteq V$ is a* ***maximal set of linearly independent vectors*** *in $V$ if the following are true:*

1. *$B$ is a linearly independent set.*
2. *For all $\mathbf{w} \in V$ such that $\mathbf{w} \notin B$, the set $B \cup \{\mathbf{w}\}$ is linearly dependent.*

**Theorem 3.53.** *If $V$ is a vector space and $S$ a maximal set of linearly independent vectors in $V$, then $S$ is a basis for $V$.*

**Proof.** Suppose that $V$ is a vector space and $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a maximal set of linearly independent vectors. Let $\mathbf{u} \in V$. Then the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{u}\}$ is linearly dependent, and so there exist scalars $c_0, \ldots, c_n$ not all zero such that

$$c_0\mathbf{u} + c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = \mathbf{0}. \tag{3.22}$$

Now, if $c_0$ were 0 we would obtain $c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n = \mathbf{0}$, whereupon the linear independence of $S$ would imply that $c_1 = \cdots = c_n = 0$ and so contradict the established fact that not all the scalars $c_0, \ldots, c_n$ are zero. Hence we must have $c_0 \neq 0$, and (3.22) gives

$$\mathbf{u} = -\frac{c_1}{c_0}\mathbf{v}_1 - \cdots - \frac{c_n}{c_0}\mathbf{v}_n.$$

That is, every vector in $V$ is expressible as a linear combination of vectors in $S$, so that $\text{Span}(S) = V$ and we conclude that $S$ is a basis for $V$. ■

**Theorem 3.54.** *Let $V$ be a finite-dimensional vector space, and let $S \subseteq V$ with $|S| = \dim(V)$.*

1. *If $S$ is a linearly independent set, then $S$ is a basis for $V$.*
2. *If $\text{Span}(S) = V$, then $S$ is a basis for $V$.*

**Proof.**
*Proof of Part (1).* Setting $n = \dim(V)$, suppose $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subseteq V$ is a linearly independent set. Any basis for $V$ will span $V$ and have $n$ vectors, so by Proposition 3.44 the set $S \cup \{\mathbf{w}\}$ must be linearly dependent for every $\mathbf{w} \in V$ such that $\mathbf{w} \notin S$. Hence $S$ is a maximal set of linearly independent vectors, and therefore $S$ is a basis for $V$ by Theorem 3.53.

*Proof of Part (2).* Again set $n = \dim(V)$, and suppose $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is such that $\text{Span}(S) = V$. Assume $S$ is not a basis for $V$. Then $S$ must not be a linearly independent set. Let $B \subseteq S$ be a maximal subset of linearly independent vectors. Then $B$ cannot contain all of the vectors in $S$, so $|B| < |S| = n$. By Theorem 3.51(2) it follows that $B$ is a basis for $V$, and so

$$\dim(V) = |B| < n.$$

Since this is a contradiction, we conclude that $S$ must be a linearly independent set and therefore $S$ is a basis for $V$. ■

**Theorem 3.55.** *Let $V$ be a vector space with $\dim(V) = n > 0$. If $\mathbf{v}_1, \ldots, \mathbf{v}_r \in V$ are linearly independent vectors for some $r < n$, then vectors $\mathbf{v}_{r+1}, \ldots, \mathbf{v}_n \in V$ may be found such that $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis for $V$.*

**Proof.** Suppose that $\mathbf{v}_1, \ldots, \mathbf{v}_r \in V$ are linearly independent vectors, where $r < n$. The set $S_r = \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ cannot be a basis for $V$ since by Definition 3.46 any basis for $V$ must contain $n$ vectors. Hence $S_r$ cannot be a maximal set of linearly independent vectors by Theorem 3.53, and so there must exist some vector $\mathbf{v}_{r+1} \in V$ such that the set

$$S_{r+1} = S_r \cup \{\mathbf{v}_{r+1}\} = \{\mathbf{v}_1, \ldots, \mathbf{v}_{r+1}\}$$

is linearly independent. Now, if $r+1=n$, then Theorem 3.54 implies that $S_{r+1}$ is a basis for $V$ and the proof is done. If $r+1<n$, then we repeat the arguments made above to obtain successive sets of linearly independent vectors

$$S_{r+i} = S_{r+i-1} \cup \{\mathbf{v}_{r+i}\} = \{\mathbf{v}_1, \ldots, \mathbf{v}_{r+i}\}$$

until such time that $r+i=n$, at which point the linearly independent set

$$S_n = S_{n-1} \cup \{\mathbf{v}_n\} = \{\mathbf{v}_1, \ldots, \mathbf{v}_r, \mathbf{v}_{r+1}, \ldots, \mathbf{v}_n\}$$

will be a basis for $V$. ■

**Theorem 3.56.** *Let $V$ be a finite-dimensional vector space, and let $W$ be a subspace of $V$. Then*

1. *$W$ is finite-dimensional.*
2. $\dim(W) \leq \dim(V)$.
3. *If* $\dim(W) = \dim(V)$*, then* $W = V$.

**Proof.** If $W = \{\mathbf{0}\}$, then all three conclusions of the theorem follow trivially. Thus, we will henceforth assume $W \neq \{\mathbf{0}\}$, so that $\dim(V) = n \geq 1$.

*Proof of Part (1).* Suppose $W$ is infinite-dimensional. Let $\mathbf{w}_1$ be a nonzero vector in $W$. The set $\{\mathbf{w}_1\}$ cannot be a maximal set of linearly independent vectors in $W$ since otherwise Theorem 3.53 would imply that $\{\mathbf{w}_1\}$ is a basis for $W$ and hence $\dim(W) = 1$, a contradiction. Thus for some $k \geq 2$ additional vectors $\mathbf{w}_2, \ldots, \mathbf{w}_k \in W$ may be found such that $S_k = \{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ is a linearly independent set of vectors in $W$. However, for no $k \in \mathbb{N}$ can $S_k$ be a maximal set of linearly independent vectors in $W$, since otherwise Theorem 3.53 would imply that $\dim(W) = k$. It follows that there exists, in particular, a linearly independent set

$$\{\mathbf{w}_1, \ldots, \mathbf{w}_{n+1}\} \subseteq W \subseteq V,$$

which is impossible since by Proposition 3.44 there can be no linearly independent set in $V$ containing more than $n$ vectors. Therefore $W$ must be finite-dimensional.

*Proof of Part (2).* By Part (1) it is known that $W$ is finite-dimensional, so there exists a basis $\mathcal{B} = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ for $W$, where $m \in \mathbb{N}$. Since $\mathcal{B}$ is a linearly independent set in $V$, and by Proposition 3.44 there can be no linearly independent set in $V$ containing more than $\dim(V) = n$ vectors, it follows that $\dim(W) = m \leq n = \dim(V)$.

*Proof of Part (3).* Suppose that $\dim(W) = \dim(V) = n$, where $n$ is some integer since $V$ is given to be finite-dimensional. Let $\mathcal{B} = \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ be a basis for $W$, so that $W = \operatorname{Span}(\mathcal{B})$. Since $\dim(V) = n$ and $\mathbf{w}_1, \ldots, \mathbf{w}_n \in V$ are linearly independent, $\mathcal{B}$ is a basis for $V$ by Theorem 3.54. Thus $V = \operatorname{Span}(\mathcal{B})$, and we have $V = W$. ■

Given a matrix $\mathbf{A} \in \mathbb{F}^{m \times n}$, recall from §3.1 that the set of all $\mathbf{x} \in \mathbb{F}^n$ for which $\mathbf{A}\mathbf{x} = \mathbf{0}$ is true is a subspace of $\mathbb{F}^n$ called the **null space** of $\mathbf{A}$, denoted by $\operatorname{Nul}(\mathbf{A})$. Later on we will frequently be concerned with determining the dimension of $\operatorname{Nul}(\mathbf{A})$, which we will often refer to as the **nullity** of $\mathbf{A}$. That is,

$$\operatorname{nullity}(\mathbf{A}) = \dim(\operatorname{Nul}(\mathbf{A})).$$

**Theorem 3.57.** *Every vector space has a basis.*

**Proof.** Let $V$ be a vector space over a field $\mathbb{F}$. By definition $\varnothing$ is the basis for $\{\mathbf{0}\}$, so assume that $V$ is nontrivial. Let $\mathcal{S}$ be the collection of all linearly independent subsets of $V$:

$$\mathcal{S} = \{A \subseteq V : A \text{ is a linearly independent set}\}.$$

(Note that $\mathcal{S}$ contains at least one singleton $\{\mathbf{v}\}$ with $\mathbf{v} \neq \mathbf{0}$ since $V$ is nontrivial.) Then $\mathcal{S}$ is a nonempty partially ordered set under the inclusion relation $\subseteq$. Let $\mathcal{C} \subseteq \mathcal{S}$ be a chain in $\mathcal{S}$. We have $\mathcal{C} = \{C_i : i \in I\}$ for some index set $I$, and for every $A, B \in \mathcal{C}$ either $A \subseteq B$ or $B \subseteq A$. Claim:

$$U = \bigcup_{i \in I} C_i$$

is an upper bound for the chain $\mathcal{C}$ such that $U \in \mathcal{S}$. It is clear that $C_i \subseteq U$ for all $i \in I$. Suppose that $U \notin \mathcal{S}$, which is to say $U$ is not a linearly independent set in $V$. This implies that, for some $n \in \mathbb{N}$, there exist $\mathbf{u}_1, \dots, \mathbf{u}_n \in U$ such that $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ is linearly dependent, which in turn implies that for each $1 \leq k \leq n$ there is some $i_k \in I$ with $\mathbf{u}_k \in C_{i_k}$. For convenience we may assume the vectors $\mathbf{u}_1, \dots, \mathbf{u}_n$ are indexed such that

$$C_{i_1} \subseteq C_{i_2} \subseteq \cdots \subseteq C_{i_n},$$

recalling that each $C_{i_k}$ is an element of the totally ordered set $\mathcal{C}$. Thus $\mathbf{u}_1, \dots, \mathbf{u}_n \in C_{i_n}$, which shows that $C_{i_n}$ is not a linearly independent set and hence $C_{i_n} \notin \mathcal{S}$—a contradiction. We conclude that $U$ must be a linearly independent set, and hence $U$ is an upper bound for $\mathcal{C}$ with $U \in \mathcal{S}$. Since every chain in $\mathcal{S}$ has an upper bound in $\mathcal{S}$, Zorn's Lemma implies that $\mathcal{S}$ has a maximal element $M$.

Let $\mathbf{v} \in V$ be arbitrary. Suppose, for all $n \in \mathbb{N}$ (or $1 \leq n \leq |M|$ if $M$ is finite) and $\mathbf{v}_1, \dots, \mathbf{v}_n \in M$, the only $r_1, \dots, r_n, r \in \mathbb{F}$ that satisfy the equation

$$\sum_{k=1}^{n} r_k \mathbf{v}_k + r\mathbf{v} = \mathbf{0} \tag{3.23}$$

are $r_1 = \cdots = r_n = r = 0$. Then $M \cup \{\mathbf{v}\}$ is a linearly independent set, which implies that $M \cup \{\mathbf{v}\} \in \mathcal{S}$. Since $M \subseteq M \cup \{\mathbf{v}\}$ and $M$ is a maximal element of $\mathcal{S}$, we must have $M = M \cup \{\mathbf{v}\}$ and therefore $\mathbf{v} \in M$. In particular we see that $\mathbf{v} \in \mathrm{Span}(M)$.

Suppose, in contrast, that for some $n \in \mathbb{N}$ and $\mathbf{v}_1, \dots, \mathbf{v}_n \in M$ the equation (3.23) admits a nontrivial solution. Since $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent this means we must have $r \neq 0$ (otherwise we are forced to embrace the trivial solution). Since $\mathbb{F}$ is a field there exists some $r^{-1} \in \mathbb{F}$ such that $r^{-1}r = 1$. Hence

$$r\mathbf{v} = -\sum_{k=1}^{n} r_k \mathbf{v}_k \quad \Rightarrow \quad \mathbf{v} = r^{-1} \sum_{k=1}^{n} r_k \mathbf{v}_k = \sum_{k=1}^{n} (r^{-1} r_k) \mathbf{v}_k,$$

and we see that $\mathbf{v} \in \mathrm{Span}(M)$ once more. Thus $V = \mathrm{Span}(M)$, and since $M$ is a linearly independent set we conclude that $M$ is a basis for $V$. ∎

## Problems

1. Find the dimension of $\mathcal{P}_3(\mathbb{R})$, the vector space over $\mathbb{R}$ of polynomials in $x$ of degree at most 3 with real coefficients.

2. Recall that $\mathrm{Sym}_n(\mathbb{R})$ denotes the vector space of $n \times n$ symmetric matrices over $\mathbb{R}$.
   (a) Find a basis for $\mathrm{Sym}_2(\mathbb{R})$. What is the dimension of $\mathrm{Sym}_2(\mathbb{R})$?
   (b) Find a basis for $\mathrm{Sym}_3(\mathbb{R})$. What is the dimension of $\mathrm{Sym}_3(\mathbb{R})$?
   (c) Find a basis for $\mathrm{Sym}_4(\mathbb{R})$. What is the dimension of $\mathrm{Sym}_4(\mathbb{R})$?
   (d) Find a basis for $\mathrm{Sym}_n(\mathbb{R})$. What is the dimension of $\mathrm{Sym}_n(\mathbb{R})$?

## 3.7 – Product Spaces

**Definition 3.58.** *Let $U$ and $V$ be vector spaces over $\mathbb{F}$. The **product** of $U$ and $V$ is the set*

$$U \times V = \{(\mathbf{u}, \mathbf{v}) : \mathbf{u} \in U, \mathbf{v} \in V\}.$$

*More generally, let $V_1, \ldots, V_n$ be vector spaces over $\mathbb{F}$. The **product** of $V_1, \ldots, V_n$ is the set*

$$\prod_{k=1}^{n} V_k = \{(\mathbf{v}_1, \ldots, \mathbf{v}_n) : \mathbf{v}_k \in V_k \text{ for each } 1 \leq k \leq n\}$$

We see that the product of two or more vector spaces amounts to nothing more than the Cartesian product of the sets of objects contained within the vector spaces. Let

$$\mathfrak{u}, \mathfrak{v} \in \prod_{k=1}^{n} V_k$$

be the $n$-tuples

$$\mathfrak{u} = (\mathbf{u}_1, \ldots, \mathbf{u}_n) \quad \text{and} \quad \mathfrak{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_n),$$

and let $c \in \mathbb{F}$. If we define the **sum** of $\mathfrak{u}$ and $\mathfrak{v}$ by

$$\mathfrak{u} + \mathfrak{v} = (\mathbf{u}_1 + \mathbf{v}_1, \ldots, \mathbf{u}_n + \mathbf{v}_n),$$

and the **scalar product** of $c$ with $\mathfrak{v}$ by

$$c\mathfrak{v} = (c\mathbf{v}_1, \ldots, c\mathbf{v}_n),$$

then it is a routine matter to verify that $\prod_{k=1}^{n} V_k$ becomes a vector space in its own right, called the **product space** of $V_1, \ldots, V_n$.

## 3.8 – The Rank of a Matrix

Let $\mathbf{A} \in \mathbb{F}^{m\times n}$, so that

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}. \tag{3.24}$$

Denote the column vectors of $\mathbf{A}$ by

$$\mathbf{c}_j = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix}$$

for $1 \leq j \leq n$, and denote the row vectors of $\mathbf{A}$ by

$$\mathbf{r}_i = \begin{bmatrix} a_{i1} & \ldots & a_{in} \end{bmatrix}$$

for $1 \leq i \leq m$. The **column space** of $\mathbf{A}$ is defined to be the set

$$\text{Col}(\mathbf{A}) = \text{Span}\{\mathbf{c}_1, \ldots, \mathbf{c}_n\},$$

and the **row space** of $\mathbf{A}$ is defined to be the set

$$\text{Row}(\mathbf{A}) = \text{Span}\{\mathbf{r}_1^\top, \ldots, \mathbf{r}_m^\top\}.$$

Proposition 3.30 implies that $\text{Col}(\mathbf{A})$ is a subspace of $\mathbb{F}^m$ and $\text{Row}(\mathbf{A})$ is a subspace of $\mathbb{F}^n$. The **column rank** of $\mathbf{A}$ is the dimension of the column space of $\mathbf{A}$:

$$\text{col-rank}(\mathbf{A}) = \dim[\text{Col}(\mathbf{A})].$$

The **row rank** of $\mathbf{A}$ is the dimension of the row space:

$$\text{row-rank}(\mathbf{A}) = \dim[\text{Row}(\mathbf{A})].$$

**Proposition 3.59.** *Let $\mathbf{A} \in \mathbb{F}^{m\times n}$, with $\mathbf{c}_1, \ldots, \mathbf{c}_n \in \mathbb{F}^m$ the column vectors of $\mathbf{A}$ and $\mathbf{r}_1, \ldots, \mathbf{r}_m \in \mathbb{F}^n$ the row vectors of $\mathbf{A}$.*

1. *If $S \subseteq \{\mathbf{c}_1, \ldots, \mathbf{c}_n\}$ is a maximal subset of linearly independent vectors, then*

$$\text{col-rank}(\mathbf{A}) = |S|.$$

2. *If $S \subseteq \{\mathbf{r}_1, \ldots, \mathbf{r}_m\}$ is a maximal subset of linearly independent vectors, then*

$$\text{row-rank}(\mathbf{A}) = |S|.$$

**Proof.**

*Proof of Part (1).* Suppose $S \subseteq \{\mathbf{c}_1, \ldots, \mathbf{c}_n\}$ is a maximal subset of linearly independent vectors. Let $\text{col-rank}(\mathbf{A}) = k$. Since $\text{Col}(\mathbf{A})$ is a vector space, $\text{Col}(\mathbf{A}) = \text{Span}\{\mathbf{c}_1, \ldots, \mathbf{c}_n\}$, and $S \subseteq \{\mathbf{c}_1, \ldots, \mathbf{c}_n\}$ is a maximal subset of linearly independent vectors, it follows by Theorem 3.51 that $S$ is a basis for $\text{Col}(\mathbf{A})$. Now, because the dimension of $\text{Col}(\mathbf{A})$ is $k$, we must have $|S| = k = \text{col-rank}(\mathbf{A})$ as was to be shown.

*Proof of Part (2).* Done similarly, and so left as a problem. ■

In the proof of Proposition 3.59(1), since $|S| = \text{col-rank}(\mathbf{A}) = k$, we can conclude that $S$ consists of $k$ elements of the set $\{\mathbf{c}_1, \dots, \mathbf{c}_n\}$, and so we may write $S = \{\mathbf{c}_{n_1}, \dots, \mathbf{c}_{n_k}\}$ for some $n_1, \dots, n_k \in \{1, \dots, n\}$. That is, $\{\mathbf{c}_{n_1}, \dots, \mathbf{c}_{n_k}\}$ is a maximal subset of linearly independent vectors, which is to say the maximum number of linearly independent column vectors of $\mathbf{A}$ is col-rank($\mathbf{A}$).

What we ultimately want to show is that the row and column ranks of a matrix are always equal. It is not an obvious fact, and so a few more results will need to be developed before we are in a position to prove it.

**Lemma 3.60.** *Let $V$ and $W$ be vector spaces, with*

$$S_V = \{\mathbf{v}_1, \dots, \mathbf{v}_n\} \subseteq V \quad \textit{and} \quad S_W = \{\mathbf{w}_1, \dots, \mathbf{w}_n\} \subseteq W.$$

*If*

$$\sum_{k=1}^{n} x_k \mathbf{v}_k = \mathbf{0} \;\Leftrightarrow\; \sum_{k=1}^{n} x_k \mathbf{w}_k = \mathbf{0}$$

*for all $x_1, \dots, x_n \in \mathbb{F}$, then* $\dim(\operatorname{Span} S_V) = \dim(\operatorname{Span} S_W)$.

**Proof.** Suppose that, for all $x_1, \dots, x_n \in \mathbb{F}$, $\sum_{i=1}^n x_i \mathbf{v}_i = \mathbf{0}$ if and only if $\sum_{i=1}^n x_i \mathbf{w}_i = \mathbf{0}$. We shall refer to this hypothesis as (H). Let

$$R_V = \{\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_r}\} \subseteq S_V$$

be a maximal subset of linearly independent vectors for $S_V$, which means any subset of $S_V$ with more than $r$ elements must be linearly dependent. By Theorem 3.51 $R_V$ is a basis for $\operatorname{Span}(S_V)$, and so $\dim(\operatorname{Span} S_V) = |R_V| = r$.

Let $R_W = \{\mathbf{w}_{i_1}, \dots, \mathbf{w}_{i_r}\} \subseteq S_W$. Suppose that

$$x_{i_1} \mathbf{w}_{i_1} + \cdots + x_{i_r} \mathbf{w}_{i_r} = \mathbf{0}.$$

Then by (H) we have

$$x_{i_1} \mathbf{v}_{i_1} + \cdots + x_{i_r} \mathbf{v}_{i_r} = \mathbf{0}$$

as well, and since $\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_r}$ are linearly independent we conclude that $x_{i_1} = \cdots = x_{i_r} = 0$. That is, $\sum_{k=1}^r x_{i_k} \mathbf{w}_{i_k} = \mathbf{0}$ necessarily implies that $x_{i_k} = 0$ for all $1 \le k \le r$, and so $R_W$ is itself a linearly independent set of vectors.

Next, assume $B = \{\mathbf{w}_{j_1}, \dots, \mathbf{w}_{j_t}\} \subseteq S_W$ is such that $|B| = t > r$. Set

$$x_{j_1} \mathbf{v}_{j_1} + \cdots + x_{j_t} \mathbf{v}_{j_t} = \mathbf{0}. \tag{3.25}$$

Since any subset of $S_V$ containing more than $r$ elements must be linearly dependent, it follows that $\mathbf{v}_{j_1}, \dots, \mathbf{v}_{j_t}$ must be linearly dependent and there exist scalars $x_{j_1}, \dots, x_{j_t}$, *not all equal to zero*, which satisfy (3.25). By (H) these same scalars must satisfy

$$x_{j_1} \mathbf{w}_{j_1} + \cdots + x_{j_t} \mathbf{w}_{j_t} = \mathbf{0},$$

which shows that $\mathbf{w}_{j_1}, \dots, \mathbf{w}_{j_t}$ must also be linearly dependent. Hence there does not exist any linearly independent set $B \subseteq S_W$ for which $|B| > r$.

We conclude that $R_W \subseteq S_W$ is a maximal subset of linearly independent vectors. By Theorem 3.51 $R_W$ is a basis for $\operatorname{Span}(S_W)$, and so $\dim(\operatorname{Span} S_W) = |R_W| = r$.

Therefore $\dim(\operatorname{Span} S_V) = r = \dim(\operatorname{Span} S_W)$. ■

**Lemma 3.61.** *Suppose* $\mathbf{A} \in \mathbb{F}^{m\times m}$ *is invertible, and let* $\mathbf{B} \in \mathbb{F}^{m\times n}$. *Then* $\text{col-rank}(\mathbf{AB}) = \text{col-rank}(\mathbf{B})$.

**Proof.** Let $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{F}^m$ be the column vectors of $\mathbf{B}$, so that

$$\mathbf{B} = \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_n \end{bmatrix},$$

and thus by Proposition 2.6

$$\mathbf{AB} = \begin{bmatrix} \mathbf{Ab}_1 & \cdots & \mathbf{Ab}_n \end{bmatrix},$$

where $\mathbf{Ab}_1, \ldots, \mathbf{Ab}_n \in \mathbb{F}^m$. Let $x_1, \ldots, x_n \in \mathbb{F}$. If $\sum_{j=1}^n x_j \mathbf{b}_j = \mathbf{0}$, then by Theorem 2.7 we have

$$\sum_{j=1}^n x_j(\mathbf{Ab}_j) = \sum_{j=1}^n \mathbf{A}(x_j\mathbf{b}_j) = \mathbf{A}\sum_{j=1}^n x_j\mathbf{b}_j = \mathbf{A0} = \mathbf{0};$$

and if $\sum_{j=1}^n x_j(\mathbf{Ab}_j) = \mathbf{0}$, then since $\mathbf{A}$ is invertible we have

$$\sum_{j=1}^n x_j\mathbf{b}_j = \sum_{j=1}^n x_j(\mathbf{A}^{-1}\mathbf{Ab}_j) = \mathbf{A}^{-1}\sum_{j=1}^n x_j(\mathbf{Ab}_j) = \mathbf{A}^{-1}\mathbf{0} = \mathbf{0}.$$

Therefore

$$\text{col-rank}(\mathbf{AB}) = \dim\big(\operatorname{Span}\{\mathbf{Ab}_1, \ldots, \mathbf{Ab}_n\}\big) = \dim\big(\operatorname{Span}\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}\big) = \text{col-rank}(\mathbf{B})$$

by Lemma 3.60. ■

**Proposition 3.62.** *Let* $\mathbf{A} \in \mathbb{F}^{m\times n}$.

1. *If* $\mathbf{A}'$ *row-equivalent to* $\mathbf{A}$, *then*

$$\operatorname{Row}(\mathbf{A}) = \operatorname{Row}(\mathbf{A}') \quad \textit{and} \quad \text{col-rank}(\mathbf{A}) = \text{col-rank}(\mathbf{A}').$$

2. *If* $\mathbf{A}'$ *column-equivalent to* $\mathbf{A}$, *then*

$$\operatorname{Col}(\mathbf{A}) = \operatorname{Col}(\mathbf{A}') \quad \textit{and} \quad \text{row-rank}(\mathbf{A}) = \text{row-rank}(\mathbf{A}')$$

*Thus both* $\text{col-rank}(\mathbf{A})$ *and* $\text{row-rank}(\mathbf{A})$ *are invariant under arbitrary finite sequences of elementary row and column operations applied to* $\mathbf{A}$.

**Proof.**
*Proof of Part (1).* Suppose that $\mathbf{A}'$ is row-equivalent to $\mathbf{A}$. This means there exists a finite sequence of elementary matrices $\mathbf{M}_1, \ldots, \mathbf{M}_k \in \mathbb{F}^{m\times m}$ such that

$$\mathbf{A}' = \mathbf{M}_k \cdots \mathbf{M}_1\mathbf{A}.$$

By Proposition 2.27 each matrix $\mathbf{M}_j$ is invertible, and hence $\mathbf{M} = \mathbf{M}_k \cdots \mathbf{M}_1$ is invertible by Theorem 2.26. Therefore

$$\text{col-rank}(\mathbf{A}) = \text{col-rank}(\mathbf{MA}) = \text{col-rank}(\mathbf{A}')$$

by Lemma 3.61.

To show that $\operatorname{Row}(\mathbf{A}) = \operatorname{Row}(\mathbf{A}')$, it is sufficient to show that $\operatorname{Row}(\mathbf{A})$ is invariant under each one of the three elementary row operations. By Proposition 2.16(1) an R1 operation

$\mathbf{M}_{i,j}(c)\mathbf{A}$ replaces the row vector $\mathbf{a}_j$ of $\mathbf{A}$ by $\mathbf{a}_j + c\mathbf{a}_i$, and thus the row space of the resultant (row-equivalent) matrix is equal to $\text{Row}(\mathbf{A})$ by Proposition 3.31. By Proposition 2.16(2) an R2 operation $\mathbf{M}_{i,j}\mathbf{A}$ merely interchanges two row vectors of $\mathbf{A}$, which clearly does not alter the row space. Finally by Proposition 2.16(3) an R3 operation $\mathbf{M}_i(c)\mathbf{A}$ multiplies the row vector $\mathbf{a}_i$ of $\mathbf{A}$ by the nonzero scalar $c$, and the straightforward formal verification that the row space of the resultant matrix equals $\text{Row}(\mathbf{A})$ is left as a problem.

*Proof of Part (2).* Suppose $\mathbf{A}'$ is column-equivalent to $\mathbf{A}$, so there are elementary matrices $\mathbf{M}_1, \dots, \mathbf{M}_k \in \mathbb{F}^{n\times n}$ such that

$$\mathbf{A}' = \mathbf{A}\mathbf{M}_1^\top \cdots \mathbf{M}_k^\top,$$

and hence (taking the transpose of both sides and applying Proposition 2.13) we have

$$(\mathbf{A}')^\top = \mathbf{M}_k \cdots \mathbf{M}_1\mathbf{A}^\top.$$

Again $\mathbf{M} = \mathbf{M}_k \cdots \mathbf{M}_1$ is invertible, so Lemma 3.61 implies that

$$\text{col-rank}(\mathbf{A}^\top) = \text{col-rank}(\mathbf{M}\mathbf{A}^\top) = \text{col-rank}((\mathbf{A}')^\top).$$

Since the column spaces of $\mathbf{A}^\top$ and $(\mathbf{A}')^\top$ are the row spaces of $\mathbf{A}$ and $\mathbf{A}'$, respectively, we finally obtain $\text{row-rank}(\mathbf{A}) = \text{row-rank}(\mathbf{A}')$.

The proof that $\text{Col}(\mathbf{A}) = \text{Col}(\mathbf{A}')$ is nearly identical to the proof that $\text{Row}(\mathbf{A}) = \text{Row}(\mathbf{A}')$ in part (1), only Proposition 2.17 is employed instead of Proposition 2.16. ■

In brief, elementary row operations do not change the row space of a matrix, and elementary column operations do not change the column space. On the other hand elementary row (resp. column) operations may change the column (resp. row) space of a matrix, but the *dimension* of the column (resp. row) space will remain the same. That is, any elementary row operation may change the span of the column vectors, and any elementary column operation may change the span of the row vectors.

**Example 3.63.** Find a basis for the column space of the matrix

$$\mathbf{A} = \begin{bmatrix} 2 & 0 & 3 & 4 & 1 \\ 0 & 1 & 1 & -1 & 3 \\ 3 & 1 & 0 & 2 & -6 \\ 1 & 0 & -4 & 2 & 1 \end{bmatrix}$$

**Solution.** One way to proceed is to use elementary column operations to put the matrix into row-echelon form.

$$\begin{bmatrix} 2 & 0 & 3 & 4 & 1 \\ 0 & 1 & 1 & -1 & 3 \\ 3 & 1 & 0 & 2 & -6 \\ 1 & 0 & -4 & 2 & 1 \end{bmatrix} \xrightarrow[2c_4+c_3\to c_3]{\frac{1}{2}c_4+c_1\to c_1} \begin{bmatrix} 4 & 0 & 11 & 4 & 1 \\ -\frac{1}{2} & 1 & -1 & -1 & 3 \\ 2 & 1 & 4 & 2 & -6 \\ 0 & 0 & 0 & 2 & 1 \end{bmatrix} \xrightarrow[c_2\leftrightarrow c_3]{-\frac{1}{2}c_3+c_1\to c_1}$$

$$\begin{bmatrix} -\frac{3}{2} & 11 & 0 & 4 & 1 \\ 0 & -1 & 1 & -1 & 3 \\ 0 & 4 & 1 & 2 & -6 \\ 0 & 0 & 0 & 2 & 1 \end{bmatrix} \xrightarrow[-2c_1]{-4c_3+c_2\to c_2} \begin{bmatrix} 3 & 11 & 0 & 4 & 1 \\ 0 & -5 & 1 & -1 & 3 \\ 0 & 0 & 1 & 2 & -6 \\ 0 & 0 & 0 & 2 & 1 \end{bmatrix} \xrightarrow{-2c_5+c_4\to c_4}$$

$$\begin{bmatrix} 3 & 11 & 0 & 2 & 1 \\ 0 & -5 & 1 & -7 & 3 \\ 0 & 0 & 1 & 14 & -6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \mathbf{A}'$$

The first, second, third, and fifth column vectors of the row-echelon matrix $\mathbf{A}'$,

$$\mathbf{c}_1 = \begin{bmatrix} 3 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \mathbf{c}_2 = \begin{bmatrix} 11 \\ -5 \\ 0 \\ 0 \end{bmatrix}, \quad \mathbf{c}_3 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{c}_5 = \begin{bmatrix} 1 \\ 3 \\ -6 \\ 1 \end{bmatrix},$$

contain pivots, and so are linearly independent by Theorem 3.33. Since $\dim(\mathbb{R}^4) = 4$ and $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_5 \in \mathbb{R}^4$ are linearly independent, by Theorem 3.54(1) the set

$$S = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_5\}$$

is a basis for $\mathbb{R}^4$, and so $\mathrm{Span}(S) = \mathbb{R}^4$. By Proposition 3.44 any subset of $\mathbb{R}^4$ containing more vectors than $S$ (i.e. more than four vectors) must be linearly dependent, and therefore $S$ must be a maximal set of linearly independent vectors in $\mathrm{Col}(\mathbf{A}')$ since any vector in $\mathrm{Col}(\mathbf{A}')$ is necessarily a vector in $\mathbb{R}^4$. By Theorem 3.53 we conclude that $S$ is a basis for $\mathrm{Col}(\mathbf{A}')$. Now, because $\mathbf{A}'$ is column-equivalent to $\mathbf{A}$ we have $\mathrm{Col}(\mathbf{A}') = \mathrm{Col}(\mathbf{A})$ by Proposition 3.62. Therefore $S$ is a basis for $\mathrm{Col}(\mathbf{A})$ and we are done. ∎

The next theorem is momentous. It tells us that the column rank of a matrix $\mathbf{A}$ always equals the row rank, so that we may simply refer to the **rank** of $\mathbf{A}$, $\mathrm{rank}(\mathbf{A})$, without discriminating between the column and row spaces. That is,

$$\mathrm{rank}(\mathbf{A}) = \dim(\mathrm{Col}(\mathbf{A})) = \dim(\mathrm{Row}(\mathbf{A})).$$

Also the theorem provides a definitive strategy for determining $\mathrm{rank}(\mathbf{A})$.

**Theorem 3.64.** *If* $\mathbf{A} \in \mathbb{F}^{m\times n}$ *is such that* $\text{row-rank}(\mathbf{A}) = r$*, then* $\mathbf{A}$ *is equivalent via elementary row and column operations to the* $m \times n$ *matrix*

$$\left[\begin{array}{c|c} \mathbf{I}_r & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} \end{array}\right]. \tag{3.26}$$

*Hence* $\text{col-rank}(\mathbf{A}) = \text{row-rank}(\mathbf{A})$.

**Proof.** Suppose $\mathbf{A} \in \mathbb{F}^{m\times n}$ with $\text{row-rank}(\mathbf{A}) = r$. By Proposition 2.20, $\mathbf{A}$ is row-equivalent to a matrix $\mathbf{A}'$ in row-echelon form. Since the nonzero row vectors of $\mathbf{A}'$ are linearly independent and $\text{row-rank}(\mathbf{A}') = r$ by Proposition 3.62, it follows that the top $r$ rows of $\mathbf{A}'$ must be nonzero row vectors while the bottom $m - r$ rows must consist solely of zero entries.

Now, the pivots $p_1, \ldots, p_r$ in the top $r$ rows of $\mathbf{A}'$ are nonzero entries having only zero entries to the left of them. Each nonzero entry $x$ to the right of $p_1$ we may "eliminate" by performing a $\mathsf{C1}$ operation: namely, if $p_1$ is in column $i$ and $x$ is in column $j > i$, then add $-x/p_1$ times column $i$ to column $j$. Since all entries below $p_1$ are zero, this affects no other entries in the matrix beyond replacing the $1j$-entry $x$ with 0. In the end we obtain a matrix in which $p_1$ is the only nonzero entry in its row and column, and we repeat the process for $p_2$, $p_3$, and finally $p_r$. The resultant matrix will have only $p_1, \ldots, p_r$ as nonzero entries, still in their original row-echelon formation. Now we perform $\mathsf{C2}$ operations to make $p_i$ the $ii$-entry for each $1 \le i \le r$. Finally we perform $\mathsf{C3}$ operations: we multiply column $i$ by $1/p_i$ so that the $ii$-entry is 1 for each $1 \le i \le r$, thereby securing the desired matrix (3.26).

The matrix (3.26) clearly has row rank and column rank both equal to $r$, and since the matrix was obtained from $\mathbf{A}$ by applying a finite sequence of elementary row and column operations, Proposition 3.62 implies that the row rank and column rank of $\mathbf{A}$ are likewise both equal to $r$. This finishes the proof. ■

**Example 3.65.** Apply a sequence of elementary row and column operations to

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 3 & 4 \end{bmatrix}$$

to obtain an equivalent matrix of the form (3.26). Show that the row vectors of $\mathbf{A}$ are linearly independent, and that row-rank($\mathbf{A}$) = col-rank($\mathbf{A}$). State the rank of $\mathbf{A}$.

**Solution.** First we will get a matrix in row-echelon form using strictly elementary row operations:

$$\begin{bmatrix} 1 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 3 & 4 \end{bmatrix} \xrightarrow[-2r_1+r_3\to r_3]{-r_1+r_2\to r_2} \begin{bmatrix} 1 & 1 & 2 & 1 \\ 0 & -1 & -1 & 1 \\ 0 & -1 & -1 & 2 \end{bmatrix} \xrightarrow{-r_2+r_3\to r_3} \begin{bmatrix} 1 & 1 & 2 & 1 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Now elementary column operations will be used to first put zeros to the right of the $ii$-entries, and then to obtain a diagonal of 1's:

$$\begin{bmatrix} 1 & 1 & 2 & 1 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[-2c_1+c_3\to c_3]{-c_1+c_2\to c_2} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{-c_1+c_4\to c_4} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{c_3\leftrightarrow c_4}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \xrightarrow[-c_2+c_4\to c_4]{c_2+c_3\to c_3} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \xrightarrow{-c_2} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

The row vectors of the final matrix are $[1,0,0,0]$, $[0,1,0,0]$, and $[0,0,1,0]$, which are linearly independent, and so the row rank is 3. By Proposition 3.62 it follows that row-rank($\mathbf{A}$) = 3 as well, and therefore the row vectors of $\mathbf{A}$ must be linearly independent by Theorem 3.54(2). The nonzero column vectors of the final matrix are $[1,0,0]^\top$, $[0,1,0]^\top$, and $[0,0,1]^\top$, which are linearly independent, and so col-rank($\mathbf{A}$) = 3 by Proposition 3.62. Thus we have

$$\text{row-rank}(\mathbf{A}) = \text{col-rank}(\mathbf{A}) = 3,$$

and therefore rank($\mathbf{A}$) = 3. ■

In Example 3.65 it should be noted that rank($\mathbf{A}$) could have been determined rather easily early on, right after performing the $\mathsf{R1}$ row operation $-r_2 + r_3 \to r_3$. The row vectors at that stage were $[1, 1, 2, 1]$, $[0, -1, -1, 1]$, and $[0, 0, 0, 1]$, which can be seen to be linearly independent on account of the placement of the zeros. Thus $\text{rank}(\mathbf{A}) = \text{row-rank}(\mathbf{A}) = 3$.

With our definition of rank in hand, the findings of Proposition 3.62 and Theorem 3.64 combine to yield the following result.

**Theorem 3.66.** *If* $\mathbf{A}$ *is row-equivalent or column-equivalent to* $\mathbf{A}'$, *then* $\text{rank}(\mathbf{A}) = \text{rank}(\mathbf{A}')$.

The next example makes use of a variety of results developed throughout this chapter. What once may have required much tedious calculation now can be accomplished quickly and elegantly.

**Example 3.67.** Let

$$\mathbf{v}_1 = \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} \quad \text{and} \quad \mathbf{v}_2 = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}.$$

Show that $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2\}$ is a basis for the vector space $W \subseteq \mathbb{R}^3$ given by

$$W = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \,\middle|\, x - 2y + 3z = 0 \right\}.$$

**Solution.** Define the matrix

$$\mathbf{B} = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 1 & 2 \\ 1 & 1 \end{bmatrix},$$

and consider the first two row vectors $[a, b] = [-1, 1]$ and $[c, d] = [1, 2]$. Since

$$ad - bc = (-1)(2) - (1)(1) = -3 \neq 0,$$

these row vectors of $\mathbf{B}$ are linearly independent by Proposition 3.42, and so $\text{row-rank}(\mathbf{B}) \geq 2$. On the other hand $\mathbf{B}$ has only two columns, so $\text{col-rank}(\mathbf{B}) \leq 2$. Hence, by Theorem 3.64,

$$2 \leq \text{row-rank}(\mathbf{B}) = \text{rank}(\mathbf{B}) = \text{col-rank}(\mathbf{B}) \leq 2,$$

which implies that $\text{rank}(\mathbf{B}) = 2$. Since $\mathbf{v}_1$ and $\mathbf{v}_2$ are the column vectors of $\mathbf{B}$, it follows that $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent.

It is easily verified that $\mathbf{v}_1, \mathbf{v}_2 \in W$, so that $S = \text{Span}(\mathcal{B})$ is a subspace of $W$ and thus $\dim(S) \leq \dim(W)$ by Theorem 3.56(2). Since $\mathcal{B}$ is a basis for $S$, we have $\dim(S) = 2$; and since

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \notin W,$$

so that $W$ is a subspace of $\mathbb{R}^3$ that does not equal $\mathbb{R}^3$, it follows by Theorem 3.56 that

$$\dim(W) < \dim(\mathbb{R}^3) = 3.$$

That is,

$$2 = \dim(S) \leq \dim(W) \leq 2,$$

which shows that $\dim(W) = 2$, and therefore $\mathcal{B}$ is a basis for $W$ by Theorem 3.54(1). ■

## Problems

1. For any matrix $\mathbf{A}$ show that $\operatorname{Col}(\mathbf{A}) = \operatorname{Row}(\mathbf{A}^\top)$ and $\operatorname{Row}(\mathbf{A}) = \operatorname{Col}(\mathbf{A}^\top)$.

2. Show that $\operatorname{rank}(\mathbf{A}) = \operatorname{rank}(\mathbf{A}^\top)$ for any matrix $\mathbf{A}$.

3. Let $\mathbf{A} \in \mathbb{F}^{m\times n}$ and $\mathbf{B} \in \mathbb{F}^{n\times p}$.
   (a) Show that $\operatorname{rank}(\mathbf{AB}) \leq \operatorname{rank}(\mathbf{A})$.
   (b) Show that $\operatorname{rank}(\mathbf{AB}) \leq \operatorname{rank}(\mathbf{B})$.

# 4

# Linear Mappings

## 4.1 – Linear Mappings

A **mapping** (or **transformation**) is nothing more than a function, but usually a function between sets that have some additional structure such as a vector space. We have encountered mappings already in the definition of a vector space $V$: namely the scalar multiplication and vector addition functions, whose ranges both consist of elements of $V$. As with functions in general, to say a mapping $T$ **maps** a set $X$ into a set $Y$, written $T : X \to Y$, means that $T$ maps each object $x \in X$ to a unique object $y \in Y$. We denote this by writing $T(x) = y$, or sometimes $Tx = y$, and call $X$ the **domain** of $T$ and $Y$ the **codomain**. A little more formally a mapping $T$ is a set of ordered pairs $(x, y) \in X \times Y$ with the property that

$$\forall x \in X\big[\exists y \in Y\big(((x,y) \in T) \wedge (\hat{y} \neq y \to (x,\hat{y}) \notin T)\big)\big].$$

We call $T(x)$ the **value of $T$ at $x$**. Given any set $A \subseteq X$, we define the **image of $A$ under $T$** to be the set

$$T(A) = \{T(x) : x \in A\} \subseteq Y,$$

with $T(X)$ in particular being called the **image** of $T$ (also known as the **range** of $T$) and denoted by $\text{Img}(T)$.

A common practice is to write $x \mapsto y$ to indicate a mapping. For instance $x \mapsto \sqrt[3]{x}$ may be written to denote a mapping $T : \mathbb{R} \to \mathbb{R}$ for which $T(x) = \sqrt[3]{x}$ for all $x \in \mathbb{R}$. The symbol $\to$ is placed between *sets*, while $\mapsto$ is placed between *elements* of sets.

**Definition 4.1.** *A mapping $T : X \to Y$ is* ***injective*** *(or* ***one-to-one****) if*

$$T(x_1) = T(x_2) \quad \Rightarrow \quad x_1 = x_2.$$

*for all $x_1, x_2 \in X$. Thus if $x_1 \neq x_2$, then $T(x_1) \neq T(x_2)$.*

*A mapping $T : X \to Y$ is* ***surjective*** *(or* ***onto****) if for each $y \in Y$ there exists some $x \in X$ such that $T(x) = y$. Thus we have $T(X) = Y$.*

*If a mapping is both injective and surjective, then it is called a* ***bijection****.*

A large part of linear algebra is occupied with the study of a special kind of mapping known as a linear mapping.

**Definition 4.2.** *Let $V$ and $W$ be vector spaces over $\mathbb{F}$. A mapping $L : V \to W$ is called a* ***linear mapping*** *if the following properties hold.*
LT1. $L(\mathbf{u}+\mathbf{v}) = L(\mathbf{u}) + L(\mathbf{v})$ *for all* $\mathbf{u}, \mathbf{v} \in V$
LT2. $L(c\mathbf{u}) = cL(\mathbf{u})$ *for all* $c \in \mathbb{F}$ *and* $\mathbf{u} \in V$.

Whenever $L : V \to W$ is given to be a linear mapping, it is understood that $V$ and $W$ must be vector spaces. A **linear operator** is a linear mapping $L : V \to V$, which may be more specifically referred to as a **linear operator on** $V$ whenever the occasion warrants.

**Proposition 4.3.** *If $L : V \to W$ is a linear mapping, then*
1. $L(\mathbf{0}) = \mathbf{0}$
2. $L(-\mathbf{v}) = -L(\mathbf{v})$ *for any* $\mathbf{v} \in V$.
3. *For any* $c_1, \dots, c_n \in \mathbb{F}$, $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$,

$$L\left(\sum_{k=1}^{n} c_k\mathbf{v}_k\right) = \sum_{k=1}^{n} c_k L(\mathbf{v}_k).$$

**Proof.**
*Proof of Part (1).* Using the linearity property LT1, we have

$$L(\mathbf{0}) = L(\mathbf{0}+\mathbf{0}) = L(\mathbf{0}) + L(\mathbf{0}).$$

Subtracting $L(\mathbf{0})$ from the leftmost and rightmost sides then gives

$$L(\mathbf{0}) - L(\mathbf{0}) = [L(\mathbf{0}) + L(\mathbf{0})] - L(\mathbf{0}),$$

and thus $\mathbf{0} = L(\mathbf{0})$.

*Proof of Part (2).* Let $\mathbf{v} \in V$ be arbitrary. Using property LT1 and part (1), we have

$$L(\mathbf{v}) + L(-\mathbf{v}) = L(\mathbf{v} + (-\mathbf{v})) = L(\mathbf{0}) = \mathbf{0}.$$

This shows that $L(-\mathbf{v})$ is the additive inverse of $L(\mathbf{v})$. That is, $L(-\mathbf{v}) = -L(\mathbf{v})$.

*Proof of Part (3).* We have $L(c_1\mathbf{v}_1) = c_1L(\mathbf{v}_1)$ by property LT2. Let $n \in \mathbb{N}$ and suppose that

$$L(c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n) = c_1L(\mathbf{v}_1) + \cdots + c_nL(\mathbf{v}_n) \tag{4.1}$$

for any $c_1, \dots, c_n \in \mathbb{F}$, $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$. Let $c_1, \dots, c_{n+1} \in \mathbb{F}$ and $\mathbf{v}_1, \dots, \mathbf{v}_{n+1} \in V$ be arbitrary. Then

$$\begin{aligned}
L\Big(\sum\nolimits_{i=1}^{n+1} c_i\mathbf{v}_i\Big) &= L\big((c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n) + c_{n+1}\mathbf{v}_{n+1}\big) \\
&= L(c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n) + L(c_{n+1}\mathbf{v}_{n+1}) && \text{Property LT1} \\
&= c_1L(\mathbf{v}_1) + \cdots + c_nL(\mathbf{v}_n) + L(c_{n+1}\mathbf{v}_{n+1}) && \text{Hypothesis (4.1)} \\
&= c_1L(\mathbf{v}_1) + \cdots + c_nL(\mathbf{v}_n) + c_{n+1}L(\mathbf{v}_{n+1}) && \text{Property LT2} \\
&= \sum\nolimits_{i=1}^{n+1} c_iL(\mathbf{v}_i)
\end{aligned}$$

The proof is complete by the Principle of Induction. ■

In part (1) of Proposition 4.3 the vector $\mathbf{0}$ on the left side of $L(\mathbf{0}) = \mathbf{0}$ is the zero vector in $V$, and the $\mathbf{0}$ on the right side is the zero vector in $W$. Occasionally there may arise a need to distinguish between these two zero vectors, in which case we will denote $\mathbf{0} \in V$ by $\mathbf{0}_V$ and $\mathbf{0} \in W$ by $\mathbf{0}_W$.

**Example 4.4.** Let $V$ and $W$ be vectors spaces. The mapping $V \to W$ given by $\mathbf{v} \mapsto \mathbf{0}_W$ for all $\mathbf{v} \in V$ is called the **zero mapping** and denoted by $O$. Thus we may write $O : V \to W$ such that $O(\mathbf{v}) = \mathbf{0}$ for all $\mathbf{v} \in V$, where the symbol $\mathbf{0}$ on the right side is understood to be the zero vector in $W$. It is easy to verify that $O$ is a linear mapping. ■

**Example 4.5.** Given a vector space $V$, the mapping $I_V : V \to V$ given by $I_V(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v} \in V$ is called the **identity mapping**. It is a linear mapping as well, and may be denoted by $I$ if the vector space it is acting on is not in question. ■

**Example 4.6.** Given a vector space $V$ and $\mathbf{a} \in V$, a mapping $T_\mathbf{a} : V \to V$ given by $T_\mathbf{a}(\mathbf{v}) = \mathbf{v}+\mathbf{a}$ for all $\mathbf{v} \in V$ is a **translation by a**. Note that this mapping is not linear unless $\mathbf{a} = \mathbf{0}$, in which case it is simply an identity mapping. One geometric interpretation is to regard $\mathbf{v}$ as a "point" in $V$, and $\mathbf{v} + \mathbf{a}$ is a new "point" obtained by translating $\mathbf{v}$ by $\mathbf{a}$.

For example, fixing a nonzero vector

$$\mathbf{a} = \begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{R}^2,$$

we may define $T_\mathbf{a} : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$T_\mathbf{a}(\mathbf{x}) = \mathbf{x} + \mathbf{a} = \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} x+a \\ y+b \end{bmatrix} \tag{4.2}$$

for each $\mathbf{x} = [x, y]^\top \in \mathbb{R}^2$.

Very often a mapping $L : \mathbb{R}^n \to \mathbb{R}^n$ is taken to be a change in coordinates, for instance in order to effect a change of variables in a double or triple integral in vector calculus. In the case of $T_\mathbf{a} : \mathbb{R}^2 \to \mathbb{R}^2$ we may regard the mapping as taking the coordinates of a point $(x, y)$ in $xy$-coordinates and converting them to $uv$-coordinates $(u, v)$ by setting $u = x + a$ and $v = y + b$. Thus, if we let the symbol $\mathbb{R}^2_{xy}$ represent $\mathbb{R}^2$ in $xy$-coordinates, and let $\mathbb{R}^2_{uv}$ represent

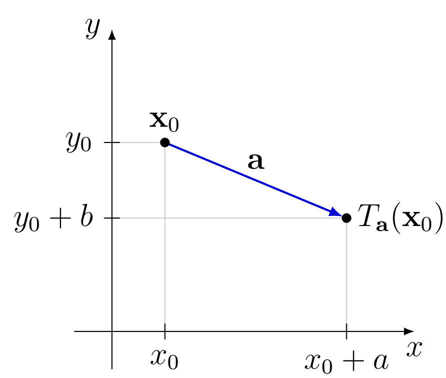



FIGURE 9. $T_\mathbf{a}$ as a translation by $\mathbf{a}$ in $\mathbb{R}^2$.

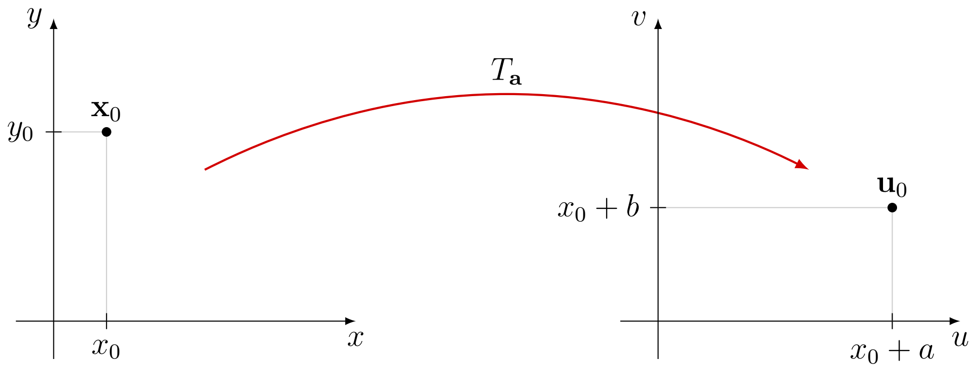



FIGURE 10. $T_{\mathbf{a}}$ as a change in coordinates $\mathbb{R}^2_{xy} \to \mathbb{R}^2_{uv}$.

$\mathbb{R}^2$ in $uv$-coordinates, then we may define the mapping $T_{\mathbf{a}}$ defined by (4.2) to be the mapping $T_{\mathbf{a}} : \mathbb{R}^2_{xy} \to \mathbb{R}^2_{uv}$ given by

$$T_{\mathbf{a}} : (x, y) \mapsto (u, v) = (x + a, y + b).$$

In vector notation we may still write $T_{\mathbf{a}} : \mathbf{x} \mapsto \mathbf{x} + \mathbf{a}$, since it makes no difference, mathematically, whether we talk of *points* $(x, y)$ and $(u, v)$, or *vectors*

$$\begin{bmatrix} x \\ y \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} u \\ v \end{bmatrix}.$$

Thus, translation by $\mathbf{a}$ in $\mathbb{R}^2$ corresponds to a change in coordinates from the $xy$-system $\mathbb{R}^2_{xy}$ to the $uv$-system $\mathbb{R}^2_{uv}$. Figure 9 shows the translation by $\mathbf{a}$ in $\mathbb{R}^2$ interpretation of $T_{\mathbf{a}}$ in the case when $a > 0$ and $b < 0$, letting

$$\begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = \mathbf{x}_0;$$

and Figure 10 shows the change in coordinates interpretation of $T_{\mathbf{a}}$ letting

$$\begin{bmatrix} u_0 \\ v_0 \end{bmatrix} = \mathbf{u}_0 = \mathbf{x}_0 + \mathbf{a}.$$

■

**Example 4.7.** Let $\mathbf{A} = [a_{ij}]$ be an $m \times n$ matrix and define $L : \mathbb{R}^n \to \mathbb{R}^m$ by $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$; that is,

$$L(\mathbf{x}) = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

for each $\mathbf{x} \in \mathbb{R}^n$. The mapping $L$ is easily shown to be linear using properties of matrix arithmetic established in Chapter 2: for each $c \in \mathbb{R}$ and $\mathbf{x} \in \mathbb{R}^n$ we have

$$L(c\mathbf{x}) = \mathbf{A}(c\mathbf{x}) = c(\mathbf{A}\mathbf{x}) = cL(\mathbf{x}),$$

and for each $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ we have

$$L(\mathbf{x}+\mathbf{y}) = \mathbf{A}(\mathbf{x}+\mathbf{y}) = \mathbf{A}\mathbf{x} + \mathbf{A}\mathbf{y} = L(\mathbf{x}) + L(\mathbf{y}).$$

This verifies properties LT1 and LT2. ■

**Definition 4.8.** *Given linear mappings $L_1, L_2 : V \to W$, we define the mapping $L_1 + L_2 : V \to W$ by*

$$(L_1 + L_2)(\mathbf{v}) = L_1(\mathbf{v}) + L_2(\mathbf{v})$$

*for each $\mathbf{v} \in V$.*

*Given linear mapping $L : V \to W$ and $c \in \mathbb{F}$, we define $cL : V \to W$ by*

$$(cL)(\mathbf{v}) = cL(\mathbf{v})$$

*for each $\mathbf{v} \in V$. In particular we define $-L = (-1)L$.*

Given vector spaces $V$ and $W$ over $\mathbb{F}$, the symbol $\mathcal{L}(V, W)$ will be used to denote the set of all linear mappings $V \to W$; that is,

$$\mathcal{L}(V, W) = \{L : V \to W \mid L \text{ is a linear mapping}\}.$$

As it turns out, $\mathcal{L}(V, W)$ is a vector space in its own right.

**Proposition 4.9.** *If $V$ and $W$ are vector spaces over $\mathbb{F}$, then $\mathcal{L}(V, W)$ is a vector space under the operations of vector addition and scalar multiplication given in Definition 4.8.*

**Proof.** Let $L_1, L_2 \in \mathcal{L}(V, W)$. For any $\mathbf{u}, \mathbf{v} \in V$,

$$\begin{aligned}
(L_1 + L_2)(\mathbf{u}+\mathbf{v}) &= L_1(\mathbf{u}+\mathbf{v}) + L_2(\mathbf{u}+\mathbf{v}) && \text{Definition 4.8} \\
&= L_1(\mathbf{u}) + L_1(\mathbf{v}) + L_2(\mathbf{u}) + L_2(\mathbf{v}) && \text{Property LT1} \\
&= [L_1(\mathbf{u}) + L_2(\mathbf{u})] + [L_1(\mathbf{v}) + L_2(\mathbf{v})] && \text{Axioms VS1 and VS2} \\
&= (L_1 + L_2)(\mathbf{u}) + (L_1 + L_2)(\mathbf{v}). && \text{Definition 4.8}
\end{aligned}$$

For any $c \in \mathbb{F}$,

$$\begin{aligned}
(L_1 + L_2)(c\mathbf{v}) &= L_1(c\mathbf{v}) + L_2(c\mathbf{v}) && \text{Definition 4.8} \\
&= cL_1(\mathbf{v}) + cL_2(\mathbf{v}) && \text{Property LT2} \\
&= c[L_1(\mathbf{v}) + L_2(\mathbf{v})] && \text{Axioms VS5} \\
&= c(L_1 + L_2)(\mathbf{v}). && \text{Definition 4.8}
\end{aligned}$$

Thus $L_1 + L_2 : V \to W$ satisfies properties LT1 and LT2, implying that $L_1 + L_2 \in \mathcal{L}(V, W)$ and therefore $\mathcal{L}(V, W)$ is closed under vector addition. The proof that $\mathcal{L}(V, W)$ is also closed under scalar multiplication is left as a problem. It remains to verify the eight axioms VS1–VS8 given in Definition 3.1.

For any $\mathbf{v} \in V$ we have

$$(L_1 + L_2)(\mathbf{v}) = L_1(\mathbf{v}) + L_2(\mathbf{v}) = L_2(\mathbf{v}) + L_1(\mathbf{v}) = (L_2 + L_1)(\mathbf{v}),$$

where the middle equality follows from VS1 for $W$. Thus $L_1 + L_2 = L_2 + L_1$, verifying VS1 for $\mathcal{L}(V,W)$.

Let $L_3 \in \mathcal{L}(V,W)$. For any $\mathbf{v} \in V$,

$$\begin{aligned}(L_1 + (L_2 + L_3))(\mathbf{v}) &= L_1(\mathbf{v}) + (L_2 + L_3)(\mathbf{v}) = L_1(\mathbf{v}) + (L_2(\mathbf{v}) + L_3(\mathbf{v}))\\ &= (L_1(\mathbf{v}) + L_2(\mathbf{v})) + L_3(\mathbf{v}) = (L_1 + L_2)(\mathbf{v}) + L_3(\mathbf{v})\\ &= ((L_1 + L_2) + L_3)(\mathbf{v}),\end{aligned}$$

where the middle equality follows from VS2 for $W$. Thus

$$L_1 + (L_2 + L_3) = (L_1 + L_2) + L_3,$$

verifying VS2 for $\mathcal{L}(V,W)$.

The zero mapping $O : V \to W$ is a linear mapping, as mentioned in Example 4.4, and thus $O \in \mathcal{L}(V,W)$. It is straightforward to verify that $O + L = L + O = L$ for any $L \in \mathcal{L}(V,W)$, and thus $\mathcal{L}(V,W)$ satisfies VS3.

For any $L \in \mathcal{L}(V,W)$ we have $-L \in \mathcal{L}(V,W)$ also, since $-L = (-1)L$ by Definition 4.8, and it has been already verified that $\mathcal{L}(V,W)$ is closed under scalar multiplication. Now, for any $\mathbf{v} \in V$,

$$\begin{aligned}(L + (-L))(\mathbf{v}) &= L(\mathbf{v}) + (-L)(\mathbf{v}) = L(\mathbf{v}) + ((-1)L)(\mathbf{v})\\ &= L(\mathbf{v}) + (-1)L(\mathbf{v}) = L(\mathbf{v}) + (-L(\mathbf{v})) = \mathbf{0},\end{aligned}$$

where the first three equalities follow from Definition 4.8, the fourth equality from Proposition 3.3, and the fifth equality from VS4 for $W$. Thus $L + (-L) = O$, verifying VS4 for $\mathcal{L}(V,W)$.

Let $a \in \mathbb{F}$. For any $\mathbf{v} \in V$,

$$\begin{aligned}(a(L_1 + L_2))(\mathbf{v}) &= a(L_1 + L_2)(\mathbf{v}) = a(L_1(\mathbf{v}) + L_2(\mathbf{v}))\\ &= aL_1(\mathbf{v}) + aL_2(\mathbf{v}) = (aL_1)(\mathbf{v}) + (aL_2)(\mathbf{v})\\ &= (aL_1 + aL_2)(\mathbf{v}),\end{aligned}$$

where the middle equality follows from VS5 for $W$. Thus $a(L_1 + L_2) = aL_1 + aL_2$, verifying VS5 for $\mathcal{L}(V,W)$.

The verification of Axiom VS6 is left as a problem, as is the verification of VS7.

Finally, for any $L \in \mathcal{L}(V,W)$ and $\mathbf{v} \in V$ we have

$$(1L)(\mathbf{v}) = 1L(\mathbf{v}) = L(\mathbf{v}),$$

by application of Definition 4.8 and VS8 for $W$. Thus $1L = L$, verifying VS8 for $\mathcal{L}(V,W)$. ■

**Definition 4.10.** *A bijective linear mapping is called an* ***isomorphism****.*

*If $V$ and $W$ are vector spaces and there exists a linear mapping $L : V \to W$ that is an isomorphism, then $V$ and $W$ are said to be* ***isomorphic*** *and we write $V \cong W$.*

Isomorphic vector spaces are truly identical in all respects save for the symbols used to represent their elements. In fact any vector space $V$ of dimension $n$ can be shown to be isomorphic to $\mathbb{R}^n$. To see this, let $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be an ordered basis for $V$ and observe that the operation of taking a vector

$$\mathbf{v} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n$$

in $V$ and giving its $\mathcal{B}$-coordinates,

$$[\mathbf{v}]_{\mathcal{B}} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix},$$

is actually a mapping $\mathbf{v} \mapsto [\mathbf{v}]_{\mathcal{B}}$ from $V$ to $\mathbb{R}^n$ called the **$\mathcal{B}$-coordinate map** (or the **coordinate map determined by $\mathcal{B}$**) and is denoted by $\varphi_{\mathcal{B}}$. Thus, by definition,

$$\varphi_{\mathcal{B}}(\mathbf{v}) = [\mathbf{v}]_{\mathcal{B}}$$

for all $\mathbf{v} \in V$. The mapping $\varphi_{\mathcal{B}}$ is a well-defined function: given $\mathbf{v} \in V$, by Theorem 3.41 there exist *unique* scalars $x_1, \ldots, x_n$ for which $\mathbf{v} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n$, and therefore

$$\varphi_{\mathcal{B}}(\mathbf{v}) = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

is the only possible definition for $\varphi_{\mathcal{B}}$. The mapping $\varphi_{\mathcal{B}}$ is, in fact, linear, injective, and surjective, which is to say it is an isomorphism.

**Theorem 4.11.** *Let $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be an ordered basis for a vector space $V$ over $\mathbb{F}$. Then the coordinate map $\varphi_{\mathcal{B}} : V \to \mathbb{F}^n$ is an isomorphism.*

**Proof.** Suppose $\mathbf{u}, \mathbf{v} \in V$ are such that

$$\varphi_{\mathcal{B}}(\mathbf{u}) = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \varphi_{\mathcal{B}}(\mathbf{v}).$$

Then $\mathbf{u} = \sum_{i=1}^n a_i\mathbf{v}_i$ and $\mathbf{v} = \sum_{i=1}^n b_i\mathbf{v}_i$ such that $a_i = b_i$ for $i = 1, \ldots, n$, whence

$$\mathbf{u} - \mathbf{v} = \sum_{i=1}^n a_i\mathbf{v}_i - \sum_{i=1}^n b_i\mathbf{v}_i = \sum_{i=1}^n (a_i - b_i)\mathbf{v}_i = \sum_{i=1}^n 0\mathbf{v}_i = \mathbf{0},$$

and so $\mathbf{u} = \mathbf{v}$. Thus $\varphi_{\mathcal{B}}$ is injective.

Next, let

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{F}^n$$

be arbitrary. Defining $\mathbf{v} \in V$ by $\mathbf{v} = \sum_{i=1}^n x_i\mathbf{v}_i$, we observe that

$$\varphi_{\mathcal{B}}(\mathbf{v}) = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix},$$

and thus $\varphi_{\mathcal{B}}$ is surjective.

Finally, for any $\mathbf{u} = \sum_{i=1}^n a_i\mathbf{v}_i$ and $\mathbf{v} = \sum_{i=1}^n b_i\mathbf{v}_i$ in $V$ we have $\mathbf{u}+\mathbf{v} = \sum_{i=1}^n (a_i+b_i)\mathbf{v}_i$, so

$$\varphi_{\mathcal{B}}(\mathbf{u}+\mathbf{v}) = \begin{bmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{bmatrix} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \varphi_{\mathcal{B}}(\mathbf{u}) + \varphi_{\mathcal{B}}(\mathbf{v})$$

by the definition of vector addition in $\mathbb{F}^n$. Also for any $c \in \mathbb{F}$ we have $c\mathbf{v} = \sum_{i=1}^n ca_i\mathbf{v}_i$, so

$$\varphi_{\mathcal{B}}(c\mathbf{u}) = \begin{bmatrix} ca_1 \\ \vdots \\ ca_n \end{bmatrix} = c\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = c\varphi_{\mathcal{B}}(\mathbf{v})$$

by the definition of scalar multiplication in $\mathbb{F}^n$. Hence $\varphi_{\mathcal{B}}$ is a linear mapping.

Therefore $\varphi_{\mathcal{B}}$ is an isomorphism. ■

**Example 4.12.** Consider the vector space $W \subseteq \mathbb{R}^3$ given by

$$W = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \,\middle|\, x - 2y + 3z = 0 \right\}.$$

Two ordered bases for $W$ are

$$\mathcal{B} = \left( \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} \right) \quad \text{and} \quad \mathcal{C} = \left( \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 0 \\ 1 \end{bmatrix} \right).$$

Given

$$\mathbf{v} = \begin{bmatrix} 5 \\ 7 \\ 3 \end{bmatrix} \in W,$$

find $[\mathbf{v}]_{\mathcal{B}}$ and $[\mathbf{v}]_{\mathcal{C}}$.

**Solution.** Since $(x, y, z) = (5, 7, 3)$ is a solution to the equation $x - 2y + 3z = 0$, it is clear that $\mathbf{v} \in W$. To find the $\mathcal{B}$-coordinates of $\mathbf{v}$, we find $a, b \in \mathbb{R}$ such that

$$a\begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} + b\begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 7 \\ 3 \end{bmatrix},$$

which is to say we solve the system

$$\begin{cases} -a + \phantom{2}b = 5 \\ \phantom{-}a + 2b = 7 \\ \phantom{-}a + \phantom{2}b = 3 \end{cases}$$

The only solution is $(a, b) = (-1, 4)$, and therefore

$$[\mathbf{v}]_{\mathcal{B}} = \begin{bmatrix} -1 \\ 4 \end{bmatrix}.$$

To find the $\mathcal{C}$-coordinates of $\mathbf{v}$, we find $a, b \in \mathbb{R}$ such that

$$a\begin{bmatrix}2\\1\\0\end{bmatrix} + b\begin{bmatrix}-3\\0\\1\end{bmatrix} = \begin{bmatrix}5\\7\\3\end{bmatrix},$$

giving the system

$$\begin{cases} 2a - 3b = 5 \\ a + 0b = 7 \\ 0a + b = 3 \end{cases}$$

which immediately yields the unique solution $(a, b) = (7, 3)$, and therefore

$$[\mathbf{v}]_{\mathcal{C}} = \begin{bmatrix}7\\3\end{bmatrix}.$$

■

## 4.2 – Images and Null Spaces

The image (or range) of a mapping was already defined in §4.1, but for convenience we give the definition again in a slightly different guise. We also narrow the focus to linear mappings in particular.

**Definition 4.13.** *Let $L : V \to W$ be a linear mapping. The **image** of $L$ is the set*

$$\text{Img}(L) = \{\mathbf{w} \in W : L(\mathbf{v}) = \mathbf{w} \text{ for some } \mathbf{v} \in V\},$$

*and the **null space** (or **kernel**) of $L$ is the set*

$$\text{Nul}(L) = \{\mathbf{v} \in V : L(\mathbf{v}) = \mathbf{0}\}.$$

Note that for $L : V \to W$ we have $\text{Img}(L) = L(V)$. Another term for the null space of $L$ is the **kernel** of $L$, denoted by $\text{Ker}(L)$ in many books.

**Proposition 4.14.** *Let $L : V \to W$ be a linear mapping. Then the following hold.*
1. $\text{Img}(L)$ *is a subspace of* $W$.
2. $\text{Nul}(L)$ *is a subspace of* $V$.

**Proof.**
*Proof of Part (1).* As we have shown in the previous section $L(\mathbf{0}) = \mathbf{0}$, and so $\mathbf{0} \in \text{Img}(L)$.

Suppose that $\mathbf{w}_1, \mathbf{w}_2 \in \text{Img}(L)$. Then there exist vectors $\mathbf{v}_1, \mathbf{v}_2 \in V$ such that $L(\mathbf{v}_1) = \mathbf{w}_1$ and $L(\mathbf{v}_2) = \mathbf{w}_2$. Now, since $\mathbf{v}_1 + \mathbf{v}_2 \in V$ and

$$L(\mathbf{v}_1 + \mathbf{v}_2) = L(\mathbf{v}_1) + L(\mathbf{v}_2) = \mathbf{w}_1 + \mathbf{w}_2,$$

we conclude that $\mathbf{w}_1 + \mathbf{w}_2 \in \text{Img}(L)$. Hence $\text{Img}(L)$ is closed under vector addition.

Finally, let $c \in \mathbb{R}$ and suppose $\mathbf{w} \in \text{Img}(L)$. Then there exists some $\mathbf{v} \in V$ such that $L(\mathbf{v}) = \mathbf{w}$, and since $c\mathbf{v} \in V$ and

$$L(c\mathbf{v}) = cL(\mathbf{v}) = c\mathbf{w},$$

we conclude that $c\mathbf{w} \in \text{Img}(L)$. Hence $\text{Img}(L)$ is closed under scalar multiplication.

Therefore $\text{Img}(L) \subseteq W$ is a subspace.

*Proof of Part (2).* Since $L(\mathbf{0}) = \mathbf{0}$ we immediately obtain $\mathbf{0} \in \text{Nul}(L)$.

Suppose that $\mathbf{v}_1, \mathbf{v}_2 \in \text{Nul}(L)$. Then $L(\mathbf{v}_1) = L(\mathbf{v}_2) = \mathbf{0}$, and since

$$L(\mathbf{v}_1 + \mathbf{v}_2) = L(\mathbf{v}_1) + L(\mathbf{v}_2) = \mathbf{0} + \mathbf{0} = \mathbf{0},$$

it follows that $\mathbf{v}_1 + \mathbf{v}_2 \in \text{Nul}(L)$ and so $\text{Nul}(L)$ is closed under vector addition.

Finally, let $c \in \mathbb{R}$ and suppose $\mathbf{v} \in \text{Nul}(L)$. Then $L(\mathbf{v}) = \mathbf{0}$, and since

$$L(c\mathbf{v}) = cL(\mathbf{v}) = c\mathbf{0} = \mathbf{0}$$

we conclude that $c\mathbf{v} \in \text{Nul}(L)$ and so $\text{Nul}(L)$ is closed under scalar multiplication.

Therefore $\text{Nul}(L) \subseteq V$ is a subspace. ■

**Proposition 4.15.** *Let $L : V \to W$ be a linear mapping. Then $L$ is injective if and only if* $\text{Nul}(L) = \{\mathbf{0}\}$.

**Proof.** Suppose that $L : V \to W$ is injective. Let $\mathbf{v} \in \text{Nul}(L)$, so that $L(\mathbf{v}) = \mathbf{0}$. By Proposition 4.3 we have $L(\mathbf{0}) = \mathbf{0}$ also, and since $L$ is injective it follows that $\mathbf{v} = \mathbf{0}$. Hence $\text{Nul}(L) \subseteq \{\mathbf{0}\}$, and $L(\mathbf{0}) = \mathbf{0}$ shows that $\{\mathbf{0}\} \subseteq \text{Nul}(L)$. Therefore $\text{Nul}(L) = \{\mathbf{0}\}$.

Next, suppose that $\text{Nul}(L) = \{\mathbf{0}\}$. Suppose that $L(\mathbf{v}_1) = L(\mathbf{v}_2)$, so $L(\mathbf{v}_1) - L(\mathbf{v}_2) = \mathbf{0}$. Then

$$L(\mathbf{v}_1 - \mathbf{v}_2) = L(\mathbf{v}_1) - L(\mathbf{v}_2) = \mathbf{0}$$

shows that $\mathbf{v}_1 - \mathbf{v}_2 \in \text{Nul}(L) = \{\mathbf{0}\}$ and thus $\mathbf{v}_1 - \mathbf{v}_2 = \mathbf{0}$. Therefore $\mathbf{v}_1 = \mathbf{v}_2$ and we conclude that $L$ is injective. ■

**Proposition 4.16.** *Let $L : V \to W$ be an injective linear mapping. If $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$ are linearly independent, then $L(\mathbf{v}_1), \dots, L(\mathbf{v}_n) \in W$ are linearly independent.*

**Proof.** Suppose $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent vectors in $V$. Let $a_1, \dots, a_n \in \mathbb{F}$ be such that

$$a_1 L(\mathbf{v}_1) + \cdots + a_n L(\mathbf{v}_n) = \mathbf{0}.$$

From this we obtain

$$L(a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) = \mathbf{0},$$

and since $\text{Nul}(L) = \{\mathbf{0}\}$ it follows that

$$a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = \mathbf{0}.$$

Now, since $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent, it follows that $a_1 = \cdots = a_n = 0$.

Therefore the vectors $L(\mathbf{v}_1), \dots, L(\mathbf{v}_n)$ in $W$ are linearly independent. ■

**Example 4.17.** Define the mapping $T : \mathbb{F}^{n\times n} \to \mathbb{F}^{n\times n}$ by

$$T(\mathbf{A}) = \frac{\mathbf{A} - \mathbf{A}^\top}{2}.$$

(a) Show that $T$ is a linear mapping.
(b) Find the null space of $T$, and give its dimension.
(c) Find the image of $T$, and give its dimension.

**Solution.**
(a) Let $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{n\times n}$ and $c \in \mathbb{F}$. Recalling Proposition 2.3, we have

$$T(c\mathbf{A}) = \frac{(c\mathbf{A}) - (c\mathbf{A})^\top}{2} = \frac{c\mathbf{A} - c\mathbf{A}^\top}{2} = c\left(\frac{\mathbf{A} - \mathbf{A}^\top}{2}\right) = cT(\mathbf{A}),$$

and

$$\begin{aligned} T(\mathbf{A} + \mathbf{B}) &= \frac{(\mathbf{A} + \mathbf{B}) - (\mathbf{A} + \mathbf{B})^\top}{2} = \frac{(\mathbf{A} + \mathbf{B}) - (\mathbf{A}^\top + \mathbf{B}^\top)}{2} \\ &= \frac{\mathbf{A} + \mathbf{B} - \mathbf{A}^\top - \mathbf{B}^\top}{2} = \frac{\mathbf{A} - \mathbf{A}^\top}{2} + \frac{\mathbf{B} - \mathbf{B}^\top}{2} \end{aligned}$$

$$= T(\mathbf{A}) + T(\mathbf{B}),$$

and therefore $T$ is linear.

(b) By definition we have

$$\text{Nul}(T) = \{\mathbf{A} \in \mathbb{F}^{n\times n} : T(\mathbf{A}) = \mathbf{O}_n\},$$

where $\mathbf{O}_n$ is the $n \times n$ zero matrix. Now,

$$T(\mathbf{A}) = \mathbf{O}_n \quad\Leftrightarrow\quad \frac{\mathbf{A} - \mathbf{A}^\top}{2} = \mathbf{O}_n \quad\Leftrightarrow\quad \mathbf{A} - \mathbf{A}^\top = \mathbf{O}_n \quad\Leftrightarrow\quad \mathbf{A} = \mathbf{A}^\top,$$

and therefore

$$\text{Nul}(T) = \{\mathbf{A} \in \mathbb{F}^{n\times n} : \mathbf{A}^\top = \mathbf{A}\} = \text{Sym}_n(\mathbb{F}).$$

That is, the null space of $T$ consists of the set of all $n \times n$ symmetric matrices. In a problem at the end of §3.6 it is found that $\dim(\text{Sym}_n(\mathbb{F})) = n(n+1)/2$, and therefore

$$\dim(\text{Nul}(T)) = \frac{n(n+1)}{2}$$

as well.

(c) By definition we have

$$\text{Img}(T) = \{T(\mathbf{A}) : \mathbf{A} \in \mathbb{F}^{n\times n}\} = \left\{\frac{\mathbf{A} - \mathbf{A}^\top}{2} : \mathbf{A} \in \mathbb{F}^{n\times n}\right\}.$$

Now, appealing to Proposition 2.3 once more, we find that

$$\left(\frac{\mathbf{A} - \mathbf{A}^\top}{2}\right)^\top = \frac{1}{2}(\mathbf{A} - \mathbf{A}^\top)^\top = \frac{1}{2}[\mathbf{A}^\top - (\mathbf{A}^\top)^\top] = \frac{1}{2}(\mathbf{A}^\top - \mathbf{A}) = -\frac{\mathbf{A} - \mathbf{A}^\top}{2},$$

and so the elements

$$\frac{\mathbf{A} - \mathbf{A}^\top}{2}$$

in the image of $T$ are skew-symmetric. Let $\text{Skw}_n(\mathbb{F})$ denote the set of $n \times n$ skew-matrices with entries in $\mathbb{F}$:

$$\text{Skw}_n(\mathbb{F}) = \{\mathbf{A} \in \mathbb{F}^{n\times n} : \mathbf{A}^\top = -\mathbf{A}\}.$$

We have just shown that $\text{Img}(T) \subseteq \text{Skw}_n(\mathbb{F})$. Suppose $\mathbf{B} \in \text{Skw}_n(\mathbb{F})$, so that $\mathbf{B}^\top = -\mathbf{B}$. Now, it happens that

$$T(\mathbf{B}) = \frac{\mathbf{B} - \mathbf{B}^\top}{2} = \frac{\mathbf{B} - (-\mathbf{B})}{2} = \frac{2\mathbf{B}}{2} = \mathbf{B},$$

and since there exists some matrix $\mathbf{A}$ for which $T(\mathbf{A}) = \mathbf{B}$ (namely we can let $\mathbf{A}$ be $\mathbf{B}$ itself), it follows that $\mathbf{B} \in \text{Img}(T)$ and hence $\text{Skw}_n(\mathbb{F}) \subseteq \text{Img}(T)$. Therefore $\text{Img}(T) = \text{Skw}_n(\mathbb{F})$. In Example 3.49 we found that $\dim(\text{Skw}_n(\mathbb{F})) = n(n-1)/2$, and therefore

$$\dim(\text{Img}(T)) = \frac{n(n-1)}{2}$$

as well. ∎

**Example 4.18.** Let $V$ be a vector space over $\mathbb{F}$ with $\dim(V) = n$ and basis $\mathcal{B}$, and let $\varphi_{\mathcal{B}} : V \to \mathbb{F}^n$ be the $\mathcal{B}$-coordinate map. Now, suppose $W$ is a subspace of $V$ with $\dim(W) = m$, and consider the restriction $\varphi_{\mathcal{B}}|_W : W \to \mathbb{F}^n$. By Proposition 4.14, $\mathrm{Img}(\varphi_{\mathcal{B}}|_W)$ is a subspace of $\mathbb{F}^n$. For brevity we define

$$[W]_{\mathcal{B}} = \mathrm{Img}(\varphi_{\mathcal{B}}|_W) = \varphi_{\mathcal{B}}(W).$$

What is the dimension of $[W]_{\mathcal{B}}$? Let $(\mathbf{w}_i)_{i=1}^m$ be any ordered basis for $W$. We wish to show that $\mathcal{C} = ([\mathbf{w}_i]_{\mathcal{B}})_{i=1}^m$ is a basis for $[W]_{\mathcal{B}}$. Since $\varphi_{\mathcal{B}}$ is injective on $V$ by Theorem 4.11, it is also injective on $W$, and thus $\mathcal{C}$ is a linearly independent set by Proposition 4.16.

If $\mathbf{x} \in [W]_{\mathcal{B}}$, then $\mathbf{x} = [\mathbf{w}]_{\mathcal{B}}$ for some $\mathbf{w} \in W$, where $\mathbf{w} = c_1\mathbf{w}_1 + \cdots + c_m\mathbf{w}_m$ for some $c_1, \ldots, c_m \in \mathbb{F}$. Now, using the linearity properties of $\varphi_{\mathcal{B}}$,

$$\mathbf{x} = [c_1\mathbf{w}_1 + \cdots + c_m\mathbf{w}_m]_{\mathcal{B}} = c_1[\mathbf{w}_1]_{\mathcal{B}} + \cdots + c_m[\mathbf{w}_m]_{\mathcal{B}} \in \mathrm{Span}(\mathcal{C})$$

Conversely, if $\mathbf{x} \in \mathrm{Span}(\mathcal{C})$, so that

$$\mathbf{x} = \sum_{i=1}^{m} c_i[\mathbf{w}_i]_{\mathcal{B}}$$

for some choice of constants $c_1, \ldots, c_m \in \mathbb{F}$, then the vector $\mathbf{w} \in W$ given by

$$\mathbf{w} = \sum_{i=1}^{m} c_i\mathbf{w}_i$$

is such that $\varphi_{\mathcal{B}}(\mathbf{w}) = [\mathbf{w}]_{\mathcal{B}} = \mathbf{x}$, and thus $\mathbf{x} \in \varphi_{\mathcal{B}}(W) = [W]_{\mathcal{B}}$. Hence $\mathrm{Span}(\mathcal{C}) = [W]_{\mathcal{B}}$, and we conclude that $\mathcal{C}$ is a basis for $[W]_{\mathcal{B}}$. It follows that $\dim([W]_{\mathcal{C}}) = |\mathcal{C}| = m$, and therefore

$$\dim([W]_{\mathcal{C}}) = \dim(W)$$

for any choice of basis $\mathcal{C}$ for $W$. ■

## Problems

1. Let $\mathbf{A}\mathbf{x} = \mathbf{b}$ be a nonhomogeneous system of linear equations, where $\mathbf{A}$ is an $m \times n$ matrix. Define $L : \mathbb{R}^n \to \mathbb{R}^m$ by $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$. Without using Theorem 2.40, prove that if $\mathbf{x}_0$ is a solution to the system then the system's solution set is

$$\mathbf{x}_0 + \mathrm{Nul}(L) = \{\mathbf{x}_0 + \mathbf{y} : \mathbf{y} \in \mathrm{Nul}(L)\}.$$

## 4.3 – Matrix Representations of Mappings

We begin with the case of Euclidean vector spaces. Let $L : \mathbb{R}^n \to \mathbb{R}^m$ be an arbitrary linear mapping. For each $1 \leq j \leq n$ let $\mathbf{e}_j$ be the $j$th standard unit vector of $\mathbb{R}^n$, represented as an $n \times 1$ column vector. Thus, as ever, $\mathbf{e}_j = [\delta_{ij}]_{n\times 1}$ such that

$$\delta_{ij} = \begin{cases} 0, & \text{if } i \neq j \\ 1, & \text{if } i = j \end{cases}$$

Also, for each $1 \leq i \leq m$ let $\boldsymbol{\epsilon}_i$ be the $i$th standard unit vector of $\mathbb{R}^m$, represented as an $m \times 1$ column vector. Choosing $\mathcal{E}_n = \{\mathbf{e}_j : 1 \leq j \leq n\}$ and $\mathcal{E}_m = \{\boldsymbol{\epsilon}_i : 1 \leq i \leq m\}$ to be the bases for $\mathbb{R}^n$ and $\mathbb{R}^m$, respectively, we view the elements of both Euclidean spaces as being column vectors in what follows.

For each $1 \leq j \leq n$ we have $L(\mathbf{e}_j) \in \mathbb{R}^m$ so that

$$L(\mathbf{e}_j) = \sum_{i=1}^{m} a_{ij}\boldsymbol{\epsilon}_i$$

for some scalars $a_{1j}, \ldots, a_{mj}$, and so the $\mathcal{E}_m$-coordinates of $L(\mathbf{e}_j)$ are

$$L(\mathbf{e}_j) = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix}.$$

(We could write $[L(\mathbf{e}_j)]_{\mathcal{E}_m}$, but since both $L(\mathbf{e}_j)$ and $[L(\mathbf{e}_j)]_{\mathcal{E}_m}$ are elements of $\mathbb{R}^m$ is would be overly fastidious.) Now,

$$L(\mathbf{e}_j) = a_{1j}\boldsymbol{\epsilon}_1 + \cdots + a_{mj}\boldsymbol{\epsilon}_m = a_{1j}\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + a_{mj}\begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix}.$$

Now, for any $\mathbf{x} \in \mathbb{R}^n$ there exist scalars $x_1, \ldots, x_n$ such that

$$\mathbf{x} = \sum_{j=1}^{n} x_j\mathbf{e}_j,$$

and so the $\mathcal{E}_n$-coordinates of $\mathbf{x}$ are

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

By the linearity of $L$ we have

$$L(\mathbf{x}) = L\left(\sum_{j=1}^{n} x_j\mathbf{e}_j\right) = \sum_{j=1}^{n} x_j L(\mathbf{e}_j) = \sum_{j=1}^{n} x_j \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix},$$

and hence, defining $\mathbf{A} = [a_{ij}]_{m,n}$,

$$L(\mathbf{x}) = \begin{bmatrix} \sum_{j=1}^{n} x_j a_{1j} \\ \vdots \\ \sum_{j=1}^{n} x_j a_{mj} \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \mathbf{A}\mathbf{x}.$$

That is, the linear mapping $L$ has a corresponding matrix $\mathbf{A}$, called the **matrix corresponding to $L : \mathbb{R}^n \to \mathbb{R}^m$ with respect to $\mathcal{E}_n$ and $\mathcal{E}_m$**. Since $L$ is arbitrary we have shown that *every* linear mapping between Euclidean spaces has a corresponding matrix, and moreover we have devised a means for determining the entries of the matrix.

**Example 4.19.** Let $L : \mathbb{R}^3 \to \mathbb{R}^2$ be given by

$$L\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right) = \begin{bmatrix} 3x_1 + 2x_2 - 7x_3 \\ 4x_1 - 6x_2 + 5x_3 \end{bmatrix}$$

Find the matrix corresponding to $L$ with respect to the standard bases for $\mathbb{R}^2$ and $\mathbb{R}^3$.

**Solution.** We must find some matrix $\mathbf{A} = [a_{ij}]_{2\times 3}$ such that $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$ for all $\mathbf{x} \in \mathbb{R}^3$; that is,

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 3x_1 + 2x_2 - 7x_3 \\ 4x_1 - 6x_2 + 5x_3 \end{bmatrix}.$$

This straightaway yields

$$\begin{bmatrix} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \end{bmatrix} = \begin{bmatrix} 3x_1 + 2x_2 - 7x_3 \\ 4x_1 - 6x_2 + 5x_3 \end{bmatrix},$$

from which we immediately obtain

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} = \begin{bmatrix} 3 & 2 & -7 \\ 4 & -6 & 5 \end{bmatrix}$$

and we're done. ■

Now that we have examined the lay of the land in the case of real Euclidean vector spaces, it is time to turn our attention to abstract vector spaces. Recall that once an ordered basis $\mathcal{B}$ for any finite-dimensional vector space $V$ over a field $\mathbb{F}$ has been chosen, every vector $\mathbf{v} \in V$ can be represented by coordinates with respect to $\mathcal{B}$ using the coordinate map $\varphi_{\mathcal{B}}$, where

$$\varphi_{\mathcal{B}}(\mathbf{v}) = [\mathbf{v}]_{\mathcal{B}}$$

as discussed in §4.1. Depending on whatever is most convenient in a given situation, we may write $[\mathbf{v}]_{\mathcal{B}}$ as a column or row matrix,

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix},$$

or more compactly as $[x_1, \ldots, x_n]$.

Let $L : V \to W$ be a linear mapping, and let $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ be an ordered basis for $V$ and $\mathcal{C} = (\mathbf{w}_1, \dots, \mathbf{w}_m)$ an ordered basis for $W$. For each $1 \le j \le n$ we have $L(\mathbf{v}_j) \in W$, and since $\mathbf{w}_1, \dots, \mathbf{w}_m$ span $W$ it follows that

$$L(\mathbf{v}_j) = a_{1j}\mathbf{w}_1 + \cdots + a_{mj}\mathbf{w}_m \tag{4.3}$$

for some scalars $a_{ij} \in \mathbb{F}$, $1 \le i \le m$. In terms of coordinates with respect to the bases $\mathcal{B}$ and $\mathcal{C}$ we may write (4.3) for each $1 \le j \le n$ as

$$\big[L(\mathbf{v}_j)\big]_{\mathcal{C}} = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix}.$$

(Recall that $[\mathbf{v}_j]_{\mathcal{B}}$, written as a column matrix, will have 1 in the $j$th row and 0 in all other rows.) Now, given any $\mathbf{v} \in V$, there exist scalars $x_1, \dots, x_n$ such that $\mathbf{v} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n$, and so

$$[\mathbf{v}]_{\mathcal{B}} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Now, by the linearity of $L$ and $\varphi_{\mathcal{C}}$,

$$\begin{aligned}\big[L(\mathbf{v})\big]_{\mathcal{C}} &= \big[L(x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n)\big]_{\mathcal{C}} = x_1\big[L(\mathbf{v}_1)\big]_{\mathcal{C}} + \cdots + x_n\big[L(\mathbf{v}_n)\big]_{\mathcal{C}} \\ &= x_1\begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix} + \cdots + x_n\begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^n x_j a_{1j} \\ \vdots \\ \sum_{j=1}^n x_j a_{mj} \end{bmatrix}.\end{aligned} \tag{4.4}$$

If we define the $m \times n$ matrix

$$[L]_{\mathcal{BC}} = \Big[\big[L(\mathbf{v}_1)\big]_{\mathcal{C}} \;\cdots\; \big[L(\mathbf{v}_n)\big]_{\mathcal{C}}\Big] = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix},$$

then we see from (4.4) that

$$\big[L(\mathbf{v})\big]_{\mathcal{C}} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix},$$

or equivalently

$$\big[L(\mathbf{v})\big]_{\mathcal{C}} = [L]_{\mathcal{BC}}[\mathbf{v}]_{\mathcal{B}} \tag{4.5}$$

for all $\mathbf{v} \in V$. The matrix $[L]_{\mathcal{BC}}$ is the **matrix corresponding to $L \in \mathcal{L}(V, W)$ with respect to $\mathcal{B}$ and $\mathcal{C}$**, also called the **$\mathcal{BC}$-matrix** of $L$. We may write (4.5) simply as $L(\mathbf{v}) = [L]_{\mathcal{BC}}\mathbf{v}$ if it is understood that $\mathcal{B}$ and $\mathcal{C}$ are the bases for $V$ and $W$, respectively. In any case $[L]_{\mathcal{BC}}[\mathbf{v}]_{\mathcal{B}}$ is seen to give the $\mathcal{C}$-coordinates (as a column matrix) of the vector $L(\mathbf{v}) \in W$. We formalize the foregoing findings as a theorem for later use.

**Theorem 4.20.** *Let $L : V \to W$ be a linear mapping, with $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ an ordered basis for $V$ and $\mathcal{C} = (\mathbf{w}_1, \dots, \mathbf{w}_m)$ an ordered basis for $W$. The $\mathcal{BC}$-matrix of $L$ is*

$$[L]_{\mathcal{BC}} = \Big[\big[L(\mathbf{v}_1)\big]_{\mathcal{C}} \quad \cdots \quad \big[L(\mathbf{v}_n)\big]_{\mathcal{C}}\Big], \tag{4.6}$$

*and*

$$[L(\mathbf{v})]_{\mathcal{C}} = [L]_{\mathcal{BC}}[\mathbf{v}]_{\mathcal{B}}.$$

*for all $\mathbf{v} \in V$.*

The situation simplifies somewhat in the commonly encountered case when $L$ is a linear operator on a vector space $V$ for which we consider only a single ordered basis $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$. To begin with, the $\mathcal{BB}$-matrix of $L$, $[L]_{\mathcal{BB}}$, is denoted by the more compact symbol $[L]_{\mathcal{B}}$, and referred to as either the **matrix corresponding to $L$ with respect to $\mathcal{B}$** or the **$\mathcal{B}$-matrix** of $L$. The following corollary is immediate.

**Corollary 4.21.** *If $L \in \mathcal{L}(V)$ and $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ is an ordered basis for $V$, then the $\mathcal{B}$-matrix of $L$ is*

$$[L]_{\mathcal{B}} = \Big[\big[L(\mathbf{v}_1)\big]_{\mathcal{B}} \quad \cdots \quad \big[L(\mathbf{v}_n)\big]_{\mathcal{B}}\Big], \tag{4.7}$$

*and*

$$[L(\mathbf{v})]_{\mathcal{B}} = [L]_{\mathcal{B}}[\mathbf{v}]_{\mathcal{B}}.$$

*for all $\mathbf{v} \in V$.*

**Example 4.22.** Let $L : \mathbb{R}^2 \to \mathbb{R}^3$ be a linear mapping for which

$$L\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad \text{and} \quad L\left(\begin{bmatrix} 1 \\ -1 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix}. \tag{4.8}$$

Find the matrix corresponding to $L$ with respect to the standard bases for $\mathbb{R}^2$ and $\mathbb{R}^3$, and then find an expression for $L([x, y]^\top)$.

**Solution.** The vectors $[1, 1]^\top$ and $[1, -1]^\top$ are linearly independent and hence form a basis for $\mathbb{R}^2$, so that (4.8) in fact uniquely determines $L$. Let $[L]$ denote the matrix corresponding to $L$ with respect to the standard bases for $\mathbb{R}^2$ and $\mathbb{R}^3$, which we'll denote by $\{\mathbf{e}_1, \mathbf{e}_2\}$ and $\mathcal{E}$ respectively. Theorem 4.20 informs us that

$$[L] = \Big[\big[L(\mathbf{e}_1)\big]_{\mathcal{E}} \quad \big[L(\mathbf{e}_2)\big]_{\mathcal{E}}\Big] = \big[L(\mathbf{e}_1) \quad L(\mathbf{e}_2)\big],$$

where the last equality is simply a recognition of the fact that, for any $\mathbf{x} \in \mathbb{R}^2$, the vector $L(\mathbf{x}) \in \mathbb{R}^3$ is already in $\mathcal{E}$-coordinates. The problem is we don't know the values of $L(\mathbf{e}_1)$ and $L(\mathbf{e}_2)$. These could be figured out with a little clever tinkering using the linearity properties of $L$, but the tack we'll take is one which will work in general.

Setting

$$\mathbf{B} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

by Proposition 2.6 and the definition of $[L]$ we have

$$[L]\mathbf{B} = \begin{bmatrix} [L]\begin{bmatrix}1\\1\end{bmatrix} & [L]\begin{bmatrix}1\\-1\end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ 1 & -1 \end{bmatrix}. \tag{4.9}$$

By the methods of §2.4 we find that $\mathbf{B}$ is invertible, with

$$\mathbf{B}^{-1} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{bmatrix}.$$

Right-multiplying through (4.9) by $\mathbf{B}^{-1}$ at once gives us $[L]$:

$$[L] = \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ 1 & -1 \end{bmatrix}\mathbf{B}^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Now for any $[x, y]^\top \in \mathbb{R}^2$ we have

$$L\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = [L]\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ y \\ y \end{bmatrix}.$$

The image of $L$ is easily verified to be $\text{Col}([L])$, which is the plane $y = z$ in $\mathbb{R}^3$. ■

**Example 4.23.** Let $L \in \mathcal{L}(\mathbb{R}^{2\times 2})$ be given by $L(\mathbf{A}) = \mathbf{A}^\top$, and let $\mathcal{E} = \mathcal{E}_{22}$, the standard ordered basis for $\mathbb{R}^{2\times 2}$. Find $[L]_{\mathcal{E}}$, the $\mathcal{E}$-matrix of $L$.

**Solution.** We have $\mathcal{E} = (\mathbf{E}_{11}, \mathbf{E}_{12}, \mathbf{E}_{21}, \mathbf{E}_{22})$, where

$$\mathbf{E}_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \mathbf{E}_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \mathbf{E}_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{E}_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Since

$$\mathbf{E}_{11} = 1\mathbf{E}_{11} + 0\mathbf{E}_{12} + 0\mathbf{E}_{21} + 0\mathbf{E}_{22}, \quad \mathbf{E}_{12} = 0\mathbf{E}_{11} + 1\mathbf{E}_{12} + 0\mathbf{E}_{21} + 0\mathbf{E}_{22},$$

and so on, the $\mathcal{E}$-coordinates of the elements of $\mathcal{E}$ are

$$[\mathbf{E}_{11}]_{\mathcal{E}} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad [\mathbf{E}_{12}]_{\mathcal{E}} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad [\mathbf{E}_{21}]_{\mathcal{E}} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad [\mathbf{E}_{22}]_{\mathcal{E}} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Now, in general,

$$L\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & c \\ b & d \end{bmatrix},$$

so that

$$L(\mathbf{E}_{12}) = L\left(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \mathbf{E}_{21}$$

and

$$L(\mathbf{E}_{21}) = L\left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\right) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \mathbf{E}_{12},$$

while $L(\mathbf{E}_{11}) = \mathbf{E}_{11}$ and $L(\mathbf{E}_{22}) = \mathbf{E}_{22}$. By Corollary 4.21,

$$[L]_{\mathcal{E}} = \Big[ \big[L(\mathbf{E}_{11})\big]_{\mathcal{E}} \;\; \big[L(\mathbf{E}_{12})\big]_{\mathcal{E}} \;\; \big[L(\mathbf{E}_{21})\big]_{\mathcal{E}} \;\; \big[L(\mathbf{E}_{22})\big]_{\mathcal{E}} \Big] = \big[ [\mathbf{E}_{11}]_{\mathcal{E}} \;\; [\mathbf{E}_{21}]_{\mathcal{E}} \;\; [\mathbf{E}_{12}]_{\mathcal{E}} \;\; [\mathbf{E}_{22}]_{\mathcal{E}} \big],$$

and therefore

$$[L]_{\mathcal{E}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is the $\mathcal{E}$-matrix of $L$. ■

**Theorem 4.24.** *If $V$ and $W$ are vector spaces over $\mathbb{F}$ with $\dim(V) = n$ and $\dim(W) = m$, then $\mathcal{L}(V, W) \cong \mathbb{F}^{m\times n}$.*

**Proof.** Let $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ and $\mathcal{C} = (\mathbf{w}_1, \ldots, \mathbf{w}_m)$ be ordered bases for $V$ and $W$, respectively. Proposition 4.9 established that $\mathcal{L}(V, W)$ is a vector space, so define $\Phi : \mathcal{L}(V, W) \to \mathbb{F}^{m\times n}$ by $\Phi(L) = [L]_{\mathcal{BC}}$. By Theorem 4.20,

$$\Phi(L) = \Big[ \varphi_{\mathcal{C}}\big(L(\mathbf{v}_1)\big) \;\; \cdots \;\; \varphi_{\mathcal{C}}\big(L(\mathbf{v}_n)\big) \Big],$$

which shows that $\Phi$ is a well-defined function since the $\mathcal{C}$-coordinate map $\varphi_{\mathcal{C}} : W \to \mathbb{F}^m$ is a well-defined function by the discussion preceding Theorem 4.11. We will show that $\Phi$ is an isomorphism.

Let $L_1, L_2 \in \mathcal{L}(V, W)$. Then by Theorem 4.20,

$$\Phi(L_1 + L_2) = [L_1 + L_2]_{\mathcal{BC}} = \Big[ \big[(L_1 + L_2)(\mathbf{v}_1)\big]_{\mathcal{C}} \;\; \cdots \;\; \big[(L_1 + L_2)(\mathbf{v}_n)\big]_{\mathcal{C}} \Big];$$

that is, $\Phi(L_1 + L_2)$ is the matrix with $j$th column vector $[(L_1 + L_2)(\mathbf{v}_n)]_{\mathcal{C}}$ for $1 \le j \le n$. Now, since $\varphi_{\mathcal{C}} : W \to \mathbb{F}^m$ is linear by Theorem 4.11,

$$\begin{aligned} \big[(L_1 + L_2)(\mathbf{v}_j)\big]_{\mathcal{C}} &= \big[L_1(\mathbf{v}_j) + L_2(\mathbf{v}_j)\big]_{\mathcal{C}} = \varphi_{\mathcal{C}}\big(L_1(\mathbf{v}_j) + L_2(\mathbf{v}_j)\big) \\ &= \varphi_{\mathcal{C}}\big(L_1(\mathbf{v}_j)\big) + \varphi_{\mathcal{C}}\big(L_2(\mathbf{v}_j)\big) = \big[L_1(\mathbf{v}_j)\big]_{\mathcal{C}} + \big[L_2(\mathbf{v}_j)\big]_{\mathcal{C}}, \end{aligned}$$

and so by the definition of matrix addition,

$$\begin{aligned} \Phi(L_1 + L_2) &= \Big[ \big[L_1(\mathbf{v}_1)\big]_{\mathcal{C}} + \big[L_2(\mathbf{v}_1)\big]_{\mathcal{C}} \;\; \cdots \;\; \big[L_1(\mathbf{v}_n)\big]_{\mathcal{C}} + \big[L_2(\mathbf{v}_n)\big]_{\mathcal{C}} \Big] \\ &= \Big[ \big[L_1(\mathbf{v}_1)\big]_{\mathcal{C}} \;\; \cdots \;\; \big[L_1(\mathbf{v}_n)\big]_{\mathcal{C}} \Big] + \Big[ \big[L_2(\mathbf{v}_1)\big]_{\mathcal{C}} \;\; \cdots \;\; \big[L_2(\mathbf{v}_n)\big]_{\mathcal{C}} \Big] \\ &= \Phi(L_1) + \Phi(L_2). \end{aligned}$$

Next, for any $c \in \mathbb{F}$ and $L \in \mathcal{L}(V, W)$, again recalling that $\varphi_{\mathcal{C}}$ is linear,

$$\begin{aligned} \Phi(cL) &= \Big[ \cdots \;\; \big[(cL)(\mathbf{v}_j)\big]_{\mathcal{C}} \;\; \cdots \Big] = \Big[ \cdots \;\; \big[cL(\mathbf{v}_j)\big]_{\mathcal{C}} \;\; \cdots \Big] \\ &= \Big[ \cdots \;\; c\big[L(\mathbf{v}_j)\big]_{\mathcal{C}} \;\; \cdots \Big] = c\Big[ \cdots \;\; \big[L(\mathbf{v}_j)\big]_{\mathcal{C}} \;\; \cdots \Big] \\ &= c\Phi(L), \end{aligned}$$

where the fourth equality follows from the definition of scalar multiplication of a matrix. We see that $\Phi$ satisfies properties LT1 and LT2, and hence is a linear mapping.

Let $L \in \text{Nul}(\Phi)$, so that

$$\Phi(L) = [L]_{\mathcal{BC}} = \Big[ \big[L(\mathbf{v}_1)\big]_{\mathcal{C}} \ \cdots \ \big[L(\mathbf{v}_n)\big]_{\mathcal{C}} \Big] = \mathbf{O}_{m,n}.$$

Thus, for each $1 \leq j \leq n$,

$$\varphi_{\mathcal{C}}(L(\mathbf{v}_j)) = \big[L(\mathbf{v}_j)\big]_{\mathcal{C}} = [0]_{m,1},$$

which shows that $L(\mathbf{v}_j) \in \text{Nul}(\varphi_{\mathcal{C}})$. However $\varphi_{\mathcal{C}}$ is injective, so $\text{Nul}(\varphi_{\mathcal{C}}) = \{\mathbf{0}\}$ by Proposition 4.15, and hence $L(\mathbf{v}_j) = \mathbf{0}$. Now, for any $\mathbf{v} \in V$ there exist $c_1, \ldots, c_k \in \mathbb{F}$ such that

$$\mathbf{v} = \sum_{j=1}^{n} c_j \mathbf{v}_j,$$

and then

$$L(\mathbf{v}) = L\left(\sum_{j=1}^{n} c_j \mathbf{v}_j\right) = \sum_{j=1}^{n} c_j L(\mathbf{v}_j) = \sum_{j=1}^{n} c_j \mathbf{0} = \mathbf{0}.$$

Thus $L(\mathbf{v}) = \mathbf{0}$ for all $\mathbf{v} \in V$, which is to say $L = O$, the zero mapping. It follows that $\text{Nul}(\Phi) \subseteq \{O\}$, and since the reverse containment obtains from Proposition 4.3(1), we have $\text{Nul}(\Phi) = \{O\}$. Hence $\Phi$ is injective by Proposition 4.15.

Next, let $\mathbf{A} \in \mathbb{F}^{m \times n}$, so

$$\mathbf{A} = \begin{bmatrix} \mathbf{a}_1 & \cdots & \mathbf{a}_n \end{bmatrix}$$

with

$$\mathbf{a}_j = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix} \in \mathbb{F}^m$$

for each $1 \leq j \leq n$. Let $L \in \mathcal{L}(V, W)$ be such that

$$L(\mathbf{v}_j) = a_{1j}\mathbf{w}_1 + \cdots + a_{mj}\mathbf{w}_m$$

for each $1 \leq j \leq n$, so that

$$[L(\mathbf{v}_j)]_{\mathcal{C}} = \mathbf{a}_j.$$

Then

$$\Phi(L) = \Big[ \big[L(\mathbf{v}_1)\big]_{\mathcal{C}} \ \cdots \ \big[L(\mathbf{v}_n)\big]_{\mathcal{C}} \Big] = \begin{bmatrix} \mathbf{a}_1 & \cdots & \mathbf{a}_n \end{bmatrix} = \mathbf{A},$$

which shows that $\Phi$ is surjective.

Since $\Phi : \mathcal{L}(V, W) \to \mathbb{F}^{m \times n}$ is linear, injective, and surjective, we conclude that it is an isomorphism. Therefore $\mathcal{L}(V, W) \cong \mathbb{F}^{m \times n}$. ■

**Corollary 4.25.** *Let $V$ and $W$ be finite-dimensional vector spaces over $\mathbb{F}$ with ordered bases $\mathcal{B}$ and $\mathcal{C}$, respectively. For every mapping $L \in \mathcal{L}(V, W)$ there is a unique matrix $\mathbf{A} \in \mathbb{F}^{m \times n}$ such that $\mathbf{A} = [L]_{\mathcal{BC}}$. For every matrix $\mathbf{A} \in \mathbb{F}^{m \times n}$ there is a unique mapping $L \in \mathcal{L}(V, W)$ such that $[L]_{\mathcal{BC}} = \mathbf{A}$.*

**Proof.** In the proof of Theorem 4.24 it was found that $\Phi : \mathcal{L}(V, W) \to \mathbb{F}^{m \times n}$ given by $\Phi(L) = [L]_{\mathcal{BC}}$ is an isomorphism. The first statement of the corollary follows from the fact that $\Phi$ is a well-defined function on $\mathcal{L}(V, W)$, and the second statement follows from the fact that $\Phi$ is surjective and injective. ■

**Example 4.26.** Another way to argue that, in particular, there is a unique matrix $\mathbf{A}$ corresponding to a linear mapping $L : V \to W$ with respect to bases $\mathcal{B}$ and $\mathcal{C}$ is as follows. Suppose that $[L]_{\mathcal{BC}}, [L]'_{\mathcal{BC}} \in \mathbb{F}^{m\times n}$ are two matrices corresponding to $L$ with respect to $\mathcal{B}$ and $\mathcal{C}$. Then

$$[L(\mathbf{v})]_{\mathcal{C}} = [L]_{\mathcal{BC}}[\mathbf{v}]_{\mathcal{B}} \quad \text{and} \quad [L(\mathbf{v})]_{\mathcal{C}} = [L]'_{\mathcal{BC}}[\mathbf{v}]_{\mathcal{B}},$$

and thus

$$\big([L]_{\mathcal{BC}} - [L]'_{\mathcal{BC}}\big)[\mathbf{v}]_{\mathcal{B}} = \mathbf{0}$$

for all $\mathbf{v} \in V$. Now, setting $\mathbf{B} = [L]_{\mathcal{BC}} - [L]'_{\mathcal{BC}}$ and observing that $[\mathbf{v}_j]_{\mathcal{B}} = [\delta_{ij}]_{n\times 1}$, we have $\mathbf{B}[\mathbf{v}_j]_{\mathcal{B}} = \mathbf{0}$ for each $1 \le j \le n$, or

$$\mathbf{B}[\mathbf{v}_j]_{\mathcal{B}} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} \delta_{1j} \\ \vdots \\ \delta_{nj} \end{bmatrix} = \begin{bmatrix} \sum_{k=1}^{n} b_{1k}\delta_{kj} \\ \vdots \\ \sum_{k=1}^{n} b_{mk}\delta_{kj} \end{bmatrix} = \begin{bmatrix} b_{1j} \\ \vdots \\ b_{mj} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Thus the $j$th column vector of $\mathbf{B}$ is $\mathbf{0}$, and since $1 \le j \le n$ is arbitrary we conclude that all the columns of $\mathbf{B}$ consist of zeros and so $\mathbf{B} = \mathbf{O}_{m,n}$. Therefore $[L]_{\mathcal{BC}} - [L]'_{\mathcal{BC}} = \mathbf{O}_{m,n}$, and it follows that $[L]_{\mathcal{BC}} = [L]'_{\mathcal{BC}}$. ■

Though there cannot be two distinct matrices corresponding to the same linear mapping $L : V \to W$ with respect to the same bases $\mathcal{B}$ and $\mathcal{C}$, a different choice of basis for either $V$ or $W$ will result in a different corresponding matrix for $L$. This turns the discussion toward the idea of changing from one basis $\mathcal{B}$ of a vector space $V$ to another basis $\mathcal{B}'$, the subject of the next section.

## Problems

1. Suppose that $L : \mathbb{R}^2 \to \mathbb{R}^3$ is the linear transformation given by

$$L\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = \begin{bmatrix} x_2 \\ -5x_1 + 13x_2 \\ -7x_1 + 16x_2 \end{bmatrix}.$$

Find $[L]_{\mathcal{BC}}$, the matrix corresponding to $L$ with respect to the ordered bases

$$\mathcal{B} = \left(\begin{bmatrix} 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 5 \\ 2 \end{bmatrix}\right) \quad \text{and} \quad \mathcal{C} = \left(\begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} -1 \\ 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}\right).$$

## 4.4 – Change of Basis

Let $V$ be an $n$-dimensional vector space over $\mathbb{F}$, where $n \geq 1$. Let

$$\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \quad \text{and} \quad \mathcal{B}' = \{\mathbf{v}_1', \ldots, \mathbf{v}_n'\}$$

be two distinct bases for $V$. We would like to devise a ready means of expressing any vector $\mathbf{v} \in V$ given in $\mathcal{B}$-coordinates in terms of $\mathcal{B}'$-coordinates instead. In other words we seek a mapping $\mathbb{F}^n \to \mathbb{F}^n$ given by $[\mathbf{v}]_{\mathcal{B}} \mapsto [\mathbf{v}]_{\mathcal{B}'}$ for all $\mathbf{v} \in V$. How to find the mapping? Consider the identity mapping $I_V : V \to V$, which of course is linear. By Theorem 4.20 the matrix corresponding to $I_V$ with respect to $\mathcal{B}$ and $\mathcal{B}'$ is

$$[I_V]_{\mathcal{B}\mathcal{B}'} = \left[ \big[I_V(\mathbf{v}_1)\big]_{\mathcal{B}'} \;\; \cdots \;\; \big[I_V(\mathbf{v}_n)\big]_{\mathcal{B}'} \right] = \left[ [\mathbf{v}_1]_{\mathcal{B}'} \;\; \cdots \;\; [\mathbf{v}_n]_{\mathcal{B}'} \right], \tag{4.10}$$

and for all $\mathbf{v} \in V$

$$[I_V]_{\mathcal{B}\mathcal{B}'}[\mathbf{v}]_{\mathcal{B}} = [I_V(\mathbf{v})]_{\mathcal{B}'} = [\mathbf{v}]_{\mathcal{B}'}.$$

This is it! To convert any $\mathbf{v} \in V$ from $\mathcal{B}$-coordinates to $\mathcal{B}'$-coordinates we simply multiply the column vector $[\mathbf{v}]_{\mathcal{B}}$ by the matrix $[I_V]_{\mathcal{B}\mathcal{B}'}$, which happens to be the matrix corresponding to the identity matrix $I_V$ with respect to $\mathcal{B}$ and $\mathcal{B}'$, but we will call it the **change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$** (or the **coordinate transformation matrix from $\mathcal{B}$ to $\mathcal{B}'$**) and denote it by $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$. We have proven the following.

**Theorem 4.27.** *Let $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ and $\mathcal{B}' = (\mathbf{v}_1', \ldots, \mathbf{v}_n')$ be two ordered bases for $V$, and define $\mathbf{I}_{\mathcal{B}\mathcal{B}'} \in \mathbb{F}^{n\times n}$ by*

$$\mathbf{I}_{\mathcal{B}\mathcal{B}'} = \left[ [\mathbf{v}_1]_{\mathcal{B}'} \;\; \cdots \;\; [\mathbf{v}_n]_{\mathcal{B}'} \right].$$

*Then*

$$\mathbf{I}_{\mathcal{B}\mathcal{B}'}[\mathbf{v}]_{\mathcal{B}} = [\mathbf{v}]_{\mathcal{B}'}$$

*for all $\mathbf{v} \in V$.*

Clearly to find $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$ we must determine the $\mathcal{B}'$-coordinates of the vectors in $\mathcal{B}$. For each $1 \leq j \leq n$ there exist scalars $a_{1j}, \ldots, a_{nj}$ such that

$$\mathbf{v}_j = a_{1j}\mathbf{v}_1' + \cdots + a_{nj}\mathbf{v}_n',$$

and so

$$[\mathbf{v}_j]_{\mathcal{B}'} = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{bmatrix}.$$

As the following example illustrates, the task of determining $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$ in practice amounts to solving a system of equations that has a unique solution.

**Example 4.28.** Let $V$ be a vector space with ordered basis $\mathcal{B} = (\mathbf{v}_1, \mathbf{v}_2)$.

(a) Show that $\mathcal{B}' = (\mathbf{v}_1', \mathbf{v}_2')$ with $\mathbf{v}_1' = -\mathbf{v}_1 + 2\mathbf{v}_2$ and $\mathbf{v}_2' = 3\mathbf{v}_1 + \mathbf{v}_2$ is another ordered basis for the vector space $V$.

(b) Determine the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$, $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$.

(c) Determine the change of basis matrix from $\mathcal{B}'$ to $\mathcal{B}$, $\mathbf{I}_{\mathcal{B}'\mathcal{B}}$.

**Solution.**
(a) We see that $\dim(V) = |\mathcal{B}| = 2$, and so by Theorem 3.54(1) to show that $\mathcal{B}'$ is a basis for $V$ is suffices to show that $\mathbf{v}_1'$ and $\mathbf{v}_2'$ are linearly independent. Suppose that $c_1, c_2 \in \mathbb{F}$ are such that

$$c_1\mathbf{v}_1' + c_2\mathbf{v}_2' = \mathbf{0}. \tag{4.11}$$

This implies that

$$c_1(-\mathbf{v}_1 + 2\mathbf{v}_2) + c_2(3\mathbf{v}_1 + \mathbf{v}_2) = \mathbf{0},$$

or equivalently

$$(-c_1 + 3c_2)\mathbf{v}_1 + (2c_1 + c_2)\mathbf{v}_2 = \mathbf{0}$$

Since $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent we must have

$$\begin{cases} -c_1 + 3c_2 = 0 \\ \ \ 2c_1 + \ \ c_2 = 0 \end{cases}$$

This system readily informs us that $c_1 = c_2 = 0$, and so (4.11) admits only the trivial solution. Therefore $\mathbf{v}_1'$ and $\mathbf{v}_2'$ must be linearly independent.

(b) By Theorem 4.27 we have

$$\mathbf{I}_{\mathcal{B}\mathcal{B}'} = \begin{bmatrix} [\mathbf{v}_1]_{\mathcal{B}'} & [\mathbf{v}_2]_{\mathcal{B}'} \end{bmatrix}.$$

We set

$$[\mathbf{v}_1]_{\mathcal{B}'} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \quad \text{and} \quad [\mathbf{v}_2]_{\mathcal{B}'} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix},$$

which is to say

$$x_1\mathbf{v}_1' + x_2\mathbf{v}_2' = \mathbf{v}_1 \quad \text{and} \quad y_1\mathbf{v}_1' + y_2\mathbf{v}_2' = \mathbf{v}_2$$

Using the fact that the coordinate map $\varphi_{\mathcal{B}}$ is a linear mapping, we obtain

$$\begin{aligned} \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= [\mathbf{v}_1]_{\mathcal{B}} = \varphi_{\mathcal{B}}(\mathbf{v}_1) = \varphi_{\mathcal{B}}(x_1\mathbf{v}_1' + x_2\mathbf{v}_2') = x_1\varphi_{\mathcal{B}}(\mathbf{v}_1') + x_2\varphi_{\mathcal{B}}(\mathbf{v}_2') \\ &= x_1[\mathbf{v}_1']_{\mathcal{B}} + x_2[\mathbf{v}_2']_{\mathcal{B}} = x_1\begin{bmatrix} -1 \\ 2 \end{bmatrix} + x_2\begin{bmatrix} 3 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \end{aligned} \tag{4.12}$$

and similarly

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} = [\mathbf{v}_2]_{\mathcal{B}} = y_1[\mathbf{v}_1']_{\mathcal{B}} + y_2[\mathbf{v}_2']_{\mathcal{B}} = y_1\begin{bmatrix} -1 \\ 2 \end{bmatrix} + y_2\begin{bmatrix} 3 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}. \tag{4.13}$$

From (4.12) and (4.13) we obtain the systems

$$\begin{cases} -x_1 + 3x_2 = 1 \\ \ \ 2x_1 + \ \ x_2 = 0 \end{cases} \quad \text{and} \quad \begin{cases} -y_1 + 3y_2 = 0 \\ \ \ 2y_1 + \ \ y_2 = 1 \end{cases}$$

Solving these systems yields $x_1 = -1/7$, $x_2 = 2/7$, $y_1 = 3/7$, and $y_2 = 1/7$. Therefore we have

$$\mathbf{I}_{\mathcal{B}\mathcal{B}'} = \begin{bmatrix} [\mathbf{v}_1]_{\mathcal{B}'} & [\mathbf{v}_2]_{\mathcal{B}'} \end{bmatrix} = \begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \end{bmatrix} = \begin{bmatrix} -1/7 & 3/7 \\ 2/7 & 1/7 \end{bmatrix}.$$

(c) As for the change of basis matrix from $\mathcal{B}'$ to $\mathcal{B}$, that's relatively straightforward since the vectors in $\mathcal{B}'$ were given in terms of the vectors in $\mathcal{B}$:

$$\mathbf{I}_{\mathcal{B}'\mathcal{B}} = \begin{bmatrix} [\mathbf{v}_1']_{\mathcal{B}} & [\mathbf{v}_2']_{\mathcal{B}} \end{bmatrix} = \begin{bmatrix} -1 & 3 \\ 2 & 1 \end{bmatrix}$$

Observe that

$$\mathbf{I}_{\mathcal{B}'\mathcal{B}}\mathbf{I}_{\mathcal{B}\mathcal{B}'} = \mathbf{I}_{\mathcal{B}\mathcal{B}'}\mathbf{I}_{\mathcal{B}'\mathcal{B}} = \mathbf{I}_2,$$

so that $\mathbf{I}_{\mathcal{B}'\mathcal{B}}$ and $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$ are in fact inverses of one another. ■

**Example 4.29.** Consider the vector space $W \subseteq \mathbb{R}^3$ given by

$$W = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \middle|\, x - 2y + 3z = 0 \right\}.$$

Two ordered bases for $W$ are

$$\mathcal{B} = (\mathbf{u}_1, \mathbf{u}_2) = \left( \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} \right) \quad \text{and} \quad \mathcal{C} = (\mathbf{v}_1, \mathbf{v}_2) = \left( \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 0 \\ 1 \end{bmatrix} \right).$$

Find the change of basis matrix from $\mathcal{B}$ to $\mathcal{C}$, and use it to find the $\mathcal{C}$-coordinates of $\mathbf{v} \in W$ given that $[\mathbf{v}]_{\mathcal{B}} = [-1 \;\; 4]^\top$

**Solution.** By Theorem 4.27 we have

$$\mathbf{I}_{\mathcal{B}\mathcal{C}} = \Big[ [\mathbf{u}_1]_{\mathcal{C}} \;\; [\mathbf{u}_2]_{\mathcal{C}} \Big],$$

and so we must find the $\mathcal{C}$-coordinates of $\mathbf{u}_1$ and $\mathbf{u}_2$. Starting with $\mathbf{u}_1$, we find $a, b \in \mathbb{R}$ such that $a\mathbf{v}_1 + b\mathbf{v}_2 = \mathbf{u}_1$; that is,

$$a \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} -3 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix},$$

which has $(a, b) = (1, 1)$ as the only solution, and hence

$$[\mathbf{u}_1]_{\mathcal{C}} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Next, we find $a, b \in \mathbb{R}$ such that $a\mathbf{v}_1 + b\mathbf{v}_2 = \mathbf{u}_2$; that is,

$$a \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} -3 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix},$$

which has $(a, b) = (2, 1)$ as the only solution, and hence

$$[\mathbf{u}_2]_{\mathcal{C}} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

Therefore

$$\mathbf{I}_{\mathcal{B}\mathcal{C}} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$$

is the change of basis matrix from $\mathcal{B}$ to $\mathcal{C}$. Now,

$$[\mathbf{v}]_{\mathcal{C}} = \mathbf{I}_{\mathcal{B}\mathcal{C}}[\mathbf{v}]_{\mathcal{B}} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} -1 \\ 4 \end{bmatrix} = \begin{bmatrix} 7 \\ 3 \end{bmatrix},$$

which agrees with the results of Example 4.12. ■

**Example 4.30.** Two ordered bases for the vector space

$$\mathcal{P}_2(\mathbb{R}) = \{a_0 + a_1x + a_2x^2 : a_0, a_1, a_2 \in \mathbb{R}\}$$

are

$$\mathcal{B} = (1, x, x^2) \quad \text{and} \quad \mathcal{D} = (1, 1+x, 1+x+x^2).$$

(a) Find the change of basis matrix from $\mathcal{B}$ to $\mathcal{D}$.
(b) Find the change of basis matrix from $\mathcal{D}$ to $\mathcal{B}$.

**Solution.**
(a) We have $\mathcal{B} = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ with $\mathbf{v}_1 = 1$, $\mathbf{v}_2 = x$, and $\mathbf{v}_3 = x^2$, and $\mathcal{D} = (\mathbf{v}_1', \mathbf{v}_2', \mathbf{v}_3')$ with $\mathbf{v}_1' = 1$, $\mathbf{v}_2' = 1 + x$, and $\mathbf{v}_3' = 1 + x + x^2$. By Theorem 4.27,

$$\mathbf{I}_{\mathcal{B}\mathcal{D}} = \Big[ [1]_{\mathcal{D}} \;\; [x]_{\mathcal{D}} \;\; [x^2]_{\mathcal{D}} \Big].$$

Setting

$$[1]_{\mathcal{D}} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}, \quad [x]_{\mathcal{D}} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}, \quad [x^2]_{\mathcal{D}} = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix},$$

three equations arise:

$$a_1(1) + a_2(1+x) + a_3(1+x+x^2) = 1,$$
$$b_1(1) + b_2(1+x) + b_3(1+x+x^2) = x,$$
$$c_1(1) + c_2(1+x) + c_3(1+x+x^2) = x^2.$$

Rewriting these equations as

$$(a_1 + a_2 + a_3) + (a_2 + a_3)x + a_3x^2 = 1,$$
$$(b_1 + b_2 + b_3) + (b_2 + b_3)x + b_3x^2 = x,$$
$$(c_1 + c_2 + c_3) + (c_2 + c_3)x + c_3x^2 = x^2,$$

we obtain the systems

$$\begin{cases} a_1 + a_2 + a_3 = 1 \\ \phantom{a_1 +{}} a_2 + a_3 = 0 \\ \phantom{a_1 + a_2 +{}} a_3 = 0 \end{cases} \qquad \begin{cases} b_1 + b_2 + b_3 = 0 \\ \phantom{b_1 +{}} b_2 + b_3 = 1 \\ \phantom{b_1 + b_2 +{}} b_3 = 0 \end{cases} \qquad \begin{cases} c_1 + c_2 + c_3 = 0 \\ \phantom{c_1 +{}} c_2 + c_3 = 0 \\ \phantom{c_1 + c_2 +{}} c_3 = 1 \end{cases}$$

which have solutions

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix}.$$

Therefore

$$\mathbf{I}_{\mathcal{B}\mathcal{D}} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}.$$

(b) By Theorem 4.27

$$\mathbf{I}_{\mathcal{DB}} = \Big[[1]_{\mathcal{B}} \;\; [1+x]_{\mathcal{B}} \;\; [1+x+x^2]_{\mathcal{B}}\Big].$$

Clearly

$$[1]_{\mathcal{B}} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad [1+x]_{\mathcal{B}} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \quad [1+x+x^2]_{\mathcal{B}} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix},$$

and therefore

$$\mathbf{I}_{\mathcal{DB}} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

■

**Proposition 4.31.** *Let $\mathcal{B}$ and $\mathcal{B}'$ be ordered bases for a finite-dimensional vector space $V$. Then the change of basis matrix $\mathbf{I}_{\mathcal{BB}'}$ is invertible, with*

$$\mathbf{I}_{\mathcal{BB}'}^{-1} = \mathbf{I}_{\mathcal{B}'\mathcal{B}}.$$

**Proof.** By Theorem 4.27

$$\mathbf{I}_{\mathcal{BB}'}[\mathbf{v}]_{\mathcal{B}} = [\mathbf{v}]_{\mathcal{B}'} \quad \text{and} \quad \mathbf{I}_{\mathcal{B}'\mathcal{B}}[\mathbf{v}]_{\mathcal{B}'} = [\mathbf{v}]_{\mathcal{B}},$$

for all $\mathbf{v} \in V$, and so

$$\mathbf{I}_{\mathcal{B}'\mathcal{B}}\mathbf{I}_{\mathcal{BB}'}[\mathbf{v}]_{\mathcal{B}} = \mathbf{I}_{\mathcal{B}'\mathcal{B}}[\mathbf{v}]_{\mathcal{B}'} = [\mathbf{v}]_{\mathcal{B}} \tag{4.14}$$

and

$$\mathbf{I}_{\mathcal{BB}'}\mathbf{I}_{\mathcal{B}'\mathcal{B}}[\mathbf{v}]_{\mathcal{B}'} = \mathbf{I}_{\mathcal{BB}'}[\mathbf{v}]_{\mathcal{B}} = [\mathbf{v}]_{\mathcal{B}'} \tag{4.15}$$

for all $\mathbf{v} \in V$.

Let $n = \dim(V)$, and fix $\mathbf{x} \in \mathbb{F}^n$. By Theorem 4.11 the coordinate maps $\varphi_{\mathcal{B}}, \varphi_{\mathcal{B}'} : V \to \mathbb{F}^n$ are isomorphisms, and so there exist unique vectors $\mathbf{u}, \mathbf{u}' \in V$ such that

$$\varphi_{\mathcal{B}}(\mathbf{u}) = [\mathbf{u}]_{\mathcal{B}} = \mathbf{x} \quad \text{and} \quad \varphi_{\mathcal{B}'}(\mathbf{u}') = [\mathbf{u}']_{\mathcal{B}'} = \mathbf{x},$$

whereupon equations (4.14) and (4.15) give

$$\mathbf{I}_{\mathcal{B}'\mathcal{B}}\mathbf{I}_{\mathcal{BB}'}\mathbf{x} = \mathbf{x} \quad \text{and} \quad \mathbf{I}_{\mathcal{BB}'}\mathbf{I}_{\mathcal{B}'\mathcal{B}}\mathbf{x} = \mathbf{x},$$

respectively. Since $\mathbf{x} \in \mathbb{F}^n$ is arbitrary, we conclude that

$$(\mathbf{I}_{\mathcal{B}'\mathcal{B}}\mathbf{I}_{\mathcal{BB}'})\mathbf{x} = \mathbf{x} \quad \text{and} \quad (\mathbf{I}_{\mathcal{BB}'}\mathbf{I}_{\mathcal{B}'\mathcal{B}})\mathbf{x} = \mathbf{x}$$

for all $\mathbf{x} \in \mathbb{F}^n$. It follows by Proposition 2.12(1) that

$$\mathbf{I}_{\mathcal{B}'\mathcal{B}}\mathbf{I}_{\mathcal{BB}'} = \mathbf{I}_n \quad \text{and} \quad \mathbf{I}_{\mathcal{BB}'}\mathbf{I}_{\mathcal{B}'\mathcal{B}} = \mathbf{I}_n,$$

and therefore $\mathbf{I}_{\mathcal{BB}'}$ is invertible with $\mathbf{I}_{\mathcal{BB}'}^{-1} = \mathbf{I}_{\mathcal{B}'\mathcal{B}}$. ■

Now suppose that $L$ is a linear operator on a vector space $V$, which is to say $L$ is a linear mapping $V \to V$. Let $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be an ordered basis for $V$. For any $\mathbf{v} \in V$ we have $L(\mathbf{v}) \in V$ given by

$$[L(\mathbf{v})]_{\mathcal{B}} = [L]_{\mathcal{B}}[\mathbf{v}]_{\mathcal{B}},$$

where

$$[L]_{\mathcal{B}} = \Big[ \big[L(\mathbf{v}_1)\big]_{\mathcal{B}} \ \cdots \ \big[L(\mathbf{v}_n)\big]_{\mathcal{B}} \Big]$$

by Corollary 4.21. If $\mathcal{B}' = (\mathbf{v}_1', \ldots, \mathbf{v}_n')$ is another ordered basis for $V$, then another corresponding matrix $[L]_{\mathcal{B}'}$ is obtained for the operator $L$:

$$[L]_{\mathcal{B}'} = \Big[ \big[L(\mathbf{v}_1')\big]_{\mathcal{B}'} \ \cdots \ \big[L(\mathbf{v}_n')\big]_{\mathcal{B}'} \Big],$$

where for any $\mathbf{v} \in V$ we have $L(\mathbf{v}) \in V$ given by

$$[L(\mathbf{v})]_{\mathcal{B}'} = [L]_{\mathcal{B}'}[\mathbf{v}]_{\mathcal{B}'}.$$

We would like to determine the relationship between $[L]_{\mathcal{B}}$ and $[L]_{\mathcal{B}'}$.

Recall that if $\mathbf{AB}$ is defined and $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$, then by Proposition 2.6

$$\mathbf{AB} = \mathbf{A}\big[\mathbf{b}_1 \ \cdots \ \mathbf{b}_n\big] = \big[\mathbf{Ab}_1 \ \cdots \ \mathbf{Ab}_n\big].$$

We therefore have

$$\begin{aligned}
\mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}} &= \mathbf{I}_{\mathcal{B}\mathcal{B}'}\Big[ \big[L(\mathbf{v}_1)\big]_{\mathcal{B}} \ \cdots \ \big[L(\mathbf{v}_n)\big]_{\mathcal{B}} \Big] \\
&= \Big[ \mathbf{I}_{\mathcal{B}\mathcal{B}'}\big[L(\mathbf{v}_1)\big]_{\mathcal{B}} \ \cdots \ \mathbf{I}_{\mathcal{B}\mathcal{B}'}\big[L(\mathbf{v}_n)\big]_{\mathcal{B}} \Big] \\
&= \Big[ \big[L(\mathbf{v}_1)\big]_{\mathcal{B}'} \ \cdots \ \big[L(\mathbf{v}_n)\big]_{\mathcal{B}'} \Big] = [L]_{\mathcal{B}\mathcal{B}'},
\end{aligned} \tag{4.16}$$

the last equality a direct consequence of Theorem 4.20. On the other hand,

$$\begin{aligned}
[L]_{\mathcal{B}'}\mathbf{I}_{\mathcal{B}\mathcal{B}'} &= [L]_{\mathcal{B}'}\Big[ [\mathbf{v}_1]_{\mathcal{B}'} \ \cdots \ [\mathbf{v}_n]_{\mathcal{B}'} \Big] = \Big[ [L]_{\mathcal{B}'}[\mathbf{v}_1]_{\mathcal{B}'} \ \cdots \ [L]_{\mathcal{B}'}[\mathbf{v}_n]_{\mathcal{B}'} \Big] \\
&= \Big[ \big[L(\mathbf{v}_1)\big]_{\mathcal{B}'} \ \cdots \ \big[L(\mathbf{v}_n)\big]_{\mathcal{B}'} \Big] = [L]_{\mathcal{B}\mathcal{B}'}
\end{aligned} \tag{4.17}$$

Comparing (4.16) and (4.17), we have proven the following.

**Proposition 4.32.** *Suppose $V$ is a finite-dimensional vector space and $L \in \mathcal{L}(V)$. If $\mathcal{B}$ and $\mathcal{B}'$ are ordered bases for $V$, then*

$$\mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}} = [L]_{\mathcal{B}'}\mathbf{I}_{\mathcal{B}\mathcal{B}'} = [L]_{\mathcal{B}\mathcal{B}'}.$$

Note that $[L]_{\mathcal{B}\mathcal{B}'}$ is the matrix corresponding to the operator $L : V \to V$ in the case when each input $\mathbf{v}$ for $L$ is given in $\mathcal{B}$-coordinates but the output $L(\mathbf{v})$ is given in $\mathcal{B}'$-coordinates. That is, the $V$ comprising the domain of $L$ has basis $\mathcal{B}$ and the $V$ comprising the codomain of $L$ has basis $\mathcal{B}'$!

**Corollary 4.33.** *Suppose $V$ is a finite-dimensional vector space and $L \in \mathcal{L}(V)$. If $\mathcal{B}$ and $\mathcal{B}'$ are ordered bases for $V$, then*

$$[L]_{\mathcal{B}'} = \mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}}\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}.$$

**Proof.** Suppose that $\mathcal{B}$ and $\mathcal{B}'$ are ordered bases for $V$. Then $\mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}} = [L]_{\mathcal{B}'}\mathbf{I}_{\mathcal{B}\mathcal{B}'}$ by Proposition 4.32, and thus

$$\mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}} = [L]_{\mathcal{B}'}\mathbf{I}_{\mathcal{B}\mathcal{B}'} \quad \Rightarrow \quad \mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}}\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1} = [L]_{\mathcal{B}'}\mathbf{I}_{\mathcal{B}\mathcal{B}'}\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1} \quad \Rightarrow \quad [L]_{\mathcal{B}'} = \mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}}\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}$$

since the matrix $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$ is invertible by Proposition 4.31. ∎

## Problems

1. The ordered sets
$$\mathcal{E} = \left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right) \quad \text{and} \quad \mathcal{B} = \left(\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}-2\\1\end{bmatrix}\right)$$
are bases for $\mathbb{R}^2$ (the former being the standard basis).
   (a) Find the change of basis matrix $\mathbf{I}_{\mathcal{E}\mathcal{B}}$ for changing from the basis $\mathcal{E}$ to the basis $\mathcal{B}$.
   (b) Use $\mathbf{I}_{\mathcal{E}\mathcal{B}}$ to find the $\mathcal{B}$-coordinates of $\mathbf{x} = [2, -5]^\top$.
   (c) Find $\mathbf{I}_{\mathcal{B}\mathcal{E}}$ using Proposition 4.31.

2. The ordered sets
$$\mathcal{B} = \left(\begin{bmatrix}7\\5\end{bmatrix}, \begin{bmatrix}-3\\-1\end{bmatrix}\right) \quad \text{and} \quad \mathcal{C} = \left(\begin{bmatrix}1\\-5\end{bmatrix}, \begin{bmatrix}-2\\2\end{bmatrix}\right)$$
are bases for $\mathbb{R}^2$. Find the change of basis matrices $\mathbf{I}_{\mathcal{B}\mathcal{C}}$ and $\mathbf{I}_{\mathcal{C}\mathcal{B}}$.

## 4.5 – The Rank-Nullity Theorem

Given a matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$, recall from §3.5 that the nullity of $\mathbf{A}$ is defined to be $\text{nullity}(\mathbf{A}) = \dim(\text{Nul}(\mathbf{A}))$, and also recall from §3.6 that the rank of $\mathbf{A}$ may be characterized as $\text{rank}(\mathbf{A}) = \dim(\text{Col}(\mathbf{A}))$. We now attribute similar terminology to linear mappings.

**Definition 4.34.** *Let $L : V \to W$ be a linear mapping. The* ***rank*** *of $L$ is the dimension of the image of $L$,*

$$\text{rank}(L) = \dim(\text{Img}(L)),$$

*and the* ***nullity*** *of $L$ is the dimension of the null space of $L$,*

$$\text{nullity}(L) = \dim(\text{Nul}(L)).$$

From here onward we will use the new notation $\text{rank}(L)$ and $\text{nullity}(L)$ interchangeably with the old notation $\dim(\text{Img}(L))$ and $\dim(\text{Nul}(L))$, since both are used extensively in the literature. The motivation behind Definition 4.34 will become more apparent presently.

In the statement of the next proposition we take

$$[\text{Img}(L)]_{\mathcal{C}} = \varphi_{\mathcal{C}}\big(\text{Img}(L)\big) = \{\varphi_{\mathcal{C}}(\mathbf{w}) : \mathbf{w} \in \text{Img}(L)\} = \{[\mathbf{w}]_{\mathcal{C}} : \mathbf{w} \in \text{Img}(L)\}.$$

**Proposition 4.35.** *Let $V$ and $W$ be finite-dimensional vector spaces with ordered bases $\mathcal{B}$ and $\mathcal{C}$, respectively. If $L : V \to W$ is a linear mapping, then*

$$[\text{Img}(L)]_{\mathcal{C}} = \text{Col}([L]_{\mathcal{BC}}).$$

**Proof.** Let $\mathcal{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$, and suppose $L : V \to W$ is a linear mapping. By Theorem 4.20 we have

$$[L]_{\mathcal{BC}} = \Big[\big[L(\mathbf{b}_1)\big]_{\mathcal{C}} \;\; \cdots \;\; \big[L(\mathbf{b}_n)\big]_{\mathcal{C}}\Big].$$

Now fix $\mathbf{y} \in [\text{Img}(L)]_{\mathcal{C}}$. Then $\mathbf{y} = [\mathbf{w}]_{\mathcal{C}}$ for some $\mathbf{w} \in \text{Img}(L)$, and so there exists some $\mathbf{v} \in V$, where

$$[\mathbf{v}]_{\mathcal{B}} = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix},$$

such that $\mathbf{w} = L(\mathbf{v})$. Since $\mathbf{v} = v_1\mathbf{b}_1 + \cdots + v_n\mathbf{b}_n$, and both $L$ and $\varphi_{\mathcal{C}}$ are linear mappings, we have

$$\mathbf{y} = [\mathbf{w}]_{\mathcal{C}} = [L(v_1\mathbf{b}_1 + \cdots + v_n\mathbf{b}_n)]_{\mathcal{C}} = v_1[L(\mathbf{b}_1)]_{\mathcal{C}} + \cdots + v_n[L(\mathbf{b}_n)]_{\mathcal{C}} \in \text{Col}([L]_{\mathcal{BC}}),$$

and therefore $[\text{Img}(L)]_{\mathcal{C}} \subseteq \text{Col}([L]_{\mathcal{BC}})$.

Conversely, $\mathbf{y} \in \text{Col}([L]_{\mathcal{BC}})$ implies that

$$\mathbf{y} = x_1[L(\mathbf{b}_1)]_{\mathcal{C}} + \cdots + x_n[L(\mathbf{b}_n)]_{\mathcal{C}}$$

for some $x_1, \ldots, x_n \in \mathbb{F}$, and then

$$\mathbf{y} = [L(x_1\mathbf{b}_1 + \cdots + x_n\mathbf{b}_n)]_{\mathcal{C}}$$

for $L(x_1\mathbf{b}_1 + \cdots + x_n\mathbf{b}_n) \in \text{Img}(L)$ shows $\mathbf{y} \in [\text{Img}(L)]_{\mathcal{C}}$. Hence $\text{Col}([L]_{\mathcal{BC}}) \subseteq [\text{Img}(L)]_{\mathcal{C}}$. ■

As a consequence of Proposition 4.35 we have

$$\operatorname{rank}([L]_{\mathcal{BC}}) = \dim(\operatorname{Col}([L]_{\mathcal{BC}})) = \dim([\operatorname{Img}(L)]_{\mathcal{C}}) = \dim(\operatorname{Img}(L)) = \operatorname{rank}(L),$$

where the third equality follows from Example 4.18. Thus the rank of a linear mapping $L : V \to W$ equals the rank of its corresponding matrix with respect to any choice of ordered bases for $V$ and $W$, and so the thrust behind Definition 4.34 should now be clear. We have proven the following.

**Corollary 4.36.** *If $V$ and $W$ are finite-dimensional and $L \in \mathcal{L}(V, W)$, then*

$$\operatorname{rank}(L) = \operatorname{rank}([L]),$$

*where $[L]$ is the matrix corresponding to $L$ with respect to any choice of ordered bases for $V$ and $W$.*

**Theorem 4.37 (Rank-Nullity Theorem for Mappings).** *Let $V$ be a finite-dimensional vector space. If $L : V \to W$ is a linear mapping, then*

$$\operatorname{rank}(L) + \operatorname{nullity}(L) = \dim(V).$$

**Proof.** Let $n = \dim(V)$, $p = \operatorname{nullity}(L)$, and $q = \operatorname{rank}(L)$. We must demonstrate that $n = p+q$.

If $\operatorname{nullity}(L) = n$, then $\operatorname{Nul}(L) = V$ by Theorem 3.56(3); that is, $L(\mathbf{v}) = \mathbf{0}$ for all $\mathbf{v} \in V$, so $\operatorname{Img}(L) = \{\mathbf{0}\}$ and therefore

$$\operatorname{nullity}(L) + \operatorname{rank}(L) = \dim(V) + \dim(\{\mathbf{0}\}) = n + 0 = n = \dim(V)$$

as desired.

If $\operatorname{nullity}(L) = 0$, then $\operatorname{Nul}(L) = \{\mathbf{0}\}$. Let $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis for $V$. The set $\{L(\mathbf{v}_1), \dots, L(\mathbf{v}_n)\} \subseteq \operatorname{Img}(L)$ is linearly independent by Proposition 4.16. Now,

$$S = \operatorname{Span}\{L(\mathbf{v}_1), \dots, L(\mathbf{v}_n)\} \subseteq \operatorname{Img}(L)$$

since $\operatorname{Img}(L)$ is a subspace of $W$. Let $\mathbf{w} \in \operatorname{Img}(L)$, so that $\mathbf{w} = L(\mathbf{v})$ for some $\mathbf{v} \in V$. There exist scalars $c_1, \dots, c_n$ such that $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n$, and then

$$\mathbf{w} = L(\mathbf{v}) = L\left(\sum_{i=1}^{n} c_i\mathbf{v}_i\right) = \sum_{i=1}^{n} c_i L(\mathbf{v}_i) \in \operatorname{Span}\{L(\mathbf{v}_1), \dots, L(\mathbf{v}_n)\} = S$$

shows that $\operatorname{Img}(L) \subseteq S$. Hence $S = \operatorname{Img}(L)$ and we've shown that $S$ is a basis for $\operatorname{Img}(L)$. Therefore

$$\operatorname{nullity}(L) + \operatorname{rank}(L) = 0 + |S| = 0 + n = \dim(V)$$

once again.

Finally, assume that $0 < \operatorname{nullity}(L) < n$, so that $\operatorname{Nul}(L)$ is neither $\{\mathbf{0}\}$ nor $V$. Since $\operatorname{Nul}(L) \neq V$ there exists some $\mathbf{v} \in V$ such that $L(\mathbf{v}) \neq \mathbf{0}$, which implies that $\operatorname{Img}(L) \neq \{\mathbf{0}\}$ and hence $\operatorname{rank}(L) = q \geq 1$. Also $\operatorname{Nul}(L) \neq \{\mathbf{0}\}$ implies that $\operatorname{nullity}(L) = p \geq 1$. Thus $\operatorname{Img}(L)$ has some basis $\{\mathbf{w}_1, \dots, \mathbf{w}_q\} \neq \varnothing$, and $\operatorname{Nul}(L)$ has some basis $\{\mathbf{u}_1, \dots, \mathbf{u}_p\} \neq \varnothing$. Since $\{\mathbf{w}_1, \dots, \mathbf{w}_q\} \subseteq \operatorname{Img}(L)$, for each $1 \leq i \leq q$ there exists some $\mathbf{v}_i \in V$ such that $L(\mathbf{v}_i) = \mathbf{w}_i$. The claim is that

$$\mathcal{B} = \{\mathbf{u}_1, \dots, \mathbf{u}_p, \mathbf{v}_1, \dots, \mathbf{v}_q\} \tag{4.18}$$

is a basis for $V$.

Let $\mathbf{v} \in V$. Then $L(\mathbf{v}) = \mathbf{w}$ for some $\mathbf{w} \in W$, and since $\mathbf{w} \in \mathrm{Img}(L)$ there exist scalars $b_1, \ldots, b_q$ such that

$$\mathbf{w} = b_1\mathbf{w}_1 + \cdots + b_q\mathbf{w}_q.$$

Hence, by the linearity of $L$,

$$L(\mathbf{v}) = \mathbf{w} = b_1 L(\mathbf{v}_1) + \cdots + b_q L(\mathbf{v}_q) = L(b_1\mathbf{v}_1 + \cdots + b_q\mathbf{v}_q),$$

and so

$$L(\mathbf{v} - (b_1\mathbf{v}_1 + \cdots + b_q\mathbf{v}_q)) = L(\mathbf{v}) - L(b_1\mathbf{v}_1 + \cdots + b_q\mathbf{v}_q) = \mathbf{0}.$$

So we have $\mathbf{v} - (b_1\mathbf{v}_1 + \cdots + b_q\mathbf{v}_q) \in \mathrm{Nul}(L)$, and since $\{\mathbf{u}_1, \ldots, \mathbf{u}_p\}$ is a basis for $\mathrm{Nul}(L)$ there exist scalars $a_1, \ldots, a_p$ such that

$$\mathbf{v} - (b_1\mathbf{v}_1 + \cdots + b_q\mathbf{v}_q) = a_1\mathbf{u}_1 + \cdots + a_p\mathbf{u}_p.$$

From this we obtain

$$\mathbf{v} = a_1\mathbf{u}_1 + \cdots + a_p\mathbf{u}_p + b_1\mathbf{v}_1 + \cdots + b_q\mathbf{v}_q \in \mathrm{Span}\{\mathbf{u}_1, \ldots, \mathbf{u}_p, \mathbf{v}_1, \ldots, \mathbf{v}_q\},$$

and therefore

$$V = \mathrm{Span}\{\mathbf{u}_1, \ldots, \mathbf{u}_p, \mathbf{v}_1, \ldots, \mathbf{v}_q\}.$$

It remains to shows that $\mathbf{u}_1, \ldots, \mathbf{u}_p, \mathbf{v}_1, \ldots, \mathbf{v}_q$ are linearly independent. Suppose that

$$a_1\mathbf{u}_1 + \cdots + a_p\mathbf{u}_p + b_1\mathbf{v}_1 + \cdots + b_q\mathbf{v}_q = \mathbf{0}. \tag{4.19}$$

Then

$$\begin{aligned}
\mathbf{0} &= L(a_1\mathbf{u}_1 + \cdots + a_p\mathbf{u}_p + b_1\mathbf{v}_1 + \cdots + b_q\mathbf{v}_q) \\
&= L(a_1\mathbf{u}_1 + \cdots + a_p\mathbf{u}_p) + L(b_1\mathbf{v}_1 + \cdots + b_q\mathbf{v}_q) \\
&= a_1 L(\mathbf{u}_1) + \cdots + a_p L(\mathbf{u}_p) + b_1 L(\mathbf{v}_1) + \cdots + b_q L(\mathbf{v}_q) \\
&= a_1\mathbf{0} + \cdots + a_p\mathbf{0} + b_1\mathbf{w}_1 + \cdots + b_q\mathbf{w}_q \\
&= b_1\mathbf{w}_1 + \cdots + b_q\mathbf{w}_q,
\end{aligned}$$

and since $\mathbf{w}_1, \ldots, \mathbf{w}_q$ are linearly independent we obtain $b_1 = \cdots = b_q = 0$. Now (4.19) becomes $a_1\mathbf{u}_1 + \cdots + a_p\mathbf{u}_p = 0$, but since $\mathbf{u}_1, \ldots, \mathbf{u}_p$ are linearly independent we obtain $a_1 = \cdots = a_p = 0$. Hence all coefficients in (4.19) are zero and we conclude that the set $\mathcal{B}$ in (4.18) is a linearly independent set.

We have now shown that $\mathcal{B}$ is a basis for $V$, from which is follows that

$$\dim(V) = |\mathcal{B}| = p + q = \mathrm{nullity}(L) + \mathrm{rank}(L)$$

and the proof is done. ∎

Notice that the rank-nullity theorem we have just proved holds even in the case when $W$ is an infinite-dimensional vector space!

**Example 4.38.** Recall the mapping $T : \mathbb{F}^{n\times n} \to \mathbb{F}^{n\times n}$ given by

$$T(\mathbf{A}) = \frac{\mathbf{A} - \mathbf{A}^\top}{2}.$$

in Example 4.17. We found that $\text{Nul}(T) = \text{Sym}_n(\mathbb{F})$ in part (b) of the example, and so by Theorem 4.37 we obtain

$$\dim(\text{Img}(T)) = \dim(\mathbb{F}^{n\times n}) - \dim(\text{Nul}(T)) = n^2 - \frac{n(n+1)}{2} = \frac{n(n-1)}{2},$$

recalling from Example 3.48 that $\dim(\mathbb{F}^{n\times n}) = n^2$. We see that, with Theorem 4.37 in hand, the determination of $\dim(\text{Img}(T))$ does not depend on knowing that $\text{Img}(T) = \text{Skw}_n(\mathbb{F})$. Once the dimensions of a linear mapping's domain and null space are known, the dimension of the image follows immediately. ■

**Example 4.39.** Determine the dimension of the subspace $U$ of $\mathbb{R}^n$ given by

$$U = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{a} \cdot \mathbf{x} = 0\},$$

where $n \geq 1$ and $\mathbf{a} \neq \mathbf{0}$.

**Solution.** Define the mapping $L : \mathbb{R}^n \to \mathbb{R}$ by

$$L(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x},$$

which is easily verified to be linear using properties of the Euclidean dot product established in §1.4: for any $\mathbf{x} = [x_1, \ldots, x_n]$ and $\mathbf{y} = [y_1, \ldots, y_n]$ in $\mathbb{R}^n$ and $c \in \mathbb{R}$ we have

$$L(\mathbf{x} + \mathbf{y}) = \mathbf{a} \cdot (\mathbf{x} + \mathbf{y}) = \mathbf{a} \cdot \mathbf{x} + \mathbf{a} \cdot \mathbf{y} = L(\mathbf{x}) + L(\mathbf{y})$$

and

$$L(c\mathbf{x}) = \mathbf{a} \cdot (c\mathbf{x}) = c(\mathbf{a} \cdot \mathbf{x}) = cL(\mathbf{x}).$$

Moreover,

$$\text{Nul}(L) = \{\mathbf{x} \in \mathbb{R}^n : L(\mathbf{x}) = 0\} = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{a} \cdot \mathbf{x} = 0\} = U.$$

Now, $\text{Img}(L)$ is a subspace of $\mathbb{R}$ by Proposition 4.14. Since $\dim(\mathbb{R}) = 1$, by Theorem 3.56(2) $\dim(\text{Img}(L))$ is either 0 or 1. But $\dim(\text{Img}(L)) = 0$ if and only if $\text{Img}(L) = \{0\}$, which cannot be the case since $\mathbf{a} \neq \mathbf{0}$ implies that

$$L(\mathbf{a}) = \mathbf{a} \cdot \mathbf{a} = \|\mathbf{a}\|^2 \neq 0,$$

and therefore $\dim(\text{Img}(L)) = 1$. (By Theorem 3.56(3) it further follows that $\text{Img}(L) = \mathbb{R}$ since $\dim(\text{Img}(L)) = \dim(\mathbb{R})$, but we do not need this fact.) Recalling that $\dim(\mathbb{R}^n) = n$ and $\text{Nul}(L) = U$, by Theorem 4.37 we have

$$n = \dim(\mathbb{R}^n) = \dim(\text{Nul}(L)) + \dim(\text{Img}(L)) = \dim(U) + 1,$$

and hence $\dim(U) = n - 1$. That is, $U$ is a hyperplane in $\mathbb{R}^n$. ■

**Theorem 4.40 (Rank-Nullity Theorem for Matrices).** *If* $\mathbf{A} \in \mathbb{F}^{m\times n}$*, then*

$$\text{rank}(\mathbf{A}) + \text{nullity}(\mathbf{A}) = n.$$

**Proof.** Suppose that $\mathbf{A} \in \mathbb{F}^{m\times n}$. Let $L : \mathbb{F}^n \to \mathbb{F}^m$ be given by $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$. Then $L$ is a linear mapping such that

$$\mathrm{Nul}(L) = \{\mathbf{x} \in \mathbb{F}^n : L(\mathbf{x}) = \mathbf{0}\} = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{A}\mathbf{x} = \mathbf{0}\} = \mathrm{Nul}(\mathbf{A}).$$

Also by Proposition 4.35 we have

$$\mathrm{Img}(L) = \mathrm{Col}(\mathbf{A}).$$

with respect to the standard bases. Now by the Rank-Nullity Theorem for Mappings we have

$$\begin{aligned} n = \dim(\mathbb{F}^n) &= \mathrm{rank}(L) + \mathrm{nullity}(L) = \dim(\mathrm{Img}(L)) + \dim(\mathrm{Nul}(L)) \\ &= \dim(\mathrm{Col}(\mathbf{A})) + \dim(\mathrm{Nul}(\mathbf{A})) = \mathrm{rank}(\mathbf{A}) + \mathrm{nullity}(\mathbf{A}). \end{aligned}$$

That is, $\mathrm{rank}(\mathbf{A}) + \mathrm{nullity}(\mathbf{A}) = n$, as desired. ■

**Example 4.41.** Find the dimension of the solution space $S$ for the system of equations

$$\begin{cases} 4x_1 + 7x_2 - \pi x_3 = 0 \\ 2x_1 - \phantom{7}x_2 + \phantom{\pi}x_3 = 0 \end{cases}$$

and also find a basis for $S$.

**Solution.** Letting

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \quad \text{and} \quad \mathbf{A} = \begin{bmatrix} 4 & 7 & -\pi \\ 2 & -1 & 1 \end{bmatrix},$$

we find that $S$ is the set of all $\mathbf{x} \in \mathbb{R}^3$ that satisfy the matrix equation $\mathbf{A}\mathbf{x} = \mathbf{0}$, and so $S = \mathrm{Nul}(\mathbf{A})$. By the Rank-Nullity Theorem for Matrices we have

$$\dim(S) = \mathrm{nullity}(\mathbf{A}) = \dim(\mathbb{R}^3) - \mathrm{rank}(\mathbf{A}) = 3 - \mathrm{rank}(\mathbf{A}).$$

Since

$$\mathbf{A} = \begin{bmatrix} 4 & 7 & -\pi \\ 2 & -1 & 1 \end{bmatrix} \xrightarrow{-2r_2+r_1\to r_1} \begin{bmatrix} 0 & 9 & -2-\pi \\ 2 & -1 & 1 \end{bmatrix}$$

and the row rank of the matrix on the right is clearly 2, it follows that $\mathrm{rank}(\mathbf{A}) = 2$ and so $\dim(S) = 3 - 2 = 1$.

Next we set to the task of finding a basis for $S$. From the second equation in the system we have

$$x_2 = 2x_1 + x_3. \tag{4.20}$$

Putting this into the first equation then yields

$$4x_1 + 7(2x_1 + x_3) - \pi x_3 = 0,$$

and thus

$$x_1 = \frac{\pi - 7}{18} x_3. \tag{4.21}$$

Substituting this into (4.20), we get

$$x_2 = 2\left(\frac{\pi - 7}{18} x_3\right) + x_3 = \frac{\pi + 2}{9} x_3. \tag{4.22}$$

From (4.21) and (4.22), replacing $x_3$ with $t$, we find that

$$S = \left\{ t\left[\frac{\pi - 7}{18}, \frac{\pi + 2}{9}, 1\right]^\top : t \in \mathbb{R} \right\}, \tag{4.23}$$

which shows that

$$\mathcal{B} = \left\{ \left[\frac{\pi - 7}{18}, \frac{\pi + 2}{9}, 1\right]^\top \right\}$$

would qualify as a basis for $S$. This is not the only possibility, however, since any nonzero element of $S$ will span $S$. For instance, if we set $t = 18$ we find from (4.23) that $[\pi - 7, 2\pi + 4, 18]^\top$ is in $S$, and so

$$\mathcal{B} = \left\{ [\pi - 7, 2\pi + 4, 18]^\top \right\}$$

is a basis for $S$. ■

**Example 4.42.** Find the dimension of the subspace of $\mathbb{R}^7$ consisting of all vectors that are orthogonal to the vectors

$$\mathbf{r}_1 = [1, 1, -2, 3, 4, 5, 6]^\top \quad \text{and} \quad \mathbf{r}_2 = [0, 0, 2, 1, 0, 7, 0]^\top,$$

**Solution.** The subspace of $\mathbb{R}^7$ in question consists of the set of vectors

$$S = \{\mathbf{x} \in \mathbb{R}^7 : \mathbf{r}_1 \cdot \mathbf{x} = 0 \text{ and } \mathbf{r}_2 \cdot \mathbf{x} = 0\}.$$

Indeed, if we define $\mathbf{A} \in \mathbb{F}^{m \times n}$ by

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & -2 & 3 & 4 & 5 & 6 \\ 0 & 0 & 2 & 1 & 0 & 7 & 0 \end{bmatrix}$$

then we find that

$$S = \{\mathbf{x} \in \mathbb{R}^7 : \mathbf{A}\mathbf{x} = \mathbf{0}\} = \text{Nul}(\mathbf{A}).$$

By Theorem 4.40 we have

$$\dim(S) = \dim(\text{Nul}(\mathbf{A})) = 7 - \text{rank}(\mathbf{A}).$$

Now, $\mathbf{A}$ is already in row-echelon form, and so it should be clear that the row vectors of $\mathbf{A}$, which are $\mathbf{r}_1^\top$ and $\mathbf{r}_2^\top$, are linearly independent. Thus $\text{rank}(\mathbf{A}) = \text{row-rank}(\mathbf{A}) = 2$, and therefore $\dim(S) = 7 - 2 = 5$. ■

## 4.6 – Dimension and Rank Formulas

**Proposition 4.43.** *If $U$ and $W$ are subspaces of a vector space $V$, then*

$$\dim(U+W) = \dim(U) + \dim(W) - \dim(U \cap W).$$

**Proof.** Suppose that $U$ and $W$ are subspaces of a vector space $V$. The product space $U \times W$ defined in section 3.1 is a vector space, and so we define a mapping $L : U \times W \to V$ by $L(u, w) = u - w$. For any $(\mathbf{u}, \mathbf{w}), (\mathbf{u}', \mathbf{w}') \in U \times W$ and $c \in \mathbb{R}$ we have

$$\begin{aligned} L((\mathbf{u}, \mathbf{w}) + (\mathbf{u}', \mathbf{w}')) &= L(\mathbf{u}+\mathbf{u}', \mathbf{w}+\mathbf{w}') = (\mathbf{u}+\mathbf{u}') - (\mathbf{w}+\mathbf{w}') \\ &= (\mathbf{u}-\mathbf{w}) + (\mathbf{u}'-\mathbf{w}') = L(\mathbf{u}, \mathbf{w}) + L(\mathbf{u}', \mathbf{w}') \end{aligned}$$

and

$$L(c(\mathbf{u}, \mathbf{w})) = L(c\mathbf{u}, c\mathbf{w}) = c\mathbf{u} - c\mathbf{w} = c(\mathbf{u}-\mathbf{w}) = cL(\mathbf{u}, \mathbf{w}),$$

so $L$ is a linear mapping.

If $\mathbf{v} \in \operatorname{Img}(L)$, then there exists some $(\mathbf{u}, \mathbf{w}) \in U \times W$ such that

$$L(\mathbf{u}, \mathbf{w}) = \mathbf{u} - \mathbf{w} = \mathbf{v},$$

so $\mathbf{v} = \mathbf{u} + (-\mathbf{w}) \in U + W$ and we have $\operatorname{Img}(L) \subseteq U + W$. If $\mathbf{v} \in U + W$, then $\mathbf{v} = \mathbf{u} + \mathbf{w}$ for some $\mathbf{u} \in U$ and $\mathbf{w} \in W$, and then

$$L(\mathbf{u}, -\mathbf{w}) = \mathbf{u} - (-\mathbf{w}) = \mathbf{u} + \mathbf{w} = \mathbf{v}$$

shows $\mathbf{v} \in \operatorname{Img}(L)$ and thus $U + W \subseteq \operatorname{Img}(L)$. Therefore $\operatorname{Img}(L) = U + W$.

Let $\mathbf{u} \in U$ and $\mathbf{w} \in W$, and suppose $(\mathbf{u}, \mathbf{w}) \in \operatorname{Nul}(L)$. Then $L(\mathbf{u}, \mathbf{w}) = \mathbf{u} - \mathbf{w} = \mathbf{0}$, which implies that $\mathbf{w} = \mathbf{u}$ and thus $(\mathbf{u}, \mathbf{w}) = (\mathbf{u}, \mathbf{u})$ with $\mathbf{u} \in U \cap W$. From this we conclude that $\operatorname{Nul}(L) \subseteq \{(\mathbf{v}, \mathbf{v}) : \mathbf{v} \in U \cap W\}$, and since the reverse containment is easy to verify we obtain

$$\operatorname{Nul}(L) = \{(\mathbf{v}, \mathbf{v}) : \mathbf{v} \in U \cap W\}. \tag{4.24}$$

Let $\{\mathbf{v}_1, \dots, \mathbf{v}_r\}$ be a basis for $U \cap W$. We wish to show the set

$$B = \{(\mathbf{v}_i, \mathbf{v}_i) : 1 \le i \le r\}$$

is a basis for $\operatorname{Nul}(L)$. Let $(\mathbf{u}, \mathbf{w}) \in \operatorname{Nul}(L)$. By (4.24), $(\mathbf{u}, \mathbf{w}) = (\mathbf{v}, \mathbf{v})$ for some $\mathbf{v} \in U \cap W$, and since there exist scalars $c_1, \dots, c_r$ such that $\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_r\mathbf{v}_r$, we find that

$$(\mathbf{u}, \mathbf{v}) = \left( \sum_{i=1}^r c_i\mathbf{v}_i, \sum_{i=1}^r c_i\mathbf{v}_i \right) = \sum_{i=1}^r (c_i\mathbf{v}_i, c_i\mathbf{v}_i) = \sum_{i=1}^r c_i(\mathbf{v}_i, \mathbf{v}_i)$$

and thus

$$(\mathbf{u}, \mathbf{v}) \in \operatorname{Span}\{(\mathbf{v}_i, \mathbf{v}_i) : 1 \le i \le r\} = \operatorname{Span}(B). \tag{4.25}$$

On the other hand if we suppose that (4.25) is true, so that $(\mathbf{u}, \mathbf{w}) = \sum_{i=1}^r c_i(\mathbf{v}_i, \mathbf{v}_i)$ for some scalars $c_1, \dots, c_r$, then

$$L(\mathbf{u}, \mathbf{w}) = L\left( \sum_{i=1}^r c_i(\mathbf{v}_i, \mathbf{v}_i) \right) = \sum_{i=1}^r c_i L(\mathbf{v}_i, \mathbf{v}_i) = \sum_{i=1}^r c_i(\mathbf{v}_i - \mathbf{v}_i) = \mathbf{0}$$

demonstrates that $(\mathbf{u}, \mathbf{w}) \in \mathrm{Nul}(L)$ and so

$$\mathrm{Nul}(L) = \mathrm{Span}\{(\mathbf{v}_i, \mathbf{v}_i) : 1 \le i \le r\} = \mathrm{Span}(B).$$

Next, set

$$\sum_{i=1}^{r} c_i(\mathbf{v}_i, \mathbf{v}_i) = (\mathbf{0}, \mathbf{0}).$$

Then

$$(\mathbf{0}, \mathbf{0}) = \sum_{i=1}^{r}(c_i\mathbf{v}_i, c_i\mathbf{v}_i) = \left(\sum_{i=1}^{r} c_i\mathbf{v}_i, \sum_{i=1}^{r} c_i\mathbf{v}_i\right),$$

which gives

$$\sum_{i=1}^{r} c_i\mathbf{v}_i = \mathbf{0}$$

and hence $c_1 = \cdots = c_r = 0$ since $\mathbf{v}_1, \ldots, \mathbf{v}_r$ are linearly independent. Therefore $B$ is a linearly independent set and $\mathrm{Span}(B) = \mathrm{Nul}(L)$, which shows that $B$ is a basis for $\mathrm{Nul}(L)$ and then

$$\dim(\mathrm{Nul}(L)) = |B| = r = \dim(U \cap W).$$

Because $L : U \times W \to V$ is a linear mapping,

$$\dim(U \times W) = \dim(\mathrm{Nul}(L)) + \dim(\mathrm{Img}(L))$$

by Theorem 4.37. But $\mathrm{Img}(L) = U + W$ and $\dim(\mathrm{Nul}(L)) = \dim(U \cap W)$, so that

$$\dim(U \times W) = \dim(U \cap W) + \dim(U + W).$$

In §3.5 we established that $\dim(U \times W) = \dim(U) + \dim(W)$, and thus

$$\dim(U) + \dim(W) = \dim(U \cap W) + \dim(U + W)$$

obtains and the proof is done. ■

Recall the concept of a direct sum introduced in section §3.3. The dimension formula furnished by Proposition 4.43 becomes especially nice if a vector space $V$ happens to be the direct sum of two subspaces $U$ and $W$.

**Proposition 4.44.** *Let $V$ be a vector space. If $U$ and $W$ are subspaces such that $V = U \oplus W$, then* $\dim(V) = \dim(U) + \dim(W)$.

**Proof.** From $U \cap W = \{\mathbf{0}\}$ we have $\dim(U \cap W) = 0$, so that

$$\dim(U + W) = \dim(U) + \dim(W)$$

by Proposition 4.43. The conclusion follows from $U + W = V$. ■

**Theorem 4.45.** *Let $V$ be a vector space, and let $U_1, \ldots, U_n$ be subspaces of $V$. Then*

$$V = \bigoplus_{k=1}^{n} U_k \;\Rightarrow\; \dim(V) = \sum_{k=1}^{n} \dim(U_k).$$

**Proof.** The statement of the proposition is trivially true when $n = 1$. Let $n \in \mathbb{N}$ be arbitrary, and suppose the proposition is true for $n$. Let $U_1, \dots, U_{n+1}$ be subspaces of a vector space $V$ such that

$$V = \bigoplus_{k=1}^{n+1} U_k.$$

Define $U = U_1 + \cdots + U_n$ and $W = U_{n+1}$, so that $V = U + W$. Note that $U$ is a subspace of $V$ by Proposition 3.20. By Definition 3.21 it is immediate that

$$U \cap W = U_{n+1} \cap \sum_{k=1}^{n} U_k = \{\mathbf{0}\},$$

and so in fact $V = U \oplus W$.

Let $\mathbf{v} \in U$, so that for $1 \leq k \leq n$ there exist vectors $\mathbf{u}_k \in U_k$ such that

$$\sum_{k=1}^{n} \mathbf{u}_k = \mathbf{v}.$$

Suppose that for $1 \leq k \leq n$ the vectors $\mathbf{u}'_k \in U_k$ are such that

$$\sum_{k=1}^{n} \mathbf{u}'_k = \mathbf{v}$$

also. Setting $\mathbf{u}_{n+1} = \mathbf{u}'_{n+1} = \mathbf{0}$, we obtain

$$\mathbf{v} = \sum_{k=1}^{n+1} \mathbf{u}_k = \sum_{k=1}^{n+1} \mathbf{u}'_k \in V = \bigoplus_{k=1}^{n+1} U_k,$$

and so by Theorem 3.23 we must have $\mathbf{u}_k = \mathbf{u}'_k$ for all $1 \leq k \leq n+1$. Since $\mathbf{v} \in U$ is arbitrary, we conclude that for each $\mathbf{v} \in U$ there exist unique vectors $\mathbf{u}_1 \in U_1, \dots, \mathbf{u}_n \in U_n$ such that $\mathbf{v} = \mathbf{u}_1 + \cdots + \mathbf{u}_n$, and therefore

$$U = \bigoplus_{k=1}^{n} U_k$$

by Theorem 3.23. Now, by Proposition 4.44 and our inductive hypothesis,

$$\dim(V) = \dim(U) + \dim(W) = \sum_{k=1}^{n} \dim(U_k) + \dim(U_{n+1}) = \sum_{k=1}^{n+1} \dim(U_k)$$

as desired. ∎

**Proposition 4.46.** *If $V$ is a subspace of $\mathbb{R}^n$, then $\dim(V) + \dim(V^\perp) = n$.*

**Proof.** Suppose that $V$ is a subspace of $\mathbb{R}^n$. Setting $r = \dim(V)$, so that $r \leq n$, let

$$\mathcal{B}_V = \{\mathbf{b}_1, \dots, \mathbf{b}_r\}$$

be a basis for $V$, where

$$\mathbf{b}_i = \begin{bmatrix} b_{i1} \\ \vdots \\ b_{in} \end{bmatrix}$$

for each $1 \leq i \leq r$. Let $\mathbf{A}$ be the $n \times n$ matrix given by

$$\mathbf{A} = \begin{bmatrix} \mathbf{b}_1^\top \\ \vdots \\ \mathbf{b}_r^\top \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{r1} & \cdots & b_{rn} \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix}$$

and observe that

$$\operatorname{Row}(\mathbf{A}) = \operatorname{Span}\{\mathbf{b}_1, \dots, \mathbf{b}_r, \mathbf{0}\} = \operatorname{Span}\{\mathbf{b}_1, \dots, \mathbf{b}_r\} = V.$$

Now, define $L : \mathbb{R}^n \to \mathbb{R}^n$ to be the linear mapping given by $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$ for all $\mathbf{x} \in \mathbb{R}^n$. Since $\operatorname{Img}(L) = \operatorname{Col}(\mathbf{A})$ by Proposition 4.35, we have

$$\dim(\operatorname{Img}(L)) = \dim(\operatorname{Col}(\mathbf{A})) = \operatorname{rank}(\mathbf{A}) = \dim(\operatorname{Row}(\mathbf{A})) = \dim(V).$$

Suppose $\mathbf{x} \in \operatorname{Nul}(L)$, so that $\mathbf{A}\mathbf{x} = \mathbf{0}$ and we obtain $\mathbf{b}_i^\top \mathbf{x} = 0$ for all $1 \leq i \leq r$. Let $\mathbf{v} \in V$. Then $\mathbf{v} = a_1\mathbf{b}_1 + \cdots + a_r\mathbf{b}_r$ for some $a_1, \dots, a_r \in \mathbb{R}$, and since

$$\mathbf{x} \cdot \mathbf{v} = \mathbf{v}^\top \mathbf{x} = (a_1\mathbf{b}_1^\top + \cdots + a_r\mathbf{b}_r^\top)\mathbf{x} = a_1\mathbf{b}_1^\top\mathbf{x} + \cdots + a_r\mathbf{b}_r^\top\mathbf{x} = a_1(0) + \cdots + a_n(0) = 0$$

we conclude that $\mathbf{x} \in V^\perp$ and so $\operatorname{Nul}(L) \subseteq V^\perp$.

Now suppose that $\mathbf{x} \in V^\perp$. Then $\mathbf{x} \cdot \mathbf{v} = 0$ for all $\mathbf{v} \in V$, and in particular $\mathbf{x} \cdot \mathbf{b}_i = 0$ for each $1 \leq i \leq r$. Thus

$$L(\mathbf{x}) = \mathbf{A}\mathbf{x} = \begin{bmatrix} \mathbf{b}_1^\top\mathbf{x} \\ \vdots \\ \mathbf{b}_r^\top\mathbf{x} \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} \mathbf{x} \cdot \mathbf{b}_1 \\ \vdots \\ \mathbf{x} \cdot \mathbf{b}_r \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \mathbf{0},$$

which shows that $\mathbf{x} \in \operatorname{Nul}(L)$ and so $V^\perp \subseteq \operatorname{Nul}(L)$.

We now have $\operatorname{Nul}(L) = V^\perp$, and so of course $\dim(\operatorname{Nul}(L)) = \dim(V^\perp)$. By Theorem 4.37

$$\dim(\mathbb{R}^n) = \dim(\operatorname{Nul}(L)) + \dim(\operatorname{Img}(L)),$$

and from this we obtain $n = \dim(V^\perp) + \dim(V)$. ■

For the remainder of this section we develop a few formulas involving the ranks of matrices that will be useful later on.

**Theorem 4.47.**

1. *If* $\mathbf{A} \in \mathbb{F}^{n\times n}$ *is invertible, then* $\operatorname{rank}(\mathbf{A}) = \operatorname{rank}(\mathbf{A}^{-1})$.
2. *If* $\mathbf{A} \in \mathbb{F}^{m\times m}$ *is invertible and* $\mathbf{B} \in \mathbb{F}^{m\times n}$*, then* $\operatorname{rank}(\mathbf{AB}) = \operatorname{rank}(\mathbf{B})$.
3. *If* $\mathbf{B} \in \mathbb{F}^{n\times n}$ *is invertible and* $\mathbf{A} \in \mathbb{F}^{m\times n}$*, then* $\operatorname{rank}(\mathbf{AB}) = \operatorname{rank}(\mathbf{A})$.
4. *If* $\mathbf{A}, \mathbf{C} \in \mathbb{F}^{n\times n}$ *are invertible and* $\mathbf{B} \in \mathbb{F}^{n\times n}$*, then* $\operatorname{rank}(\mathbf{ABC}) = \operatorname{rank}(\mathbf{B})$.

**Proof.**
*Proof of Part (1).* Suppose $\mathbf{A} \in \mathbb{F}^{n\times n}$ is invertible. Since $\mathbf{A}^{-1}$ is also invertible, both $\mathbf{A}$ and $\mathbf{A}^{-1}$ are row-equivalent to $\mathbf{I}_n$ by Theorem 2.30, and then by Theorem 3.66 we have $\operatorname{rank}(\mathbf{A}) = \operatorname{rank}(\mathbf{I}_n)$ and $\operatorname{rank}(\mathbf{A}^{-1}) = \operatorname{rank}(\mathbf{I}_n)$. Therefore $\operatorname{rank}(\mathbf{A}) = \operatorname{rank}(\mathbf{A}^{-1}) = n$.

*Proof of Part (2).* Suppose $\mathbf{A} \in \mathbb{F}^{m\times m}$ is invertible and $\mathbf{B} \in \mathbb{F}^{m\times n}$. By the Rank-Nullity Theorem for Matrices,

$$\operatorname{rank}(\mathbf{AB}) + \operatorname{nullity}(\mathbf{AB}) = n \quad \text{and} \quad \operatorname{rank}(\mathbf{B}) + \operatorname{nullity}(\mathbf{B}) = n,$$

and hence

$$\operatorname{rank}(\mathbf{AB}) + \operatorname{nullity}(\mathbf{AB}) = \operatorname{rank}(\mathbf{B}) + \operatorname{nullity}(\mathbf{B}). \tag{4.26}$$

Now, since $\mathbf{A}$ is invertible,

$$\mathbf{A}(\mathbf{Bx}) = \mathbf{0} \;\Rightarrow\; \mathbf{A}^{-1}[\mathbf{A}(\mathbf{Bx})] = \mathbf{A}^{-1}\mathbf{0} \;\Rightarrow\; \mathbf{Bx} = \mathbf{0},$$

and so

$$\mathbf{x} \in \operatorname{Nul}(\mathbf{B}) \;\Leftrightarrow\; \mathbf{Bx} = \mathbf{0} \;\Leftrightarrow\; \mathbf{A}(\mathbf{Bx}) = \mathbf{0} \;\Leftrightarrow\; (\mathbf{AB})\mathbf{x} = \mathbf{0} \;\Leftrightarrow\; \mathbf{x} \in \operatorname{Nul}(\mathbf{AB}),$$

Hence $\operatorname{Nul}(\mathbf{B}) = \operatorname{Nul}(\mathbf{AB})$, so that $\operatorname{nullity}(\mathbf{B}) = \operatorname{nullity}(\mathbf{AB})$, and then (4.26) gives $\operatorname{rank}(\mathbf{AB}) = \operatorname{rank}(\mathbf{B})$.

*Proof of Part (3).* Suppose $\mathbf{B} \in \mathbb{F}^{n\times n}$ is invertible and $\mathbf{A} \in \mathbb{F}^{m\times n}$. Since $\mathbf{B}^\top$ is invertible by Proposition 2.32, we use Problem 3.8.2 and Part (2) to obtain

$$\operatorname{rank}(\mathbf{AB}) = \operatorname{rank}\big((\mathbf{AB})^\top\big) = \operatorname{rank}(\mathbf{B}^\top\mathbf{A}^\top) = \operatorname{rank}(\mathbf{A}^\top) = \operatorname{rank}(\mathbf{A}).$$

*Proof of Part (4).* Suppose $\mathbf{A}, \mathbf{C} \in \mathbb{F}^{n\times n}$ are invertible and $\mathbf{B} \in \mathbb{F}^{n\times n}$. We have

$$\operatorname{rank}(\mathbf{ABC}) = \operatorname{rank}\big(\mathbf{A}(\mathbf{BC})\big) = \operatorname{rank}(\mathbf{BC}) = \operatorname{rank}(\mathbf{B}),$$

where the second equality follows from Part (2), and the third equality follows from Part (3). ∎

## 4.7 – Compositions of Mappings

**Definition 4.48.** *Given mappings $S : X \to Y$ and $T : Y \to Z$, the **composition** of $T$ with $S$ is the mapping $T \circ S : X \to Z$ given by*

$$(T \circ S)(x) = T(S(x))$$

*for all $x \in X$.*

The composition operation $\circ$ is not commutative in general (i.e. $T \circ S$ is generally not the same function as $S \circ T$), but it does have associative and distributive properties as the next two theorems establish.

**Theorem 4.49.** *Let $X_1$, $X_2$, $X_3$, $X_4$ be sets. If $T_1 : X_1 \to X_2$, $T_2 : X_2 \to X_3$, and $T_3 : X_3 \to X_4$ are mappings, then*

$$T_3 \circ (T_2 \circ T_1) = (T_3 \circ T_2) \circ T_1.$$

**Proof.** For any $x \in X_1$,

$$\begin{aligned}(T_3 \circ (T_2 \circ T_1))(x) &= T_3((T_2 \circ T_1)(x)) = T_3(T_2(T_1(x))) \\ &= (T_3 \circ T_2)(T_1(x)) = ((T_3 \circ T_2) \circ T_1)(x).\end{aligned}$$

Therefore $T_3 \circ (T_2 \circ T_1) = (T_3 \circ T_2) \circ T_1$. ■

Given mappings

$$T_1 : X_1 \to X_2, \quad T_2 : X_2 \to X_3, \quad T_3 : X_3 \to X_4,$$

it is routine to write the composition as simply $T_3 \circ T_2 \circ T_1$ without fear of ambiguity. Whether we interpret $T_3 \circ T_2 \circ T_1$ as signifying $T_3 \circ (T_2 \circ T_1)$ or $(T_3 \circ T_2) \circ T_1$ makes no difference according to Theorem 4.49. This idea extends naturally to the composition of any finite number of mappings.

**Theorem 4.50.** *Let $V_1$, $V_2$, $V_3$ be vector spaces over $\mathbb{F}$. Let $S_1, S_2 : V_1 \to V_2$ and $T_1, T_2 : V_2 \to V_3$ be mappings, and let $c \in \mathbb{F}$. Then*

1. $(T_1 \pm T_2) \circ S_1 = T_1 \circ S_1 \pm T_2 \circ S_1$
2. $T_1 \circ (S_1 \pm S_2) = T_1 \circ S_1 \pm T_1 \circ S_2$ *if $T_1$ is linear.*
3. $(cT_1) \circ S_1 = c(T_1 \circ S_1)$
4. $T_1 \circ (cS_1) = c(T_1 \circ S_1)$ *if $T_1$ is linear.*

**Proof.**
*Proof of Part (1).* For any $\mathbf{u} \in V_1$

$$\begin{aligned}((T_1 + T_2) \circ S_1)(\mathbf{u}) &= (T_1 + T_2)(S_1(\mathbf{u})) = T_1(S_1(\mathbf{u})) + T_2(S_1(\mathbf{u})) \\ &= (T_1 \circ S_1)(\mathbf{u}) + (T_2 \circ S_1)(\mathbf{u}) = (T_1 \circ S_1 + T_2 \circ S_1)(\mathbf{u}),\end{aligned}$$

and therefore $(T_1 + T_2) \circ S_1 = T_1 \circ S_1 + T_2 \circ S_1$. The proof that $(T_1 - T_2) \circ S_1 = T_1 \circ S_1 - T_2 \circ S_1$ is similar.

*Proof of Part (2).* For any $\mathbf{u} \in V_1$

$$
\begin{aligned}
(T_1 \circ (S_1 + S_2))(\mathbf{u}) &= T_1((S_1 + S_2)(\mathbf{u})) = T_1(S_1(\mathbf{u})) + S_2(\mathbf{u})) \\
&= T_1(S_1(\mathbf{u})) + T_1(S_2(\mathbf{u})) = (T_1 \circ S_1)(\mathbf{u}) + (T_1 \circ S_2)(\mathbf{u}) \\
&= (T_1 \circ S_1 + T_1 \circ S_2)(\mathbf{u}),
\end{aligned}
$$

where the third equality obtains from the linearity of $T_1$. Therefore

$$T_1 \circ (S_1 + S_2) = T_1 \circ S_1 + T_1 \circ S_2$$

if $T_1$ is linear. The proof that $T_1 \circ (S_1 - S_2) = T_1 \circ S_1 - T_1 \circ S_2$ if $T_1$ is linear is similar.

*Proof of Part (3).* For any $\mathbf{u} \in V_1$

$$((cT_1) \circ S_1)(\mathbf{u}) = (cT_1)(S_1(\mathbf{u})) = cT_1(S_1(\mathbf{u})) = c(T_1 \circ S_1)(\mathbf{u}),$$

and therefore $(cT_1) \circ S_1 = c(T_1 \circ S_1)$.

*Proof of Part (4).* Suppose that $T_1$ is a linear mapping. For any $\mathbf{u} \in V_1$

$$(T_1 \circ (cS_1))(\mathbf{u}) = T_1((cS_1)(\mathbf{u})) = T_1(cS_1(\mathbf{u})) = cT_1(S_1(\mathbf{u})) = c(T_1 \circ S_1)(\mathbf{u}),$$

where the third equality obtains from the linearity of $T_1$. Therefore $T_1 \circ (cS_1) = c(T_1 \circ S_1)$ if $T_1$ is linear. ■

**Proposition 4.51.** *Let $V_1$, $V_2$, $V_3$ be vector spaces over $\mathbb{F}$. If $L_1 : V_1 \to V_2$ and $L_2 : V_2 \to V_3$ are linear mappings, then the composition $L_2 \circ L_1 : V_1 \to V_3$ is linear.*

**Proof.** For any $\mathbf{u}, \mathbf{v} \in V_1$ we have

$$
\begin{aligned}
(L_2 \circ L_1)(\mathbf{u} + \mathbf{v}) &= L_2(L_1(\mathbf{u} + \mathbf{v})) = L_2(L_1(\mathbf{u}) + L_1(\mathbf{v})) \\
&= L_2(L_1(\mathbf{u})) + L_2(L_1(\mathbf{v})) = (L_2 \circ L_1)(\mathbf{u}) + (L_2 \circ L_1)(\mathbf{v}),
\end{aligned}
$$

and for any $c \in \mathbb{F}$ and $\mathbf{u} \in V_1$ we have

$$(L_2 \circ L_1)(c\mathbf{u}) = L_2(L_1(c\mathbf{u})) = L_2(cL_1(\mathbf{u})) = cL_2(L_1(\mathbf{u})) = c(L_2 \circ L_1)(\mathbf{u}).$$

Therefore $L_2 \circ L_1$ is linear. ■

If $L : V \to V$ is a linear operator on a vector space $V$, then $L \circ L$ is likewise a linear operator on $V$, as is $L \circ L \circ L$ and so on. A useful notation is to let $L^2$ denote $L \circ L$, $L^3$ denote $L \circ L \circ L$, and in general

$$L^n = \underbrace{L \circ L \circ \cdots \circ L}_{n\ L\text{'s}}$$

for any $n \in \mathbb{N}$. We also define $L^0 = I_V$, the identity operator on $V$.

A linear operator $\Pi : V \to V$ for which $\Pi^2 = \Pi$ is called a **projection** and is of special theoretical importance. We have

$$\Pi(\Pi(\mathbf{v})) = (\Pi \circ \Pi)(\mathbf{v}) = \Pi^2(\mathbf{v}) = \Pi(\mathbf{v})$$

for any $\mathbf{v} \in V$.

**Example 4.52.** Let $V$ be a vector space, and let $\Pi : V \to V$ be a projection.
(a) Show that $V = \text{Nul}(\Pi) + \text{Img}(\Pi)$.
(b) Show that $\text{Nul}(\Pi) \cap \text{Img}(\Pi) = \{\mathbf{0}\}$.
Therefore $V = \text{Nul}(\Pi) \oplus \text{Img}(\Pi)$.

**Solution.**
(a) Let $\mathbf{v} \in V$, and let $I_V : V \to V$ be the identity operator on $V$ so that $I_V(\mathbf{v}) = \mathbf{v}$. By Theorem 4.50(2) we have

$$\begin{aligned}\Pi(\mathbf{v} - \Pi(\mathbf{v})) &= \Pi(I_V(\mathbf{v}) - \Pi(\mathbf{v})) = \Pi((I_V - \Pi)(\mathbf{v})) = (\Pi \circ (I_V - \Pi))(\mathbf{v}) \\ &= (\Pi \circ I_V - \Pi \circ \Pi)(\mathbf{v}) = (\Pi \circ I_V)(\mathbf{v}) - (\Pi \circ \Pi)(\mathbf{v}) \\ &= \Pi(I_V(\mathbf{v})) - \Pi^2(\mathbf{v}) = \Pi(\mathbf{v}) - \Pi(\mathbf{v}) = \mathbf{0},\end{aligned}$$

and so $\mathbf{v} - \Pi(\mathbf{v}) \in \text{Nul}(\Pi)$. Noting that $\Pi(\mathbf{v}) \in \text{Img}(\Pi)$, we readily obtain

$$\mathbf{v} = (\mathbf{v} - \Pi(\mathbf{v})) + \Pi(\mathbf{v}) \in \text{Nul}(\Pi) + \text{Img}(\Pi).$$

Thus $V \subseteq \text{Nul}(\Pi) + \text{Img}(\Pi)$, and since the reverse containment follows from the closure properties of a vector space, we conclude that $V = \text{Nul}(\Pi) + \text{Img}(\Pi)$.

(b) Let $\mathbf{v} \in \text{Nul}(\Pi) \cap \text{Img}(\Pi)$. Then $\Pi(\mathbf{v}) = \mathbf{0}$ and there exists some $\mathbf{u} \in V$ such that $\Pi(\mathbf{u}) = \mathbf{v}$. With these results and the hypothesis $\Pi^2 = \Pi$, we have

$$\mathbf{0} = \Pi(\mathbf{v}) = \Pi(\Pi(\mathbf{u})) = \Pi^2(\mathbf{u}) = \Pi(\mathbf{u}) = \mathbf{v},$$

implying $\mathbf{v} \in \{\mathbf{0}\}$ and so $\text{Nul}(\Pi) \cap \text{Img}(\Pi) \subseteq \{\mathbf{0}\}$. The reverse containment holds since $\text{Nul}(\Pi)$ and $\text{Img}(\Pi)$ are subspaces of $V$ and so must both contain $\mathbf{0}$. Therefore $\text{Nul}(\Pi) \cap \text{Img}(\Pi) = \{\mathbf{0}\}$. ■

We found in §4.4 (Theorem 4.24) that every linear mapping $L : V \to W$ has a unique corresponding matrix $[L]_{\mathcal{BC}}$ with respect to chosen bases $\mathcal{B}$ and $\mathcal{C}$ for the vector spaces $V$ and $W$, respectively. Let $U$, $V$, and $W$ be vector spaces with bases $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$, respectively. Let $L_1 : U \to V$ have corresponding matrix $[L_1]_{\mathcal{AB}}$ with respect to $\mathcal{A}$ and $\mathcal{B}$, and let $L_2 : V \to W$ have corresponding matrix $[L_2]_{\mathcal{BC}}$ with respect to $\mathcal{B}$ and $\mathcal{C}$, so that

$$[L_1(\mathbf{u})]_{\mathcal{B}} = [L_1]_{\mathcal{AB}}[\mathbf{u}]_{\mathcal{A}} \quad \text{and} \quad [L_2(\mathbf{v})]_{\mathcal{C}} = [L_2]_{\mathcal{BC}}[\mathbf{v}]_{\mathcal{B}}.$$

Thus for any $\mathbf{u} \in U$ we have

$$[(L_2 \circ L_1)(\mathbf{u})]_{\mathcal{C}} = [L_2(L_1(\mathbf{u}))]_{\mathcal{C}} = [L_2]_{\mathcal{BC}}[L_1(\mathbf{u})]_{\mathcal{B}} = [L_2]_{\mathcal{BC}}[L_1]_{\mathcal{AB}}[\mathbf{u}]_{\mathcal{A}}$$

Thus we see that the matrix $\mathbf{A}$ corresponding to $L_2 \circ L_1 : U \to W$ with respect to $\mathcal{A}$ and $\mathcal{C}$ is given by $\mathbf{A} = [L_2]_{\mathcal{BC}}[L_1]_{\mathcal{AB}}$. That is,

$$[L_2 \circ L_1]_{\mathcal{AC}} = [L_2]_{\mathcal{BC}}[L_1]_{\mathcal{AB}}$$

and we have proven the following.

**Proposition 4.53.** *Let $L_1 : V_1 \to V_2$ and $L_2 : V_2 \to V_3$ be linear mappings, and let $\mathcal{B}_i$ be a basis for $V_i$. Then*

$$[L_2 \circ L_1]_{\mathcal{B}_1\mathcal{B}_3} = [L_2]_{\mathcal{B}_2\mathcal{B}_3}[L_1]_{\mathcal{B}_1\mathcal{B}_2}.$$

## 4.8 – The Inverse of a Mapping

**Definition 4.54.** *Let $T : X \to Y$ be a mapping. We say $T$ is **invertible** if there exists a mapping $S : Y \to X$ such that $S \circ T = I_X$ and $T \circ S = I_Y$, in which case $S$ is called the **inverse** of $T$ and we write $S = T^{-1}$.*

**Proposition 4.55.** *If $T : X \to Y$ is an invertible mapping, then*

$$\operatorname{Img}(T^{-1}) = \operatorname{Dom}(T) = X \quad \text{and} \quad \operatorname{Dom}(T^{-1}) = \operatorname{Img}(T) = Y,$$

*and for all $x \in X$, $y \in Y$,*

$$T(x) = y \;\Leftrightarrow\; T^{-1}(y) = x.$$

**Proof.** Suppose that $T : X \to Y$ is invertible, so that there is a mapping $T^{-1} : Y \to X$ such that $T^{-1} \circ T = I_X$ and $T \circ T^{-1} = I_Y$. From this it is immediate that

$$\operatorname{Img}(T^{-1}) \subseteq X = \operatorname{Dom}(T) \quad \text{and} \quad \operatorname{Img}(T) \subseteq Y = \operatorname{Dom}(T^{-1}).$$

Let $x \in X$, so that $T(x) = y$ for some $y \in Y$. Then

$$T^{-1}(y) = T^{-1}(T(x)) = (T^{-1} \circ T)(x) = I_X(x) = x$$

shows that $x \in \operatorname{Img}(T^{-1})$, and so $\operatorname{Img}(T^{-1}) = X$ and

$$T(x) = y \;\Rightarrow\; T^{-1}(y) = x$$

for all $x \in X$.

Next, for any $y \in Y$ we have $T^{-1}(y) = x$ for some $x \in X$, whence

$$T(x) = T(T^{-1}(y)) = (T \circ T^{-1})(y) = I_Y(y) = y$$

shows that $y \in \operatorname{Img}(T)$, and so $\operatorname{Img}(T) = Y$ and

$$T^{-1}(y) = x \;\Rightarrow\; T(x) = y$$

for all $y \in Y$. ■

**Proposition 4.56.** *If $S : X \to Y$ and $T : Y \to Z$ are invertible mappings, then*

$$(T \circ S)^{-1} = S^{-1} \circ T^{-1}.$$

**Proof.** Suppose that $S : X \to Y$ and $T : Y \to Z$ are invertible mappings. Then $S$ and $T$ are bijective, from which it follows that $T \circ S$ is likewise bijective and so $(T \circ S)^{-1} : Z \to X$ exists. That is, $T \circ S$ is invertible.

Let $z \in Z$. Then $(T \circ S)^{-1}(z) = x$ for some $x \in X$, and by repeated use of Proposition 4.55 we obtain

$$\begin{aligned}(T \circ S)^{-1}(z) = x \;&\Leftrightarrow\; (T \circ S)(x) = z \;\Leftrightarrow\; T(S(x)) = z \\ &\Leftrightarrow\; S(x) = T^{-1}(z) \;\Leftrightarrow\; x = S^{-1}(T^{-1}(z)). \\ &\Leftrightarrow\; (S^{-1} \circ T^{-1})(z) = x\end{aligned}$$

Hence

$$(T \circ S)^{-1}(z) = (S^{-1} \circ T^{-1})(z)$$

for all $z \in Z$, and we conclude that $(T \circ S)^{-1} = S^{-1} \circ T^{-1}$. ■

**Proposition 4.57.** *Let $V$ and $W$ be vector spaces over $\mathbb{F}$. If $L : V \to W$ is an invertible linear mapping, then its inverse $L^{-1} : W \to V$ is also linear.*

**Proof.** Suppose that $L : V \to W$ is an invertible linear mapping, and let $L^{-1} : W \to V$ be its inverse. Let $\mathbf{w}_1, \mathbf{w}_2 \in W$. Then $L^{-1}(\mathbf{w}_1)$ and $L^{-1}(\mathbf{w}_2)$ are vectors in $V$, and by the linearity of $L$ we obtain

$$\begin{aligned} L(L^{-1}(\mathbf{w}_1) + L^{-1}(\mathbf{w}_2)) &= L(L^{-1}(\mathbf{w}_1)) + L(L^{-1}(\mathbf{w}_2)) \\ &= (L \circ L^{-1})(\mathbf{w}_1) + (L \circ L^{-1})(\mathbf{w}_2) \\ &= I_W(\mathbf{w}_1) + I_W(\mathbf{w}_2) = \mathbf{w}_1 + \mathbf{w}_2, \end{aligned}$$

and hence

$$L^{-1}(\mathbf{w}_1 + \mathbf{w}_2) = L^{-1}(\mathbf{w}_1) + L^{-1}(\mathbf{w}_2)$$

by Proposition 4.55.

Next, let $\mathbf{w} \in W$ and $c \in \mathbb{F}$. Then $cL^{-1}(\mathbf{w})$ is a vector in $V$, and from

$$L(cL^{-1}(\mathbf{w})) = cL(L^{-1}(\mathbf{w})) = c(L \circ L^{-1})(\mathbf{w}) = cI_W(\mathbf{w}) = c\mathbf{w}$$

we obtain

$$L^{-1}(c\mathbf{w}) = cL^{-1}(\mathbf{w})$$

by Proposition 4.55. ■

There is a close connection between the idea of an invertible linear mapping and that of an invertible matrix which the following theorem makes clear.

**Theorem 4.58.** *Let $V$ and $W$ be vector spaces with ordered bases $\mathcal{B}$ and $\mathcal{C}$, respectively, and suppose that $\dim(V) = \dim(W) = n$ and $L \in \mathcal{L}(V, W)$. Then $L$ is invertible if and only if $[L]_{\mathcal{BC}}$ is invertible, in which case*

$$[L]_{\mathcal{BC}}^{-1} = [L^{-1}]_{\mathcal{CB}}.$$

**Proof.** Suppose that $L$ is invertible. Then there exists a mapping $L^{-1} : W \to V$ such that $L^{-1} \circ L = I_V$ and $L \circ L^{-1} = I_W$, and since $L^{-1}$ is linear by Proposition 4.57 it has a corresponding matrix $[L^{-1}]_{\mathcal{CB}} \in \mathbb{F}^{n \times n}$ with respect to the bases $\mathcal{C}$ and $\mathcal{B}$. For all $\mathbf{v} \in V$ we have

$$[L(\mathbf{v})]_{\mathcal{C}} = [L]_{\mathcal{BC}}[\mathbf{v}]_{\mathcal{B}},$$

and for all $\mathbf{w} \in W$

$$[L^{-1}(\mathbf{w})]_{\mathcal{B}} = [L^{-1}]_{\mathcal{CB}}[\mathbf{w}]_{\mathcal{C}}.$$

Now, for all $\mathbf{w} \in W$,

$$\begin{aligned} \big([L]_{\mathcal{BC}}[L^{-1}]_{\mathcal{CB}}\big)[\mathbf{w}]_{\mathcal{C}} &= [L]_{\mathcal{BC}}\big([L^{-1}]_{\mathcal{CB}}[\mathbf{w}]_{\mathcal{C}}\big) = [L]_{\mathcal{BC}}[L^{-1}(\mathbf{w})]_{\mathcal{B}} \\ &= [L(L^{-1}(\mathbf{w}))]_{\mathcal{C}} = [(L \circ L^{-1})(\mathbf{w})]_{\mathcal{C}} = [I_W(\mathbf{w})]_{\mathcal{C}} = [\mathbf{w}]_{\mathcal{C}}, \end{aligned}$$

which shows that $[L]_{\mathcal{BC}}[L^{-1}]_{\mathcal{CB}} = \mathbf{I}_n$ by Proposition 2.12(1). Similarly, for all $\mathbf{v} \in V$,

$$\begin{aligned}\big([L^{-1}]_{\mathcal{CB}}[L]_{\mathcal{BC}}\big)[\mathbf{v}]_{\mathcal{B}} &= [L^{-1}]_{\mathcal{CB}}\big([L]_{\mathcal{BC}}[\mathbf{v}]_{\mathcal{B}}\big) = [L^{-1}]_{\mathcal{CB}}[L(\mathbf{v})]_{\mathcal{C}} \\ &= [L^{-1}(L(\mathbf{v}))]_{\mathcal{B}} = [(L^{-1} \circ L)(\mathbf{v})]_{\mathcal{B}} = [I_V(\mathbf{v})]_{\mathcal{B}} = [\mathbf{v}]_{\mathcal{B}},\end{aligned}$$

and so $[L^{-1}]_{\mathcal{CB}}[L]_{\mathcal{BC}} = \mathbf{I}_n$. Thus $[L^{-1}]_{\mathcal{CB}}$ is the inverse for $[L]_{\mathcal{BC}}$, which is to say $[L]_{\mathcal{BC}}$ is invertible and

$$[L]_{\mathcal{BC}}^{-1} = [L^{-1}]_{\mathcal{CB}}.$$

For the converse, suppose that $[L]_{\mathcal{BC}}$ is invertible. Then there exists a matrix $[L]_{\mathcal{BC}}^{-1} \in \mathbb{F}^{n\times n}$ such that

$$[L]_{\mathcal{BC}}[L]_{\mathcal{BC}}^{-1} = [L]_{\mathcal{BC}}^{-1}[L]_{\mathcal{BC}} = \mathbf{I}_n.$$

Let $\Lambda : W \to V$ be the linear mapping with corresponding matrix $[L]_{\mathcal{BC}}^{-1}$ with respect to $\mathcal{C}$ and $\mathcal{B}$, so that

$$[\Lambda(\mathbf{w})]_{\mathcal{B}} = [L]_{\mathcal{BC}}^{-1}[\mathbf{w}]_{\mathcal{C}}$$

for each $\mathbf{w} \in W$. For each $\mathbf{w} \in W$ we have

$$[(L \circ \Lambda)(\mathbf{w})]_{\mathcal{C}} = [L(\Lambda(\mathbf{w}))]_{\mathcal{C}} = [L]_{\mathcal{BC}}[\Lambda(\mathbf{w})]_{\mathcal{B}} = [L]_{\mathcal{BC}}[L]_{\mathcal{BC}}^{-1}[\mathbf{w}]_{\mathcal{C}} = [\mathbf{w}]_{\mathcal{C}},$$

and since the coordinate map $\mathbf{w} \mapsto [\mathbf{w}]_{\mathcal{C}}$ is an isomorphism—and hence injective—by Theorem 4.11, it follows that $(L \circ \Lambda)(\mathbf{w}) = \mathbf{w}$. Next, for each $\mathbf{v} \in V$ we have

$$[(\Lambda \circ L)(\mathbf{v})]_{\mathcal{B}} = [\Lambda(L(\mathbf{v}))]_{\mathcal{B}} = [L]_{\mathcal{BC}}^{-1}[L(\mathbf{v})]_{\mathcal{C}} = [L]_{\mathcal{BC}}^{-1}[L]_{\mathcal{BC}}[\mathbf{v}]_{\mathcal{B}} = [\mathbf{v}]_{\mathcal{B}},$$

and since the coordinate map $\mathbf{v} \mapsto [\mathbf{v}]_{\mathcal{B}}$ is an isomorphism it follows that $(\Lambda \circ L)(\mathbf{v}) = \mathbf{v}$. Since $L \circ \Lambda = I_W$ and $\Lambda \circ L = I_V$, we conclude that $\Lambda$ is the inverse of $L$, and therefore $L$ is invertible. Finally, since $\Lambda = L^{-1}$ and $[\Lambda]_{\mathcal{CB}} = [L]_{\mathcal{BC}}^{-1}$, we find that

$$[L]_{\mathcal{BC}}^{-1} = [L^{-1}]_{\mathcal{CB}}$$

once again. ■

The result $[L^{-1}]_{\mathcal{CB}} = [L]_{\mathcal{BC}}^{-1}$ given in the theorem reduces the task of finding the inverse of an invertible linear mapping $L \in \mathcal{L}(V, W)$ to an exercise in finding the inverse of the matrix corresponding to $L$ with respect to $\mathcal{B}$ and $\mathcal{C}$. Indeed, once a linear mapping's corresponding matrix is known, the mapping itself is effectively known.

**Corollary 4.59.** *Let $V$ be a vector space with ordered basis $\mathcal{B}$, and let $L \in \mathcal{L}(V)$. Then $L$ is invertible if and only if $[L]_{\mathcal{B}}$ is invertible, in which case*

$$[L]_{\mathcal{B}}^{-1} = [L^{-1}]_{\mathcal{B}}.$$

**Theorem 4.60.** *A mapping $T : X \to Y$ is invertible if and only if it is a bijection.*

**Theorem 4.61.** *Let $V$ and $W$ be finite-dimensional vector spaces such that* $\dim(V) = \dim(W)$, *and let $L : V \to W$ be a linear mapping.*

1. *If $L$ is injective, then $L$ is invertible.*
2. *If $L$ is surjective, then $L$ is invertible.*

**Proof.**
*Proof of Part (1).* Suppose that $L$ is injective. By Proposition 4.15 $\text{Nul}(L) = \{\mathbf{0}\}$, and so

$$\dim(W) = \dim(V) = \dim(\text{Nul}(L)) + \dim(\text{Img}(L)) = 0 + \dim(\text{Img}(L)) = \dim(\text{Img}(L))$$

by the Rank-Nullity Theorem for Mappings. Now, since $\text{Img}(L)$ is a subspace of $W$ and $\dim(\text{Img}(L)) = \dim(W)$, by Theorem 3.56(3) $\text{Img}(L) = W$ and so $L$ is surjective. Since $L$ is injective and surjective, it follows by Theorem 4.60 that $L$ is invertible.

*Proof of Part(2).* Suppose that $L$ is surjective, so that $\text{Img}(L) = W$. By the Rank-Nullity Theorem for Mappings

$$\dim(V) = \dim(\text{Nul}(L)) + \dim(\text{Img}(L)) = \dim(\text{Nul}(L)) + \dim(W) = \dim(\text{Nul}(L)) + \dim(V),$$

whence $\dim(\text{Nul}(L)) = 0$ and so $\text{Nul}(L) = \{\mathbf{0}\}$. Now, by Proposition 4.15 we conclude that $L$ is injective, and therefore $L$ is invertible by Theorem 4.60. ■

**Proposition 4.62.** *Let $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n \in \mathbb{F}^n$. The $n \times n$ matrix*

$$\mathbf{A} = \begin{bmatrix} \mathbf{a}_1 & \mathbf{a}_2 & \cdots & \mathbf{a}_n \end{bmatrix}$$

*is invertible if and only if $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$ are linearly independent.*

**Proof.** Suppose that $\mathbf{A}$ is invertible. Let $L : \mathbb{F}^n \to \mathbb{F}^n$ be the linear mapping with associated matrix $\mathbf{A}$, so that $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$ for all $\mathbf{x} \in \mathbb{F}^n$. Then $L$ is invertible by Theorem 4.58, and so by Theorem 4.60 $L$ is bijective and we have $\text{Img}(L) = \mathbb{F}^n$. But by Proposition 4.35 we also have $\text{Img}(L) = \text{Col}(\mathbf{A}) = \text{Span}\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$, whence

$$\dim(\text{Span}\{\mathbf{a}_1, \dots, \mathbf{a}_n\}) = \dim(\text{Img}(L)) = \dim(\mathbb{F}^n).$$

Since $\text{Span}\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ is a subspace of $\mathbb{F}^n$ with dimension equal to $\dim(\mathbb{F}^n)$, by Theorem 3.56(3) we conclude that $\text{Span}\{\mathbf{a}_1, \dots, \mathbf{a}_n\} = \mathbb{F}^n$, and thus $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ is a basis for $\mathbb{F}^n$ by Theorem 3.54(2). That is, the vectors $\mathbf{a}_1, \dots, \mathbf{a}_n$ are linearly independent.

Next, suppose that $\mathbf{a}_1, \dots, \mathbf{a}_n$ are linearly independent. Then $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ is a basis for $\mathbb{F}^n$ by Theorem 3.54(1), so that $\text{Span}\{\mathbf{a}_1, \dots, \mathbf{a}_n\} = \mathbb{F}^n$. Let $L : \mathbb{F}^n \to \mathbb{F}^n$ be the linear mapping given by $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$ for all $\mathbf{x} \in \mathbb{F}^n$. By Proposition 4.35

$$\text{Img}(L) = \text{Col}(\mathbf{A}) = \text{Span}\{\mathbf{a}_1, \dots, \mathbf{a}_n\} = \mathbb{F}^n,$$

and thus $L$ is surjective and it follows by Theorem 4.61(2) that $L$ is invertible. Therefore $\mathbf{A}$ is invertible by Theorem 4.58. ■

We can employ Proposition 4.62 to show that a change of basis matrix is always invertible—a fact already established in §4.5 by quite different means. Let $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ and $\mathcal{B}'$ be ordered bases for a vector space $V$. By Theorem 4.27 the change of basis matrix $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$ is given by

$$\mathbf{I}_{\mathcal{B}\mathcal{B}'} = \Big[ [\mathbf{v}_1]_{\mathcal{B}'} \quad \cdots \quad [\mathbf{v}_n]_{\mathcal{B}'} \Big] = \Big[ \varphi_{\mathcal{B}'}(\mathbf{v}_1) \quad \cdots \quad \varphi_{\mathcal{B}'}(\mathbf{v}_n) \Big].$$

The coordinate map $\varphi_{\mathcal{B}'} : V \to \mathbb{F}^n$ is an isomorphism by Theorem 4.11, and so in particular is an injective linear mapping. Thus $\text{Nul}(\varphi_{\mathcal{B}'}) = \{\mathbf{0}\}$ by Proposition 4.15, and since the basis vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent, it follows by Proposition 4.16 that the column vectors $\varphi_{\mathcal{B}'}(\mathbf{v}_1), \ldots, \varphi_{\mathcal{B}'}(\mathbf{v}_n)$ of $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$ are likewise linearly independent. Therefore $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$ is invertible by Proposition 4.62.

We finish this section with a theorem that establishes that, in a certain sense, there is only "one kind" of vector space for each dimension value $n \geq 0$.

**Theorem 4.63.** *Let $V$ and $W$ be finite-dimensional vector spaces. Then $V \cong W$ if and only if $\dim(V) = \dim(W)$.*

**Proof.** Suppose that $V \cong W$, so there exists an isomorphism $L : V \to W$. Since $L$ is injective, $\mathrm{Nul}(L) = \{\mathbf{0}\}$ by Proposition 4.15, and then

$$\mathrm{nullity}(L) = \dim(\mathrm{Nul}(L)) = 0.$$

Since $L$ is surjective, $\mathrm{Img}(L) = W$, and then

$$\mathrm{rank}(L) = \dim(\mathrm{Img}(L)) = \dim(W).$$

Now, by the Rank-Nullity Theorem for Mappings,

$$\dim(V) = \mathrm{rank}(L) + \mathrm{nullity}(L) = \dim(W) + 0 = \dim(W)$$

as desired.

Now suppose that $\dim(V) = \dim(W) = n$. Let $\mathcal{B}$ be a basis for $V$ and $\mathcal{C}$ a basis for $W$. By Theorem 4.11 the coordinate maps $\varphi_{\mathcal{B}} : V \to \mathbb{F}^n$ and $\varphi_{\mathcal{C}} : W \to \mathbb{F}^n$ are isomorphisms. Since $\varphi_{\mathcal{C}}$ is a bijection, by Theorem 4.60 it is invertible, with the inverse $\varphi_{\mathcal{C}}^{-1} : \mathbb{F}^n \to W$ being a linear mapping by Proposition 4.57. Of course $\varphi_{\mathcal{C}}^{-1}$ is itself invertible with inverse $\varphi_{\mathcal{C}}$, so that Theorem 4.60 implies that $\varphi_{\mathcal{C}}^{-1}$ is bijective and hence an isomorphism. Now, by Proposition 4.51 the composition $\varphi_{\mathcal{C}}^{-1} \circ \varphi_{\mathcal{B}} : V \to W$ is a linear mapping that is easily verified to be an isomorphism, and therefore $V \cong W$. ■

**Example 4.64.** Given vector spaces $V$ and $W$ over $\mathbb{F}$, with $\dim(V) = n$ and $\dim(W) = m$, by Theorem 4.24 we found that $\mathcal{L}(V, W) \cong \mathbb{F}^{m \times n}$. Therefore

$$\dim\big(\mathcal{L}(V, W)\big) = \dim\big(\mathbb{F}^{m \times n}\big) = mn$$

by Theorem 4.63. ■

## 4.9 – Properties of Invertible Operators and Matrices

Linear operators play a central role in the more advanced developments of linear algebra, and so it will be convenient to collect some of their most important general properties into a single theorem.

**Theorem 4.65** (**Invertible Operator Theorem**). *Let $V$ be a finite-dimensional vector space, and let $L \in \mathcal{L}(V)$. Then the following statements are equivalent.*

1. *$L$ is invertible.*
2. *$L$ is an isomorphism.*
3. *$L$ is injective.*
4. *$L$ is surjective.*
5. $\mathrm{Nul}(L) = \{\mathbf{0}\}$.
6. *$[L]_{\mathcal{B}}$ is invertible for any basis $\mathcal{B}$.*
7. *$[L]_{\mathcal{B}}$ is invertible for some basis $\mathcal{B}$.*

**Proof.**
*(1) ⇒ (2):* If $L$ is invertible, then $L$ is bijective by Theorem 4.60, and hence $L$ is an isomorphism by Definition 4.10.

*(2) ⇒ (3):* If $L$ is an isomorphism, then of course it must be injective.

*(3) ⇒ (4):* If $L : V \to V$ is injective, then $L$ is invertible by Theorem 4.61(1). By Theorem 4.60 it follows that $L$ is bijective, and therefore $L$ is surjective.

*(4) ⇒ (5):* If $L : V \to V$ is surjective, then $L$ is invertible by Theorem 4.61(2). By Theorem 4.60 it follows that $L$ is bijective, which implies that $L$ is injective. We conclude that $\mathrm{Nul}(L) = \{\mathbf{0}\}$ by Proposition 4.15.

*(5) ⇒ (6):* Suppose that $\mathrm{Nul}(L) = \{\mathbf{0}\}$, and let $\mathcal{B}$ be any basis for $V$. Now, $L$ is injective by Proposition 4.15, and hence must be invertible by Theorem 4.61(1). The invertibility of $[L]_{\mathcal{B}}$ now follows from Corollary 4.59.

*(6) ⇒ (7):* This is trivial.

*(7) ⇒ (1):* If $[L]_{\mathcal{B}}$ is invertible for some basis $\mathcal{B}$, then $L$ is invertible by Corollary 4.59. ■

The following proposition will be improved on in the next chapter, at which point it will be promoted to a theorem.

**Proposition 4.66** (**Invertible Matrix Proposition**). *Let $\mathbf{A} \in \mathbb{F}^{n\times n}$, and let $L_{\mathbf{A}}$ be the linear operator on $\mathbb{F}^n$ having corresponding matrix $\mathbf{A}$ with respect to the standard basis $\mathcal{E}$ of $\mathbb{F}^n$. Then the following statements are equivalent.*

1. *$\mathbf{A}$ is invertible.*
2. *$\mathbf{A}^\top$ is invertible.*

3. $\mathbf{A}$ *is row-equivalent to* $\mathbf{I}_n$.
4. *The row vectors of* $\mathbf{A}$ *are linearly independent.*
5. $\mathbf{A}$ *is column-equivalent to* $\mathbf{I}_n$.
6. *The column vectors of* $\mathbf{A}$ *are linearly independent.*
7. $\text{col-rank}(\mathbf{A}) = n$.
8. $\text{row-rank}(\mathbf{A}) = n$.
9. $\text{rank}(\mathbf{A}) = n$.
10. *The system* $\mathbf{Ax} = \mathbf{b}$ *has a unique solution for each* $\mathbf{b} \in \mathbb{F}^n$.
11. *The system* $\mathbf{Ax} = \mathbf{0}$ *has only the trivial solution.*
12. $\text{Nul}(\mathbf{A}) = \{\mathbf{0}\}$.
13. $L_{\mathbf{A}} \in \mathcal{L}(\mathbb{F}^n)$ *is invertible.*

**Proof.**
*(1) ⇒ (2):* This follows immediately from Proposition 2.32.

*(2) ⇒ (3):* Suppose $\mathbf{A}^\top$ is invertible. Then by Proposition 2.32 $(\mathbf{A}^\top)^\top$ is invertible, where of course $(\mathbf{A}^\top)^\top = \mathbf{A}$. Now, by Theorem 2.30 the invertibility of $\mathbf{A}$ implies that $\mathbf{A}$ is row-equivalent to $\mathbf{I}_n$.

*(3) ⇒ (4):* Suppose that $\mathbf{A}$ is row-equivalent to $\mathbf{I}_n$. Then $\mathbf{A}$ is invertible by Theorem 2.30, so by Proposition 2.32 $\mathbf{A}^\top$ is invertible, and then by Proposition 4.62 the column vectors of $\mathbf{A}^\top$ are linearly independent. Since the row vectors of $\mathbf{A}$ are the column vectors of $\mathbf{A}^\top$, we conclude that the row vectors of $\mathbf{A}$ are linearly independent.

*(4) ⇒ (5):* Suppose the row vectors of $\mathbf{A}$ are linearly independent. Then the column vectors of $\mathbf{A}^\top$ are linearly independent, whereupon Proposition 4.62 implies that $\mathbf{A}^\top$ is invertible. By Theorem 2.30 $\mathbf{A}^\top$ is row-equivalent to $\mathbf{I}_n$, which is to say there exist elementary matrices $\mathbf{M}_1, \ldots, \mathbf{M}_k$ such that

$$\mathbf{M}_k \cdots \mathbf{M}_2\mathbf{M}_1\mathbf{A}^\top = \mathbf{I}_n,$$

where each left-multiplication by $\mathbf{M}_i$ is an elementary row operation by Definition 2.15. Taking the transpose of each side then yields

$$\mathbf{A}\mathbf{M}_1^\top\mathbf{M}_2^\top \cdots \mathbf{M}_k^\top = \mathbf{I}_n,$$

where each right-multiplication by $\mathbf{M}_i^\top$ is an elementary column operation by Definition 2.15. Therefore $\mathbf{A}$ is column-equivalent to $\mathbf{I}_n$.

*(5) ⇒ (6):* Suppose $\mathbf{A}$ is column-equivalent to $\mathbf{I}_n$. Then

$$\text{col-rank}(\mathbf{A}) = \text{rank}(\mathbf{A}) = \text{rank}(\mathbf{I}_n) = n$$

by the definition of rank and Theorem 3.66, which implies that the $n$ column vectors of $\mathbf{A}$ are linearly independent.

*(6) ⇒ (7):* Suppose the column vectors of $\mathbf{A}$ are linearly independent. There are $n$ column vectors, so $\text{col-rank}(\mathbf{A}) = n$.

*(7) ⇒ (8):* Suppose col-rank$(\mathbf{A}) = n$. Then row-rank$(\mathbf{A}) = n$ by Theorem 3.64.

*(8) ⇒ (9):* Suppose row-rank$(\mathbf{A}) = n$. By definition rank$(\mathbf{A}) =$ row-rank$(\mathbf{A}) = n$.

*(9) ⇒ (10):* Suppose that rank$(\mathbf{A}) = n$. Then col-rank$(\mathbf{A}) = n$, which is to say the dimension of the span of the column vectors of $\mathbf{A}$ is $n$. Since $\mathbf{A}$ has $n$ column vectors in all, it follows that the column vectors of $\mathbf{A}$ are linearly independent, and so by Proposition 4.62 $\mathbf{A}$ is invertible. Thus $\mathbf{A}^{-1}$ exists. Let $\mathbf{b} \in \mathbb{F}^n$ be arbitrary. Then $\mathbf{A}^{-1}\mathbf{b}$ is a solution to the system, for when we substitute $\mathbf{A}^{-1}\mathbf{b}$ for $\mathbf{x}$ in the equation $\mathbf{A}\mathbf{x} = \mathbf{b}$, we obtain

$$\mathbf{A}(\mathbf{A}^{-1}\mathbf{b}) = (\mathbf{A}\mathbf{A}^{-1})\mathbf{b} = \mathbf{I}_n\mathbf{b} = \mathbf{b}.$$

This proves the existence of a solution. As for uniqueness, suppose $\mathbf{x}_1$ and $\mathbf{x}_2$ are solutions to the system, so that $\mathbf{A}\mathbf{x}_1 = \mathbf{b}$ and $\mathbf{A}\mathbf{x}_2 = \mathbf{b}$. Now, for $i \in \{1, 2\}$,

$$\mathbf{A}\mathbf{x}_i = \mathbf{b} \;\Rightarrow\; \mathbf{A}^{-1}(\mathbf{A}\mathbf{x}_i) = \mathbf{A}^{-1}\mathbf{b} \;\Rightarrow\; (\mathbf{A}^{-1}\mathbf{A})\mathbf{x}_i = \mathbf{A}^{-1}\mathbf{b} \;\Rightarrow\; \mathbf{x}_i = \mathbf{A}^{-1}\mathbf{b}.$$

That is, $\mathbf{x}_1 = \mathbf{x}_2 = \mathbf{A}^{-1}\mathbf{b}$, which proves the uniqueness of a solution.

*(10) ⇒ (11):* Suppose that the system $\mathbf{A}\mathbf{x} = \mathbf{b}$ has a unique solution for each $\mathbf{b} \in \mathbb{F}^n$. Then if we choose $\mathbf{b} = \mathbf{0}$, it follows that the system $\mathbf{A}\mathbf{x} = \mathbf{0}$ has a unique solution, and clearly that solution must be the trivial solution $\mathbf{0}$.

*(11) ⇒ (12):* If $\mathbf{A}\mathbf{x} = \mathbf{0}$ admits only the trivial solution, then

$$\text{Nul}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{A}\mathbf{x} = \mathbf{0}\} = \{\mathbf{0}\}$$

obtains immediately.

*(12) ⇒ (13):* Suppose Nul$(\mathbf{A}) = \{\mathbf{0}\}$, and suppose $\mathbf{x} \in \mathbb{F}^n$ is such that $L_{\mathbf{A}}(\mathbf{x}) = \mathbf{0}$. Since

$$L_{\mathbf{A}}(\mathbf{x}) = \mathbf{0} \;\Rightarrow\; \mathbf{A}\mathbf{x} = \mathbf{0} \;\Rightarrow\; \mathbf{x} \in \text{Nul}(\mathbf{A}) \;\Rightarrow\; \mathbf{x} = \mathbf{0},$$

it follows that Nul$(L_{\mathbf{A}}) = \{\mathbf{0}\}$. Therefore $L_{\mathbf{A}}$ must be invertible by the Invertible Operator Theorem.

*(13) ⇒ (1):* Suppose that $L_{\mathbf{A}} \in \mathcal{L}(\mathbb{F}^n)$ is invertible. Then $[L_{\mathbf{A}}]_{\mathcal{E}}$ is invertible by Corollary 4.59, and since $[L_{\mathbf{A}}]_{\mathcal{E}} = \mathbf{A}$ we conclude that $\mathbf{A}$ is invertible. ■

With the help of the Invertible Matrix Proposition we now prove that any square matrix with either a left-inverse or a right-inverse must be invertible,

**Proposition 4.67.** *Let* $\mathbf{A} \in \mathbb{F}^{n\times n}$*. Then the following statements are equivalent:*

1. $\mathbf{A}$ *is invertible.*
2. *There exists some* $\mathbf{D} \in \mathbb{F}^{n\times n}$ *such that* $\mathbf{A}\mathbf{D} = \mathbf{I}_n$*.*
3. *There exists some* $\mathbf{C} \in \mathbb{F}^{n\times n}$ *such that* $\mathbf{C}\mathbf{A} = \mathbf{I}_n$*.*

**Proof.**
*(1) ⇒ (2):* Suppose that $\mathbf{A}$ is invertible. Then by definition there exists some $\mathbf{D} \in \mathbb{F}^{n\times n}$ such that $\mathbf{AD} = \mathbf{DA} = \mathbf{I}_n$.

*(2) ⇒ (1):* Suppose that

$$\mathbf{D} = \begin{bmatrix} \mathbf{d}_1 & \cdots & \mathbf{d}_n \end{bmatrix} \in \mathbb{F}^{n\times n}$$

is such that $\mathbf{AD} = \mathbf{I}_n$. If $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{F}^n$ are such that $\mathbf{a}_1^\top, \ldots, \mathbf{a}_n^\top$ are the row vectors for $\mathbf{A}$, then we have

$$\begin{bmatrix} \mathbf{a}_1^\top \\ \vdots \\ \mathbf{a}_n^\top \end{bmatrix} \begin{bmatrix} \mathbf{d}_1 & \cdots & \mathbf{d}_n \end{bmatrix} = \mathbf{I}_n,$$

and thus

$$\mathbf{a}_i^\top \mathbf{d}_j = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \tag{4.27}$$

Now, let

$$\mathbf{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \in \mathbb{F}^n$$

be arbitrary and consider the system $\mathbf{Ax} = \mathbf{b}$. Choose

$$\mathbf{x} = \sum_{i=1}^n b_i \mathbf{d}_i.$$

Then we obtain

$$\mathbf{Ax} = \begin{bmatrix} \mathbf{a}_1^\top \\ \vdots \\ \mathbf{a}_n^\top \end{bmatrix} \mathbf{x} = \begin{bmatrix} \mathbf{a}_1^\top \mathbf{x} \\ \vdots \\ \mathbf{a}_n^\top \mathbf{x} \end{bmatrix} = \begin{bmatrix} \mathbf{a}_1^\top (\sum_{i=1}^n b_i \mathbf{d}_i) \\ \vdots \\ \mathbf{a}_n^\top (\sum_{i=1}^n b_i \mathbf{d}_i) \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^n b_i (\mathbf{a}_1^\top \mathbf{d}_i) \\ \vdots \\ \sum_{i=1}^n b_i (\mathbf{a}_n^\top \mathbf{d}_i) \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \mathbf{b},$$

where the penultimate equality follows from (4.27). This shows that $\mathbf{Ax} = \mathbf{b}$ has a solution for any $\mathbf{b} \in \mathbb{F}^n$.

Let $L_{\mathbf{A}} \in \mathcal{L}(\mathbb{F}^n)$ be the linear operator with corresponding matrix $\mathbf{A}$ with respect to the standard basis $\mathcal{E}$. For each $\mathbf{b} \in \mathbb{F}^n$ there exists some $\mathbf{x} \in \mathbb{F}^n$ such that $\mathbf{Ax} = \mathbf{b}$, and hence $L_{\mathbf{A}}(\mathbf{x}) = \mathbf{b}$. This shows that $L_{\mathbf{A}}$ is surjective, so $L_{\mathbf{A}}$ is invertible by the Invertible Operator Theorem, and hence $\mathbf{A}$ is invertible by the Invertible Matrix Proposition.

*(1) ⇒ (3):* Suppose that $\mathbf{A}$ is invertible. Then by definition there exists some $\mathbf{C} \in \mathbb{F}^{n\times n}$ such that $\mathbf{CA} = \mathbf{AC} = \mathbf{I}_n$.

*(3) ⇒ (1):* Suppose there exists some $\mathbf{C} \in \mathbb{F}^{n\times n}$ such that $\mathbf{CA} = \mathbf{I}_n$. Then $\mathbf{A}$ is a right-inverse for $\mathbf{C}$, and by the equivalency of parts (1) and (2) it follows that $\mathbf{C}$ is invertible. Thus $\mathbf{C}^{-1}$ exists (and is invertible), and since

$$\mathbf{CA} = \mathbf{I}_n \;\Rightarrow\; \mathbf{C}^{-1}(\mathbf{CA}) = \mathbf{C}^{-1}\mathbf{I}_n \;\Rightarrow\; (\mathbf{C}^{-1}\mathbf{C})\mathbf{A} = \mathbf{C}^{-1} \;\Rightarrow\; \mathbf{A} = \mathbf{C}^{-1},$$

we conclude that $\mathbf{A}$ is invertible. ■

An immediate application of Proposition 4.67 provides something of a converse to Theorem 2.26.

**Proposition 4.68.** *Let* $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{n\times n}$. *If* $\mathbf{AB}$ *is invertible, then* $\mathbf{A}$ *and* $\mathbf{B}$ *are invertible.*

**Proof.** Suppose that $\mathbf{AB}$ is invertible. Then there exists some $\mathbf{D} \in \mathbb{F}^{n\times n}$ such that $(\mathbf{AB})\mathbf{D} = \mathbf{I}_n$, and so by associativity of matrix multiplication we obtain $\mathbf{A}(\mathbf{BD}) = \mathbf{I}_n$. Therefore $\mathbf{A}$ is invertible by Proposition 4.67.

Now, the invertibility of $\mathbf{A}$ means that $\mathbf{A}^{-1}$ exists, and since $\mathbf{A}^{-1}$ and $\mathbf{AB}$ are invertible, by Theorem 2.26 $\mathbf{A}^{-1}(\mathbf{AB})$ is invertible. But

$$\mathbf{A}^{-1}(\mathbf{AB}) = (\mathbf{A}^{-1}\mathbf{A})\mathbf{B} = \mathbf{I}_n\mathbf{B} = \mathbf{B},$$

and therefore $\mathbf{B}$ is invertible. ■

The following proposition (and its corollary) could have been proved at the end of the previous chapter and has wide application in the calculus of manifolds, among other fields.

**Proposition 4.69.** *For* $\mathbf{A} \in \mathbb{F}^{m\times n}$ *let* $1 \le k < \min\{m, n\}$. *Then there is an invertible* $(k+1)\times(k+1)$ *submatrix of* $\mathbf{A}$ *if and only if* $\operatorname{rank}(\mathbf{A}) \ge k+1$.

**Proof.** Suppose $\mathbf{A} = [\mathbf{a}_1 \ \cdots \ \mathbf{a}_n]$ has an invertible $(k+1)\times(k+1)$ submatrix. If the submatrix is formed by the entries that are in rows $i_1, \dots, i_{k+1}$ and columns $j_1, \dots, j_{k+1}$ of $\mathbf{A}$, and we designate the ordered index sets $\alpha = (i_1, \dots, i_{k+1})$ and $\beta = (j_1, \dots, j_{k+1})$, then we may denote the submatrix by $\mathbf{A}[\alpha, \beta]$. Let $\mathbf{A}[\cdot, \beta]$ denote the $m \times (k+1)$ submatrix formed by the entries in rows $1, \dots, m$ (i.e. all the rows) and columns $j_1, \dots, j_{k+1}$, which is to say

$$\mathbf{A}[\cdot, \beta] = \begin{bmatrix} \mathbf{a}_{j_1} & \cdots & \mathbf{a}_{j_{k+1}} \end{bmatrix}.$$

Then $\mathbf{A}[\alpha, \beta]$ is a submatrix of $\mathbf{A}[\cdot, \beta]$, and in particular the $k+1$ row vectors of $\mathbf{A}[\alpha, \beta]$ are row vectors of $\mathbf{A}[\cdot, \beta]$. Now, since $\mathbf{A}[\alpha, \beta]$ is invertible, by the Invertible Matrix Proposition we have $\operatorname{rank}(\mathbf{A}[\alpha, \beta]) = k+1$. Since $\operatorname{rank}(\mathbf{A}[\alpha, \beta])$ equals the dimension of the row space of $\mathbf{A}[\alpha, \beta]$, it follows that the $k+1$ row vectors of $\mathbf{A}[\alpha, \beta]$ are linearly independent, and therefore at least $k+1$ row vectors of $\mathbf{A}[\cdot, \beta]$ are linearly independent. That is, the dimension of the row space of $\mathbf{A}[\cdot, \beta]$ is at least $k+1$, and then we find that

$$\text{col-rank}\big(\mathbf{A}[\cdot, \beta]\big) = \text{row-rank}\big(\mathbf{A}[\cdot, \beta]\big) \ge k+1.$$

In fact, since $\mathbf{A}[\cdot, \beta]$ has precisely $k+1$ column vectors we must have

$$\text{col-rank}\big(\mathbf{A}[\cdot, \beta]\big) = k+1,$$

which is to say the $k+1$ column vectors of $\mathbf{A}[\cdot, \beta]$ are linearly independent. However, the column vectors of $\mathbf{A}[\cdot, \beta]$ are also column vectors of $\mathbf{A}$ itself, and so now we have

$$\operatorname{rank}(\mathbf{A}) = \text{col-rank}(\mathbf{A}) \ge k+1 > k.$$

For the converse, suppose that $\text{rank}(\mathbf{A}) > k$. Then at least $k+1$ column vectors $\mathbf{a}_{j_1}, \ldots, \mathbf{a}_{j_{k+1}}$ of $\mathbf{A}$ are linearly independent, and with $\beta$ defined as before we construct the $n \times (k+1)$ submatrix $\mathbf{A}[\cdot, \beta]$. Since $\text{col-rank}(\mathbf{A}[\cdot, \beta]) = k+1$, it follows that $\text{row-rank}(\mathbf{A}[\cdot, \beta]) = k+1$ also. Thus there are $k+1$ linearly independent row vectors in $\mathbf{A}[\cdot, \beta]$, which we number $i_1, \ldots, i_{k+1}$. With $\alpha$ defined as before, we obtain the $(k+1) \times (k+1)$ submatrix $\mathbf{A}[\alpha, \beta]$ that has $k+1$ linearly independent row vectors. Now,

$$\text{rank}\big(\mathbf{A}[\alpha, \beta]\big) = \text{row-rank}\big(\mathbf{A}[\alpha, \beta]\big) = k+1,$$

and the Invertible Matrix Proposition implies that $\mathbf{A}[\alpha, \beta]$ is invertible. ∎

Applying Proposition 4.69 in the case when $m = \min\{m, n\}$ and $k = m-1$, then we conclude that $\text{rank}(\mathbf{A}) \geq m$ iff some $m \times m$ submatrix of $\mathbf{A}$ is invertible, and thus (since the rank of a matrix cannot exceed its smaller dimension) $\text{rank}(\mathbf{A}) = m$ iff some $m \times m$ submatrix of $\mathbf{A}$ is invertible. A similar conclusion obtains if $n = \min\{m, n\}$. Defining a matrix $\mathbf{A} \in \mathbb{F}^{m \times n}$ to have **full rank** if $\text{rank}(\mathbf{A}) = \min\{m, n\}$ (i.e. $\mathbf{A}$ has the greatest possible rank), we have proved the following.

**Corollary 4.70.** *For $\mathbf{A} \in \mathbb{F}^{m \times n}$ let $k = \min\{m, n\}$. Then $\mathbf{A}$ has full rank if and only if $\mathbf{A}$ has an invertible $k \times k$ submatrix.*

A good exercise is to prove Corollary 4.70 from established principles, and then use it to prove Proposition 4.68. Is the argument any easier than that above?

**Proposition 4.71.** *Let $V$ and $W$ be finite-dimensional vector spaces over $\mathbb{F}$ with bases $\mathcal{B}$ and $\mathcal{C}$, let $L \in \mathcal{L}(V, W)$ be a linear mapping, and let $[L]$ be its $\mathcal{BC}$-matrix.*

1. *If $L$ is injective, then $[L]$ has full rank.*
2. *If $[L]$ has full rank and $\dim(V) \leq \dim(W)$, then $L$ is injective.*

**Proof.**
*Proof of Part (1).* Set $n = \dim(V)$ and $m = \dim(W)$, so that $[L] \in \mathbb{F}^{m \times n}$. Suppose that $L$ is injective. Proposition 4.15 implies that $\text{Nul}(L) = \{\mathbf{0}\}$, and thus $\text{Nul}([L]) = \{\mathbf{0}\}$ as well. This gives $\text{nullity}([L]) = 0$, and so $\text{rank}([L]) = n$ by the Rank-Nullity Theorem for Matrices. Since $n$ is a dimension of $[L]$, it must in fact be the smaller dimension (see remark below) and so we conclude that $[L]$ has full rank.

*Proof of Part (2).* For the converse, suppose that $L$ is not injective. Then $\text{Nul}(L) \neq \{\mathbf{0}\}$ implies $\text{Nul}([L]) \neq \{\mathbf{0}\}$, so that $\text{nullity}([L]) > 0$ and therefore $\text{rank}([L]) < n$ by the Rank-Nullity Theorem for Matrices. If $n = \dim(V) \leq \dim(W) = m$, then it follows that $[L]$ does not have full rank and we are done. ∎

**Remark.** In the proof of the first part of Proposition 4.71, note that $L : V \to L(V)$ is an isomorphism, which is to say $V \cong L(V)$, and so $\dim(L(V)) = \dim(V) = n$ by Theorem 4.63. But $L(V)$ is a vector subspace of $W$, and so $n = \dim(L(V)) \leq \dim(W) = m$ by Theorem 3.56. In short, if $L \in \mathcal{L}(V, W)$ is injective, then $\dim(V) \leq \dim(W)$. A similar truth, left as a problem, states that if $L \in \mathcal{L}(V, W)$ is surjective then $\dim(V) \geq \dim(W)$.

# 5

# Determinants

## 5.1 – Determinants of Low Order

**Definition 5.1.** *The* **$1 \times 1$ *determinant*** *function* $\det_1 : \mathbb{F}^{1\times 1} \to \mathbb{F}$ *is given by*

$$\det_1([a]) = a$$

*for each* $[a] \in \mathbb{F}^{1\times 1}$.

*The* **$2 \times 2$ *determinant*** *function* $\det_2 : \mathbb{F}^{2\times 2} \to \mathbb{F}$ *is given by*

$$\det_2\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc.$$

Generally the scalar $\det_n(\mathbf{A})$ is called the **determinant** of the matrix $\mathbf{A}$, and may also be denoted more simply by $\det(\mathbf{A})$ or $|\mathbf{A}|$.

The $1 \times 1$ determinant function has little practical value and tends to arise only in inductive arguments as in the proof of Theorem 5.4. The $2 \times 2$ determinant function, on the other hand, is highly important, and so it will be the focus of study for the remainder of this section. Henceforth we will denote $\det_2(\mathbf{A})$ simply as $\det(\mathbf{A})$.

## 5.2 – Determinants of Arbitrary Order

The general definition we will give here for the determinant of an $n \times n$ matrix is recursive in nature. That is, for $n \geq 2$, the determinant of an $n \times n$ matrix will be defined in terms of determinants of $(n-1) \times (n-1)$ matrices. Thus determinants of $n \times n$ matrices are ultimately defined in terms of determinants of $1 \times 1$ matrices, and since the determinant of a $1 \times 1$ matrix is defined to equal the sole scalar entry of the matrix, we can see that the definition rests on a firm foundation.

Before stating the definition a bit of notation needs to be established. If $\mathbf{A} = [a_{ij}]$ is an $n \times n$ matrix, then we define $\mathbf{A}_{ij}$ to be the submatrix that results when the $i$th row and $j$th column of $\mathbf{A}$ are deleted. That is,

$$\mathbf{A}_{ij} = \begin{bmatrix} a_{11} & \cdots & a_{1(j-1)} & a_{1(j+1)} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{(i-1)1} & \cdots & a_{(i-1)(j-1)} & a_{(i-1)(j+1)} & \cdots & a_{(i-1)n} \\ a_{(i+1)1} & \cdots & a_{(i+1)(j-1)} & a_{(i+1)(j+1)} & \cdots & a_{(i+1)n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{n(j-1)} & a_{n(j+1)} & \cdots & a_{nn} \end{bmatrix}.$$

We now have what we need to give the general definition for the determinant function.

**Definition 5.2.** *Let $n \geq 2$. The* ***$n \times n$ determinant*** *function* $\det_n : \mathbb{F}^{n\times n} \to \mathbb{F}$ *is given by*

$$\det_n(\mathbf{A}) = \sum_{j=1}^{n} (-1)^{1+j} a_{1j} \det_{n-1}(\mathbf{A}_{1j}) \tag{5.1}$$

*for each $n \times n$ matrix $\mathbf{A}$ with entries in $\mathbb{F}$. The scalar $\det_n(\mathbf{A})$ is called an* ***$n \times n$ determinant****.*

As is our custom we will take the field $\mathbb{F}$ to be $\mathbb{R}$ unless otherwise indicated. Often we will write $\det_n(\mathbf{A})$ as simply $\det(\mathbf{A})$. Other symbols for the determinant of $\mathbf{A}$ are

$$|\mathbf{A}|, \quad \det\left(\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}\right), \quad \text{and} \quad \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}.$$

**Example 5.3.** Given that

$$\mathbf{A} = \begin{bmatrix} -2 & 3 & -1 \\ 0 & 2 & 5 \\ 0 & -6 & 4 \end{bmatrix},$$

evaluate $\det(\mathbf{A})$.

**Solution.** We have

$$\begin{aligned} \det(\mathbf{A}) &= (-1)^{1+1}(-2)\begin{vmatrix} 2 & 5 \\ -6 & 4 \end{vmatrix} + (-1)^{1+2}(3)\begin{vmatrix} 0 & 5 \\ 0 & 4 \end{vmatrix} + (-1)^{1+3}(-1)\begin{vmatrix} 0 & 2 \\ 0 & -6 \end{vmatrix} \\ &= -2\begin{vmatrix} 2 & 5 \\ -6 & 4 \end{vmatrix} - 3\begin{vmatrix} 0 & 5 \\ 0 & 4 \end{vmatrix} - \begin{vmatrix} 0 & 2 \\ 0 & -6 \end{vmatrix} \end{aligned}$$

$$= -2[(2)(4) - (5)(-6)] - 3[(0)(4) - (5)(0)] - [(0)(-6) - (2)(0)]$$
$$= -76,$$

using Definitions 5.2 and 5.1. ■

It is frequently convenient to regard $\det_n : \mathbb{F}^{n\times n} \to \mathbb{F}$ as being a function of the column vectors of a matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$. Thus, if

$$\mathbf{A} = \begin{bmatrix} \mathbf{a}_1 & \cdots & \mathbf{a}_n \end{bmatrix},$$

where $\mathbf{a}_j \in \mathbb{F}^n$ is a column vector for each $1 \le j \le n$, then we define

$$\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_n) = \det_n\left(\begin{bmatrix} \mathbf{a}_1 & \cdots & \mathbf{a}_n \end{bmatrix}\right)$$

so that in fact we have $\det_n : \prod_{j=1}^n \mathbb{F}^n \to \mathbb{F}$. This leads to no ambiguity since there is a natural isomorphism between the vector spaces

$$\mathbb{F}^{n\times n} = \left\{ \begin{bmatrix} \mathbf{x}_1 & \cdots & \mathbf{x}_n \end{bmatrix} : \mathbf{x}_k \in \mathbb{F}^n \text{ for } 1 \le k \le n \right\}$$

and

$$\prod_{j=1}^n \mathbb{F}^n = \{(\mathbf{x}_1, \ldots, \mathbf{x}_n) : \mathbf{x}_k \in \mathbb{F}^n \text{ for } 1 \le k \le n\}$$

that enables us to identify, in particular, the column vectors of any matrix $\mathbf{A} = [a_{ij}]_n$ in $\mathbb{F}^{n\times n}$ with a unique $n$-tuple $(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ of vectors in $\mathbb{F}^n$. We use this natural identification to express certain properties of determinants.

**Theorem 5.4.** *For all $n \in \mathbb{N}$, the determinant function $\det_n : \mathbb{F}^{n\times n} \to \mathbb{F}$ has the following properties, where all vectors represent column vectors.*

DP1. ***Multilinearity.*** *For any $1 \le j \le n$, if $\mathbf{a}_j = \mathbf{u} + \mathbf{v}$ then*

$$\det_n(\mathbf{a}_1, \ldots, \mathbf{u} + \mathbf{v}, \ldots, \mathbf{a}_n) = \det_n(\mathbf{a}_1, \ldots, \mathbf{u}, \ldots, \mathbf{a}_n) + \det_n(\mathbf{a}_1, \ldots, \mathbf{v}, \ldots, \mathbf{a}_n),$$

*and if $\mathbf{a}_j = x\mathbf{u}$ then*

$$\det_n(\mathbf{a}_1, \ldots, x\mathbf{u}, \ldots, \mathbf{a}_n) = x\det_n(\mathbf{a}_1, \ldots, \mathbf{u}, \ldots, \mathbf{a}_n).$$

DP2. ***Alternating.*** *For any $1 \le j < k \le n$,*

$$\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_j, \ldots, \mathbf{a}_k, \ldots, \mathbf{a}_n) = -\det_n(\mathbf{a}_1, \ldots, \underbrace{\mathbf{a}_k}_{j}, \ldots, \underbrace{\mathbf{a}_j}_{k}, \ldots, \mathbf{a}_n).$$

DP3. ***Normalization.***

$$\det_n(\mathbf{I}_n) = 1.$$

DP4. *If $\mathbf{A} = [\mathbf{a}_1 \cdots \mathbf{a}_n]$ with $\mathbf{a}_j = \mathbf{a}_k$ for some $j \ne k$, then $\det_n(\mathbf{A}) = 0$.*

DP5. *For any $x \in \mathbb{F}$ and $j \ne k$,*

$$\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_j, \ldots, \mathbf{a}_n) = \det_n(\mathbf{a}_1, \ldots, \mathbf{a}_j + x\mathbf{a}_k, \ldots, \mathbf{a}_n).$$

DP6. *For any $1 \le j \le n$, if $\mathbf{a}_j = \mathbf{0}$ then*

$$\det_n(\mathbf{a}_1, \ldots, \mathbf{0}, \ldots, \mathbf{a}_n) = 0.$$

**Proof.**
*Proof of DP1.* Given any $u, v \in \mathbb{F}$, we have $[u+v] \in \mathbb{F}^{1\times 1}$ with

$$\det([u+v]) = u + v = \det([u]) + \det([v])$$

by Definition 5.1. Thus DP1 holds in the case when $n = 1$. Suppose that DP1 holds for some arbitrary $n \in \mathbb{N}$. Let

$$\mathbf{A} = [a_{ij}] = [\mathbf{a}_1 \ \cdots \ \mathbf{a}_{n+1}] \in \mathbb{F}^{(n+1)\times(n+1)},$$

fix $k \in \{1, \ldots, n+1\}$, and suppose $\mathbf{a}_k = \mathbf{u} + \mathbf{v}$. For each $1 \le j \le n+1$ define

$$\mathbf{a}'_j = \begin{bmatrix} a_{2j} \\ \vdots \\ a_{(n+1)j} \end{bmatrix} \in \mathbb{F}^n,$$

and also

$$\mathbf{u}' = \begin{bmatrix} u_2 \\ \vdots \\ u_{n+1} \end{bmatrix} \quad \text{and} \quad \mathbf{v}' = \begin{bmatrix} v_2 \\ \vdots \\ v_{n+1} \end{bmatrix}.$$

By Definition 5.2

$$\det(\mathbf{A}) = \sum_{j=1}^{n+1} (-1)^{1+j} a_{1j} \det(\mathbf{A}_{1j}) = \sum_{j=1}^{n+1} (-1)^{1+j} a_{1j} \det(\mathbf{a}'_1, \ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots, \mathbf{a}_{n+1}), \tag{5.2}$$

where it's understood that

$$\det(\mathbf{a}'_1, \ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots, \mathbf{a}_{n+1}) = \det(\mathbf{a}'_2, \ldots, \mathbf{a}_{n+1})$$

if $j = 1$, and

$$\det(\mathbf{a}'_1, \ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots, \mathbf{a}_{n+1}) = \det(\mathbf{a}'_1, \ldots, \mathbf{a}_n)$$

if $j = n+1$.

Now, if $j < k$, then

$$\begin{aligned}
\det(\mathbf{A}_{ij}) &= \det(\mathbf{a}'_1, \ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots, \mathbf{a}'_k, \ldots, \mathbf{a}'_{n+1}) \\
&= \det(\mathbf{a}'_1, \ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots, \mathbf{u}' + \mathbf{v}', \ldots, \mathbf{a}'_{n+1}) \\
&= \det(\ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots, \mathbf{u}', \ldots) + \det(\ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots, \mathbf{v}', \ldots)
\end{aligned}$$

by the inductive hypothesis, since $\mathbf{A}_{ij}$ is an $n \times n$ matrix. Similarly, if $j > k$ then

$$\begin{aligned}
\det(\mathbf{A}_{ij}) &= \det(\mathbf{a}'_1, \ldots, \mathbf{a}'_k, \ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots, \mathbf{a}'_{n+1}) \\
&= \det(\mathbf{a}'_1, \ldots, \mathbf{u}' + \mathbf{v}', \ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots, \mathbf{a}'_{n+1}) \\
&= \det(\ldots, \mathbf{u}', \ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots) + \det(\ldots, \mathbf{v}', \ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots)
\end{aligned}$$

These results, together with equation (5.2), yields

$$\det(\mathbf{A}) = \sum_{j=1}^{k-1} (-1)^{1+j} a_{1j} \det(\mathbf{a}'_1, \ldots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \ldots, \mathbf{u}' + \mathbf{v}', \ldots, \mathbf{a}'_{n+1})$$

$$
\begin{aligned}
&+ (-1)^{1+k} a_{1k} \det(\mathbf{a}_1', \ldots, \mathbf{a}_{k-1}', \mathbf{a}_{k+1}', \ldots, \mathbf{a}_{n+1}') \\
&+ \sum_{j=k+1}^{n+1} (-1)^{1+j} a_{1j} \det(\mathbf{a}_1', \ldots, \mathbf{u}' + \mathbf{v}', \ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots, \mathbf{a}_{n+1}') \\
= &\sum_{j=1}^{k-1} (-1)^{1+j} a_{1j} [\det(\ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots, \mathbf{u}', \ldots) + \det(\ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots, \mathbf{v}', \ldots)] \\
&+ (-1)^{1+k} (u_1 + v_1) \det(\mathbf{a}_1', \ldots, \mathbf{a}_{k-1}', \mathbf{a}_{k+1}', \ldots, \mathbf{a}_{n+1}') \\
&+ \sum_{j=k+1}^{n+1} (-1)^{1+j} a_{1j} [\det(\ldots, \mathbf{u}', \ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots) + \det(\ldots, \mathbf{v}', \ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots)],
\end{aligned}
$$

where we use the fact that $a_{1k} = u_1 + v_1$. Observing that

$$
\det(\mathbf{a}_1', \ldots, \mathbf{a}_{k-1}', \mathbf{a}_{k+1}', \ldots, \mathbf{a}_{n+1}') = \det(\mathbf{A}_{1k}),
$$

we finally obtain

$$
\begin{aligned}
\det(\mathbf{A}) = &\left[ \sum_{j=1}^{k-1} (-1)^{1+j} a_{1j} \det(\ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots, \mathbf{u}', \ldots) + (-1)^{1+k} u_1 \det(\mathbf{A}_{1k}) \right. \\
&\left. + \sum_{j=k+1}^{n+1} (-1)^{1+j} a_{1j} \det(\ldots, \mathbf{u}', \ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots) \right] \\
&+ \left[ \sum_{j=1}^{k-1} (-1)^{1+j} a_{1j} \det(\ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots, \mathbf{v}', \ldots) + (-1)^{1+k} v_1 \det(\mathbf{A}_{1k}) \right. \\
&\left. + \sum_{j=k+1}^{n+1} (-1)^{1+j} a_{1j} \det(\ldots, \mathbf{v}', \ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots) \right] \\
= &\det(\mathbf{a}_1, \ldots, \mathbf{u}, \ldots, \mathbf{a}_{n+1}) + \det(\mathbf{a}_1, \ldots, \mathbf{v}, \ldots, \mathbf{a}_{n+1})
\end{aligned}
$$

That is,

$$
\det(\mathbf{a}_1, \ldots, \mathbf{u} + \mathbf{v}, \ldots, \mathbf{a}_{n+1}) = \det(\mathbf{a}_1, \ldots, \mathbf{u}, \ldots, \mathbf{a}_{n+1}) + \det(\mathbf{a}_1, \ldots, \mathbf{v}, \ldots, \mathbf{a}_{n+1}),
$$

and so the first multilinearity property holds for all $n \geq 1$ by induction.

We now prove the second multilinearity property. We have $\det([xa]) = xa = x\det([a])$ for any $x \in \mathbb{F}$ and $[a] \in \mathbb{F}^{1\times 1}$, so the property holds in the case when $n = 1$. Suppose it holds for some arbitrary $n \in \mathbb{N}$. For $\mathbf{A} \in \mathbb{F}^{(n+1)\times(n+1)}$, $k \in \{1, \ldots, n+1\}$ and $x \in \mathbb{F}$ we have

$$
\begin{aligned}
\det(\mathbf{a}_1, \ldots, x\mathbf{a}_k, \ldots, \mathbf{a}_{n+1}) = &\sum_{j=1}^{k-1} (-1)^{1+j} a_{1j} \det(\mathbf{a}_1', \ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots, x\mathbf{a}_k', \ldots, \mathbf{a}_{n+1}') \\
&+ (-1)^{1+k} x a_{1k} \det(\mathbf{a}_1', \ldots, \mathbf{a}_{k-1}', \mathbf{a}_{k+1}', \ldots, \mathbf{a}_{n+1}') \\
&+ \sum_{j=k+1}^{n+1} (-1)^{1+j} a_{1j} \det(\mathbf{a}_1', \ldots, x\mathbf{a}_k', \ldots, \mathbf{a}_{j-1}', \mathbf{a}_{j+1}', \ldots, \mathbf{a}_{n+1}').
\end{aligned}
$$

Since the determinants in the summations are $n \times n$, we use the inductive hypothesis to obtain

$$\begin{aligned}\det(\mathbf{a}_1, \dots, x\mathbf{a}_k, \dots, \mathbf{a}_{n+1}) &= \sum_{j=1}^{k-1}(-1)^{1+j}xa_{1j}\det(\mathbf{a}'_1, \dots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \dots, \mathbf{a}'_k, \dots, \mathbf{a}'_{n+1}) \\ &\quad + (-1)^{1+k}xa_{1k}\det(\mathbf{a}'_1, \dots, \mathbf{a}'_{k-1}, \mathbf{a}'_{k+1}, \dots, \mathbf{a}'_{n+1}) \\ &\quad + \sum_{j=k+1}^{n+1}(-1)^{1+j}xa_{1j}\det(\mathbf{a}'_1, \dots, \mathbf{a}'_k, \dots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \dots, \mathbf{a}'_{n+1}),\end{aligned}$$

and hence

$$\begin{aligned}\det(\mathbf{a}_1, \dots, x\mathbf{a}_k, \dots, \mathbf{a}_{n+1}) &= x\Bigg[\sum_{j=1}^{k-1}(-1)^{1+j}a_{1j}\det(\mathbf{a}'_1, \dots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \dots, \mathbf{a}'_k, \dots, \mathbf{a}'_{n+1}) \\ &\quad + (-1)^{1+k}a_{1k}\det(\mathbf{a}'_1, \dots, \mathbf{a}'_{k-1}, \mathbf{a}'_{k+1}, \dots, \mathbf{a}'_{n+1}) \\ &\quad + \sum_{j=k+1}^{n+1}(-1)^{1+j}a_{1j}\det(\mathbf{a}'_1, \dots, \mathbf{a}'_k, \dots, \mathbf{a}'_{j-1}, \mathbf{a}'_{j+1}, \dots, \mathbf{a}'_{n+1})\Bigg] \\ &= x\det(\mathbf{a}_1, \dots, \mathbf{a}_{n+1}).\end{aligned}$$

Therefore the second multilinearity property holds for all $n \geq 1$ by induction.

*Proof of DP2.* This is done using induction and careful bookkeeping much as with the proofs of the previous two properties, and so is left as a problem.

*Proof of DP3.* Certainly $\det([1]) = 1$, so normalization holds when $n = 1$. Suppose it holds for some $n \in \mathbb{N}$. Let $\mathbf{I} = \mathbf{I}_{n+1}$, with $ij$-entry denoted by $e_{ij}$. We have $e_{11} = 1$ and $e_{1j} = 0$ for all $2 \leq j \leq n+1$, and so

$$\det(\mathbf{I}) = \sum_{j=1}^{n+1}(-1)^{1+j}e_{1j}\det(\mathbf{I}_{1j}) = \det(\mathbf{I}_{11}) = \det(\mathbf{I}_n) = 1.$$

Therefore the normalization property holds for all $n \in \mathbb{N}$ by induction.

*Proof of DP4.* Let $\mathbf{A} \in \mathbb{F}^{n\times n}$, and fix $1 \leq j < k \leq n$. By the alternating property DP2,

$$\det(\mathbf{A}) = \det(\mathbf{a}_1, \dots, \mathbf{a}_j, \dots, \mathbf{a}_k, \dots, \mathbf{a}_n) = -\det(\mathbf{a}_1, \dots, \mathbf{a}_k, \dots, \mathbf{a}_j, \dots, \mathbf{a}_n),$$

and so if $\mathbf{a}_j = \mathbf{a}_k$ we obtain

$$\det(\mathbf{A}) = -\det(\mathbf{a}_1, \dots, \mathbf{a}_j, \dots, \mathbf{a}_k, \dots, \mathbf{a}_n) = -\det(\mathbf{A}).$$

That is, $2\det(\mathbf{A}) = 0$, and therefore $\det(\mathbf{A}) = 0$.

*Proof of DP5.* Let $\mathbf{A} \in \mathbb{F}^{n\times n}$, and fix $1 \leq j, k \leq n$ with $j \neq k$. For any $x \in \mathbb{F}$ we have by DP1,

$$\det(\mathbf{a}_1, \dots, \underbrace{\mathbf{a}_j + x\mathbf{a}_k}_{j}, \dots, \mathbf{a}_n) = \det(\mathbf{a}_1, \dots, \mathbf{a}_j, \dots, \mathbf{a}_n) + \det(\mathbf{a}_1, \dots, \underbrace{x\mathbf{a}_k}_{j}, \dots, \mathbf{a}_n)$$

$$= \det(\mathbf{a}_1, \ldots, \mathbf{a}_j, \ldots, \mathbf{a}_n) + x \det(\mathbf{a}_1, \ldots, \underbrace{\mathbf{a}_k}_{j}, \ldots, \mathbf{a}_n)$$

The matrix

$$\begin{bmatrix} \mathbf{a}_1 & \cdots & \underbrace{\mathbf{a}_k}_{j} & \cdots & \mathbf{a}_n \end{bmatrix}$$

has $j$th and $k$th column both equal to $\mathbf{a}_k$, so that

$$\det(\mathbf{a}_1, \ldots, \underbrace{\mathbf{a}_k}_{j}, \ldots, \mathbf{a}_n) = 0$$

by DP4, and we obtain

$$\det(\mathbf{a}_1, \ldots, \mathbf{a}_j + x\mathbf{a}_k, \ldots, \mathbf{a}_n) = \det(\mathbf{a}_1, \ldots, \mathbf{a}_j, \ldots, \mathbf{a}_n)$$

as desired.

*Proof of DP6.* Let $\mathbf{A} = [\mathbf{a}_1 \ \cdots \ \mathbf{0} \ \cdots \ \mathbf{a}_n]$, so $\mathbf{a}_j = \mathbf{0}$ for some $1 \leq j \leq n$. By DP1,

$$\begin{aligned} \det(\mathbf{A}) &= \det(\mathbf{a}_1, \ldots, \mathbf{0} + \mathbf{0}, \ldots, \mathbf{a}_n) \\ &= \det(\mathbf{a}_1, \ldots, \mathbf{0}, \ldots, \mathbf{a}_n) + \det(\mathbf{a}_1, \ldots, \mathbf{0}, \ldots, \mathbf{a}_n) \\ &= \det(\mathbf{A}) + \det(\mathbf{A}), \end{aligned}$$

which immediately implies that $\det(\mathbf{A}) = 0$. ■

**Proposition 5.5.** *If $\mathbf{A} \in \mathbb{F}^{n \times n}$ is an upper-triangular or lower-triangular matrix, then*

$$\det(\mathbf{A}) = \prod_{i=1}^{n} a_{ii}.$$

**Proof.** The statement of the proposition is vacuously true in the case when $n = 1$. Let $n \in \mathbb{N}$ be arbitrary and suppose whenever $\mathbf{A} = [a_{ij}]_n$ is an upper-triangular or lower-triangular matrix, then $\det(\mathbf{A}) = a_{11}a_{22} \cdots a_{nn}$.

Suppose that $\mathbf{A} \in \mathbb{F}^{n \times n}$ is an upper-triangular matrix, so that $\mathbf{A} = [a_{ij}]$ such that $a_{ij} = 0$ whenever $i > j$. Now, for all $2 \leq j \leq n + 1$ the matrix $\mathbf{A}_{1j}$ has $\mathbf{0}$ in its first column, so that $\det(\mathbf{A}_{1j}) = 0$ by DP6 and we obtain

$$\det(\mathbf{A}) = \sum_{j=1}^{n+1} (-1)^{1+j} a_{1j} \det(\mathbf{A}_{1j}) = a_{11} \det(\mathbf{A}_{11}). \tag{5.3}$$

Now, $\mathbf{A}_{11}$ is an $n \times n$ upper-triangular matrix,

$$\mathbf{A}_{11} = \begin{bmatrix} a_{22} & \cdots & a_{2(n+1)} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{(n+1)(n+1)} \end{bmatrix},$$

and so by the inductive hypothesis $\det(\mathbf{A}_{11}) = a_{22} \cdots a_{(n+1)(n+1)}$. Then from (5.3) we conclude that

$$\det(\mathbf{A}) = a_{11}a_{22} \cdots a_{(n+1)(n+1)}.$$

Next, suppose that $\mathbf{A}$ is a lower-triangular matrix, so that $a_{ij} = 0$ whenever $i < j$. Then $a_{1j} = 0$ for all $2 \le j \le n$, and since $\mathbf{A}_{11}$ is an $n \times n$ lower-triangular matrix, we once again we obtain

$$\det(\mathbf{A}) = a_{11} \det(\mathbf{A}_{11}) = a_{11}a_{22} \cdots a_{(n+1)(n+1)}$$

as desired. ∎

**Lemma 5.6.** *Define the function* $\det_n' : \mathbb{F}^{n\times n} \to \mathbb{F}$ *by*

$$\det_n'(\mathbf{A}) = \sum_{i=1}^{n} (-1)^{i+1} a_{i1} \det_{n-1}'(\mathbf{A}_{i1}), \tag{5.4}$$

*with* $\det_1'([a]) = a$ *in particular. Then* $\det_n'(\mathbf{A}) = \det_n(\mathbf{A})$ *for all* $n \in \mathbb{N}$ *and* $\mathbf{A} \in \mathbb{F}^{n\times n}$.

**Proof.** First, it can be shown via analogous arguments that the function $\det_n'$ possesses the same six properties listed in Theorem 5.4 that $\det_n$ possesses. Also Proposition 5.5 applies to $\det_n'$, with the proof being symmetric to the one given for $\det_n$.

Fix $n \in \mathbb{N}$ and let $\mathbf{A} \in \mathbb{F}^{n\times n}$. Recall the elementary row and column operations $\mathsf{R1}$, $\mathsf{R2}$, $\mathsf{C1}$, and $\mathsf{C2}$ from Definition 2.15. If $\mathbf{A}'$ is obtained from $\mathbf{A}$ by an application of $\mathsf{C1}$, then by Proposition 2.17(1) and DP5 we have $\det(\mathbf{A}) = \det(\mathbf{A}')$; and if $\mathbf{A}'$ is obtained from $\mathbf{A}$ by an application of $\mathsf{C2}$, then $\det(\mathbf{A}) = -\det(\mathbf{A}')$ by Proposition 2.14(2) and DP2. By Proposition 2.20 and the particulars of its proof, row operations $\mathsf{R1}$ and $\mathsf{R2}$ may be applied to $\mathbf{A}^\top$ to obtain an upper-triangular matrix $\mathbf{U}$, which corresponds to employing a succession of $\mathsf{C1}$ and $\mathsf{C2}$ operations to $\mathbf{A}$ to obtain a lower-triangular matrix

$$\mathbf{L} = \begin{bmatrix} \ell_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ \ell_{n1} & \cdots & \ell_{nn} \end{bmatrix} = \mathbf{U}^\top;$$

that is, $\mathbf{L} = [\ell_{ij}]_n$ with $\ell_{ij} = 0$ for $i < j$. If a total of $k$ $\mathsf{C2}$ operations are performed in doing this, then $\det(\mathbf{A}) = (-1)^k \det(\mathbf{L})$. Now

$$\det(\mathbf{A}) = (-1)^k \det(\mathbf{L}) = (-1)^k \ell_{11}\ell_{22} \cdots \ell_{nn}$$

by Proposition 5.5.

On the other hand, because Theorem 5.4 applies to $\det'$, we have $\det'(\mathbf{A}) = (-1)^k \det'(\mathbf{L})$. And then because Proposition 5.5 also applies to $\det'$, we easily obtain

$$\det'(\mathbf{A}) = (-1)^k \ell_{11}\ell_{22} \cdots \ell_{nn} = \det(\mathbf{A})$$

as claimed. ∎

**Theorem 5.7.** *For any* $\mathbf{A} \in \mathbb{F}^{n\times n}$, $\det_n(\mathbf{A}) = \det_n(\mathbf{A}^\top)$.

**Proof.** Let $\mathbf{A} \in \mathbb{F}^{n\times n}$. Let $a_{ij}^\top$ denote the $ij$-entry for $\mathbf{A}^\top$. Since $a_{1j}^\top = a_{j1}$ and $(\mathbf{A}^\top)_{1j} = (\mathbf{A}_{j1})^\top$ for all $j$,

$$\det_n(\mathbf{A}^\top) = \sum_{j=1}^{n} (-1)^{1+j} a_{1j}^\top \det_{n-1}[(\mathbf{A}^\top)_{1j}] = \sum_{j=1}^{n} (-1)^{1+j} a_{j1} \det_{n-1}[(\mathbf{A}_{j1})^\top].$$

Now, by Lemma 5.6 we have $\det_{n-1}[(\mathbf{A}_{j1})^\top] = \det'_{n-1}[(\mathbf{A}_{j1})^\top]$ so that

$$\det_n(\mathbf{A}^\top) = \sum_{j=1}^{n}(-1)^{1+j}a_{j1}\det'_{n-1}[(\mathbf{A}_{j1})^\top] = \det'_n(\mathbf{A}),$$

and therefore

$$\det_n(\mathbf{A}^\top) = \det_n(\mathbf{A})$$

by another application of Lemma 5.6. ■

**Lemma 5.8.** *For all $n \in \mathbb{N}$ and $1 \le j \le n$, define $\det'_{n,j} : \mathbb{F}^{n\times n} \to \mathbb{F}$ by*

$$\det'_{n,j}(\mathbf{A}) = \sum_{i=1}^{n}(-1)^{i+j}a_{ij}\det'_{n-1,j}(\mathbf{A}_{ij}),$$

*with $\det'_{1,1}([a]) = a$ in particular. Then, for every $n \in \mathbb{N}$, $\det'_{n,j}(\mathbf{A}) = \det'_n(\mathbf{A})$ for all $1 \le j \le n$ and $\mathbf{A} \in \mathbb{F}^{n\times n}$.*

**Proof.** The conclusion is trivially true in the case when $n = 1$, so suppose the conclusion is true for some $n \in \mathbb{N}$. Since $\det'_{n+1,1} = \det'_{n+1}$ by definition, consider $\det'_{n+1,j}$ for some $j \ge 2$. Let $\mathbf{A} = [\mathbf{a}_1 \cdots \mathbf{a}_{n+1}] \in \mathbb{F}^{(n+1)\times(n+1)}$, and let

$$\mathbf{B} = \begin{bmatrix}\mathbf{a}_j & \cdots & \mathbf{a}_{j-1} & \mathbf{a}_1 & \mathbf{a}_{j+1} & \cdots & \mathbf{a}_{n+1}\end{bmatrix}.$$

Since Theorem 5.4—and in particular DP2—applies to $\det'_{n+1}$, we have

$$\det'_{n+1}(\mathbf{A}) = -\det'_{n+1}(\mathbf{B}) = -\sum_{i=1}^{n+1}(-1)^{i+1}a_{ij}\det'_n(\mathbf{B}_{i1}), \tag{5.5}$$

where

$$\mathbf{B}_{i1} = \begin{bmatrix}\mathbf{a}'_2 & \cdots & \mathbf{a}'_{j-1} & \mathbf{a}'_1 & \mathbf{a}'_{j+1} & \cdots & \mathbf{a}'_{n+1}\end{bmatrix},$$

each $\mathbf{a}'_k$ representing $\mathbf{a}_k$ with its $i$th component deleted. A succession of $j-2$ transpositions of the column vectors of $\mathbf{B}_{i1}$ will bring $\mathbf{a}'_1$ to the position of the column without altering the relative positions of the other vectors:

$$\begin{bmatrix}\mathbf{a}'_1 & \cdots & \mathbf{a}'_{j-1} & \mathbf{a}'_{j+1} & \cdots & \mathbf{a}'_{n+1}\end{bmatrix}.$$

This matrix is precisely $\mathbf{A}_{ij}$, and since $\mathbf{A}_{ij}$ obtains from $\mathbf{B}_{i1}$ via $j-2$ column transpositions, by DP2 and the inductive hypothesis we have

$$\det'_n(\mathbf{B}_{i1}) = (-1)^{j-2}\det'_n(\mathbf{A}_{ij}) = (-1)^{j-2}\det'_{n,j}(\mathbf{A}_{ij}).$$

Substituting this result into (5.5) yields

$$\det'_{n+1}(\mathbf{A}) = -\sum_{i=1}^{n+1}(-1)^{i+1}(-1)^{j-2}a_{ij}\det'_{n,j}(\mathbf{A}_{ij}) = \sum_{i=1}^{n+1}(-1)^{i+j}a_{ij}\det'_{n,j}(\mathbf{A}_{ij}) = \det'_{n+1,j}(\mathbf{A})$$

as desired. Therefore $\det'_{n+1,j} = \det'_{n+1}$ for all $1 \le j \le n+1$. ■

**Lemma 5.9.** *For all $n \in \mathbb{N}$ and $1 \leq i \leq n$, define* $\det_{n,i} : \mathbb{F}^{n\times n} \to \mathbb{F}$ *by*

$$\det_{n,i}(\mathbf{A}) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det_{n-1,i}(\mathbf{A}_{ij}),$$

*with* $\det_{1,1}([a]) = a$ *in particular. Then, for every $n \in \mathbb{N}$,* $\det_{n,i}(\mathbf{A}) = \det_n(\mathbf{A})$ *for all $1 \leq i \leq n$ and $\mathbf{A} \in \mathbb{F}^{n\times n}$.*

**Proof.** The conclusion is trivially true in the case when $n = 1$, so suppose the conclusion is true for some $n \in \mathbb{N}$. Since $\det_{n+1,1} = \det_{n+1}$ by definition, consider $\det_{n+1,i}$ for some $i \geq 2$. Let $\mathbf{A} \in \mathbb{F}^{(n+1)\times(n+1)}$. We have

$$\det_{n+1}(\mathbf{A}) = \det_{n+1}(\mathbf{A}^\top) = \det'_{n+1}(\mathbf{A}^\top) = \det'_{n+1,i}(\mathbf{A}^\top) \tag{5.6}$$

by Theorem 5.7, Lemma 5.6, and Lemma 5.8, respectively. Letting $\mathbf{A}^\top = \mathbf{B} = [b_{jk}]_n$, where $b_{jk} = a_{kj}$, we have

$$\det'_{n+1,i}(\mathbf{A}^\top) = \det'_{n+1,i}(\mathbf{B}) = \sum_{j=1}^{n+1} (-1)^{j+i} b_{ji} \det'_{n,i}(\mathbf{B}_{ji}). \tag{5.7}$$

However, since $\mathbf{B}_{ji} = (\mathbf{A}^\top)_{ji} = (\mathbf{A}_{ij})^\top$, it follows that

$$\det'_{n,i}(\mathbf{B}_{ji}) = \det'_{n,i}\left((\mathbf{A}_{ij})^\top\right) = \det'_{n}\left((\mathbf{A}_{ij})^\top\right) = \det_{n}\left((\mathbf{A}_{ij})^\top\right) = \det_n(\mathbf{A}_{ij}) = \det_{n,i}(\mathbf{A}_{ij}),$$

making use of Lemma 5.8, Lemma 5.6, Theorem 5.7, and the inductive hypothesis, in turn. This result, along with $b_{ji} = a_{ij}$ and (5.6), turns (5.7) into

$$\det_{n+1}(\mathbf{A}) = \sum_{j=1}^{n+1} (-1)^{i+j} a_{ij} \det_{n,i}(\mathbf{A}_{ij}),$$

and therefore $\det_{n+1}(\mathbf{A}) = \det_{n+1,i}(\mathbf{A})$ as desired. ■

All of the functions $\det_{n,i}$ and $\det'_{n,j}$ are rightly called determinant functions; however Lemmas 5.6, 5.8 and 5.9, taken together, show that

$$\det_{n,i} = \det_n = \det'_n = \det'_{n,j}$$

for any $n \in \mathbb{N}$ and $1 \leq i, j \leq n$. That is, all of the determinant functions defined thus far in this section turn out to be the same function, even though they are given by different formulas! For each $i$, the formula given for $\det_{n,i}(\mathbf{A})$ is called "expansion of the determinant of $\mathbf{A}$ along the $i$th row"; and for each $j$, the formula given for $\det'_{n,j}(\mathbf{A})$ is called "expansion of the determinant of $\mathbf{A}$ along the $j$th column." Since all of the functions $\det_{n,i}$ and $\det'_{n,j}$ are the same, and since in practice it is not generally necessary or desirable to specify which way the determinant of a square matrix is being expanded, from now on we shall denote all expansions of the determinant of $\mathbf{A}$ by the symbol $\det_n(\mathbf{A})$ or $\det(\mathbf{A})$. We summarize as follows.

**Definition 5.10.** *Given* $\mathbf{A} \in \mathbb{F}^{n\times n}$*, the sum*

$$\det_n(\mathbf{A}) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det_{n-1}(\mathbf{A}_{ij})$$

*is called the* ***expansion of the determinant of*** $\mathbf{A}$ ***along the ith row****, and the sum*

$$\det_n(\mathbf{A}) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det_{n-1}(\mathbf{A}_{ij})$$

*is called the* ***expansion of the determinant of*** $\mathbf{A}$ ***along the jth column****.*

Given column vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$, we define

$$\det_n(\mathbf{a}_1^\top, \ldots, \mathbf{a}_n^\top) = \det_n\left(\begin{bmatrix} \mathbf{a}_1^\top \\ \vdots \\ \mathbf{a}_n^\top \end{bmatrix}\right);$$

that is, we take $\det_n(\mathbf{a}_1^\top, \ldots, \mathbf{a}_n^\top)$ to be the determinant of the matrix with *row vectors* $\mathbf{a}_1^\top, \ldots, \mathbf{a}_n^\top$. (It is important to bear in mind that, notational conventions aside, $\det_n$ is by definition strictly a function with domain $\mathbb{F}^{n\times n}$—which is to say the allowed "inputs" are $n \times n$ matrices, and not $n$-tuples of vectors in $\mathbb{F}^n$.) In light of Theorem 5.7 we readily obtain the following result.

**Proposition 5.11.** *The properties DP1 – DP6 given in Theorem 5.4 remain valid if* $\mathbf{a}_1, \ldots, \mathbf{a}_n$ *represent the row vectors of a matrix* $\mathbf{A} \in \mathbb{F}^{n\times n}$ *instead of the column vectors.*

**Proof.** The proof for DP1 should suffice to convey the general strategy. Given row vectors $\mathbf{a}_1, \ldots, \mathbf{u}+\mathbf{v}, \ldots, \mathbf{a}_n$, we have

$$\begin{aligned}
\det_n(\mathbf{a}_1, \ldots, \mathbf{u}+\mathbf{v}, \ldots, \mathbf{a}_n) &= \det_n\left(\begin{bmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{u}+\mathbf{v} \\ \vdots \\ \mathbf{a}_n \end{bmatrix}\right) = \det_n\left(\begin{bmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{u}+\mathbf{v} \\ \vdots \\ \mathbf{a}_n \end{bmatrix}^\top\right) \\
&= \det_n\left(\begin{bmatrix} \mathbf{a}_1^\top & \cdots & \mathbf{u}^\top + \mathbf{v}^\top & \cdots & \mathbf{a}_n^\top \end{bmatrix}\right) \\
&= \det_n\left(\begin{bmatrix} \mathbf{a}_1^\top & \cdots & \mathbf{u}^\top & \cdots & \mathbf{a}_n^\top \end{bmatrix}\right) + \det_n\left(\begin{bmatrix} \mathbf{a}_1^\top & \cdots & \mathbf{v}^\top & \cdots & \mathbf{a}_n^\top \end{bmatrix}\right) \\
&= \det_n\left(\begin{bmatrix} \mathbf{a}_1^\top & \cdots & \mathbf{u}^\top & \cdots & \mathbf{a}_n^\top \end{bmatrix}^\top\right) + \det_n\left(\begin{bmatrix} \mathbf{a}_1^\top & \cdots & \mathbf{v}^\top & \cdots & \mathbf{a}_n^\top \end{bmatrix}^\top\right) \\
&= \det_n\left(\begin{bmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{u} \\ \vdots \\ \mathbf{a}_n \end{bmatrix}\right) + \det_n\left(\begin{bmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{v} \\ \vdots \\ \mathbf{a}_n \end{bmatrix}\right) \\
&= \det_n(\mathbf{a}_1, \ldots, \mathbf{u}, \ldots, \mathbf{a}_n) + \det_n(\mathbf{a}_1, \ldots, \mathbf{v}, \ldots, \mathbf{a}_n)
\end{aligned}$$

by our notational convention and repeated use of Theorem 5.7. ■

**Example 5.12.** Evaluate the determinant

$$\begin{vmatrix} 3 & 0 & -6 \\ -2 & 4 & 7 \\ 1 & 0 & 10 \end{vmatrix}$$

**Solution.** Since the second column of the determinant has two zero entries, our labors will be lessened if we expand the determinant along the second column:

$$\begin{aligned} \begin{vmatrix} 3 & 0 & -6 \\ -2 & 4 & 7 \\ 1 & 0 & 10 \end{vmatrix} &= (-1)^{1+2}(0)\begin{vmatrix} -2 & 7 \\ 1 & 10 \end{vmatrix} + (-1)^{2+2}(4)\begin{vmatrix} 3 & -6 \\ 1 & 10 \end{vmatrix} + (-1)^{3+2}(0)\begin{vmatrix} 3 & -6 \\ -2 & 7 \end{vmatrix} \\ &= 4\begin{vmatrix} 3 & -6 \\ 1 & 10 \end{vmatrix} = 4\big[(3)(10) - (-6)(1)\big] = 144. \end{aligned}$$

Expanding along any other column or row will yield the same result. ■

**Example 5.13.** Given that

$$\mathbf{A} = \begin{bmatrix} 3 & 1 & -5 & 9 \\ -6 & 4 & 10 & -18 \\ 0 & -2 & 8 & -7 \\ 5 & 1 & -1 & 3 \end{bmatrix},$$

evaluate $\det(\mathbf{A})$.

**Solution.** Applying DP5 together with Proposition 5.11, we add twice the first row of the determinant to the second row, obtaining a new determinant having the same value as the old one:

$$\det(\mathbf{A}) = \begin{vmatrix} 3 & 1 & -5 & 9 \\ -6 & 4 & 10 & -18 \\ 0 & -2 & 8 & -7 \\ 5 & 1 & -1 & 3 \end{vmatrix} \xlongequal{2r_1+r_2\to r_2} \begin{vmatrix} 3 & 1 & -5 & 9 \\ 0 & 6 & 0 & 0 \\ 0 & -2 & 8 & -7 \\ 5 & 1 & -1 & 3 \end{vmatrix}$$

Now we find it convenient to expand the determinant of $\mathbf{A}$ along the second row, since that row contains three zero entries:

$$\det(\mathbf{A}) = (-1)^{2+2}(6) = \begin{vmatrix} 3 & -5 & 9 \\ 0 & 8 & -7 \\ 5 & -1 & 3 \end{vmatrix} = 6\begin{vmatrix} 3 & -5 & 9 \\ 0 & 8 & -7 \\ 5 & -1 & 3 \end{vmatrix}$$

Expanding the $3 \times 3$ determinant along the first column, we finally obtain

$$\begin{aligned} \det(\mathbf{A}) &= 6\left(3\begin{vmatrix} 8 & -7 \\ -1 & 3 \end{vmatrix} + 5\begin{vmatrix} -5 & 9 \\ 8 & -7 \end{vmatrix}\right) \\ &= 6\big[3(17) + 5(-37)\big] = -804 \end{aligned}$$

and we're done. ■

**Example 5.14.** The $n \times n$ **Vandermonde determinant** is

$$V_n = \det\left([x_i^{j-1}]_{n\times n}\right) = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{vmatrix}$$

The claim is that

$$V_{n+1} = \prod_{1\le i<j\le n+1} (x_j - x_i) \tag{5.8}$$

for all $n \geq 1$. This clearly holds when $n = 1$ and $n = 2$:

$$V_2 = \begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix} = x_2 - x_1 \quad \text{and} \quad V_3 = \begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^3 \end{vmatrix} = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2).$$

Let $n \geq 1$ be arbitrary, and suppose that (5.8) is true. Now, by DP5,

$$V_{n+2} = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{n+1} \\ 1 & x_2 & \cdots & x_2^{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n+2} & \cdots & x_{n+2}^{n+1} \end{vmatrix} \xlongequal[\text{for } j=n+1,\ldots,1]{-x_1c_j+c_{j+1}\to c_{j+1}} \begin{vmatrix} 1 & 0 & \cdots & 0 \\ 1 & x_2 - x_1 & \cdots & x_2^{n+1} - x_1x_2^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n+2} - x_1 & \cdots & x_{n+2}^{n+1} - x_1x_{n+2}^n \end{vmatrix}.$$

Expanding the determinant along the first row and then employing Proposition 5.11 to DP1 yields

$$V_{n+2} = \begin{vmatrix} x_2 - x_1 & x_2^2 - x_1x_2 & \cdots & x_2^{n+1} - x_1x_2^n \\ \vdots & \vdots & \ddots & \vdots \\ x_{n+2} - x_1 & x_{n+2}^2 - x_1x_{n+2} & \cdots & x_{n+2}^{n+1} - x_1x_{n+2}^n \end{vmatrix}$$

$$= (x_2 - x_1)\cdots(x_{n+2} - x_1) \begin{vmatrix} 1 & x_2 & \cdots & x_2^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n+2} & \cdots & x_{n+2}^n \end{vmatrix}$$

The last determinant is an $(n+1)\times(n+1)$ Vandermonde determinant, and so by (5.8) we have

$$\begin{vmatrix} 1 & x_2 & \cdots & x_2^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n+2} & \cdots & x_{n+2}^n \end{vmatrix} = \prod_{2\le i<j\le n+2} (x_j - x_i).$$

Hence

$$V_{n+2} = (x_2 - x_1)\cdots(x_{n+2} - x_1) \prod_{2\le i<j\le n+2} (x_j - x_i) = \prod_{1\le i<j\le n+2} (x_j - x_i),$$

and so by the principle of induction we conclude that (5.8) holds for all $n \geq 1$. ■

## 5.3 – Applications of Determinants

As a first application, we establish a few results that will enable us to significantly extend the Invertible Matrix Proposition of §4.9.

**Proposition 5.15.** *Let* $\mathbf{A} = [\mathbf{a}_1 \ \cdots \ \mathbf{a}_n] \in \mathbb{F}^{n\times n}$. *The vectors* $\mathbf{a}_1, \dots, \mathbf{a}_n$ *are linearly dependent if and only if* $\det(\mathbf{A}) = 0$.

**Proof.** Suppose that $\mathbf{a}_1, \dots, \mathbf{a}_n$ are linearly dependent, so there exist $c_1, \dots, c_n \in \mathbb{F}$ such that

$$\sum_{j=1}^{n} c_j \mathbf{a}_j = \mathbf{0},$$

and $c_k \neq 0$ for some $1 \leq k \leq n$. Now

$$c_k \mathbf{a}_k + \sum_{j\neq k} c_j \mathbf{a}_j = \mathbf{0} \quad \Rightarrow \quad \mathbf{a}_k = -\sum_{j\neq k} \frac{c_j}{c_k} \mathbf{a}_j,$$

and so

$$\begin{aligned} \det(\mathbf{A}) = \det(\mathbf{a}_1, \dots, \mathbf{a}_k, \dots, \mathbf{a}_n) &= \det\left(\mathbf{a}_1, \dots, -\sum_{j\neq k} \frac{c_j}{c_k} \mathbf{a}_j, \dots, \mathbf{a}_n\right) \\ &= -\sum_{j\neq k} \frac{c_j}{c_k} \det(\mathbf{a}_1, \dots, \mathbf{a}_j, \dots, \mathbf{a}_n) \end{aligned} \tag{5.9}$$

by the multilinearity properties of the determinant function. By DP4 we have

$$\det(\mathbf{a}_1, \dots, \underbrace{\mathbf{a}_j}_{k\text{th col.}}, \dots, \mathbf{a}_n) = 0$$

for each $1 \leq j \leq n$ such that $j \neq k$, and so from (5.9) we obtain $\det(\mathbf{A}) = 0$.

For the converse, suppose that $\mathbf{a}_1, \dots, \mathbf{a}_n$ are linearly independent, so col-rank$(\mathbf{A}) = n$. Recall the elementary row and column operations R1, R2, C1, and C2 from Definition 2.15. The proof of Theorem 3.64 shows that $\mathbf{A}$ is equivalent via the operations R1, R2, C1, and C2 to a diagonal matrix

$$\mathbf{B} = \begin{bmatrix} b_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & b_{nn} \end{bmatrix},$$

and since by Theorem 3.66

$$\text{col-rank}(\mathbf{B}) = \text{col-rank}(\mathbf{A}) = n,$$

it follows that $b_{jj} \neq 0$ for all $1 \leq j \leq n$.

Now, if $p$ is the number of R2 and C2 operations performed (which by Propositions 2.16(2) and 2.17(2) correspond to swapping rows and columns) in passing from $\mathbf{A}$ to $\mathbf{B}$, then by DP2 and 5.4(5), together with Proposition 5.11, we have

$$\det(\mathbf{A}) = (-1)^p \det(\mathbf{B}).$$

Of course, $\mathbf{B}$ is an upper-triangular matrix, and so

$$\det(\mathbf{A}) = (-1)^p b_{11}b_{22}\cdots b_{nn} \neq 0$$

by Proposition 5.5. ■

**Proposition 5.16.** *$\mathbf{A} \in \mathbb{F}^{n\times n}$ is invertible if and only if $\det_n(\mathbf{A}) \neq 0$.*

**Proof.** By the Invertible Matrix Proposition (Proposition 4.66),

$$\mathbf{A} = \begin{bmatrix} \mathbf{a}_1 & \cdots & \mathbf{a}_n \end{bmatrix}$$

is invertible if and only if $\mathbf{a}_1, \dots, \mathbf{a}_n$ are linearly independent, and by Proposition 5.15 the vectors $\mathbf{a}_1, \dots, \mathbf{a}_n$ are linearly independent if and only if $\det_n(\mathbf{A}) \neq 0$. The conclusion is now self-evident. ■

We now improve on the Invertible Matrix Proposition given in §4.9 to obtain what we shall call the Invertible Matrix Theorem, incorporating also the results of Proposition 4.67 as well as observing that $\text{nullity}(\mathbf{A}) = 0$ is equivalent to $\text{Nul}(\mathbf{A}) = \{\mathbf{0}\}$.

**Theorem 5.17 (Invertible Matrix Theorem).** *Let $\mathbf{A} \in \mathbb{F}^{n\times n}$, and let $L_{\mathbf{A}}$ be the linear operator on $\mathbb{F}^n$ having corresponding matrix $\mathbf{A}$ with respect to the standard basis $\mathcal{E}$ of $\mathbb{F}^n$. Then the following statements are equivalent.*

1. *$\mathbf{A}$ is invertible.*
2. *$\mathbf{A}^\top$ is invertible.*
3. *$\mathbf{A}$ is row-equivalent to $\mathbf{I}_n$.*
4. *The row vectors of $\mathbf{A}$ are linearly independent.*
5. *$\mathbf{A}$ is column-equivalent to $\mathbf{I}_n$.*
6. *The column vectors of $\mathbf{A}$ are linearly independent.*
7. $\text{col-rank}(\mathbf{A}) = n$.
8. $\text{row-rank}(\mathbf{A}) = n$.
9. $\text{rank}(\mathbf{A}) = n$.
10. *The system $\mathbf{Ax} = \mathbf{b}$ has a unique solution for each $\mathbf{b} \in \mathbb{F}^n$.*
11. *The system $\mathbf{Ax} = \mathbf{0}$ has only the trivial solution.*
12. $\text{Nul}(\mathbf{A}) = \{\mathbf{0}\}$.
13. $\text{nullity}(\mathbf{A}) = 0$.
14. *$L_{\mathbf{A}} \in \mathcal{L}(\mathbb{F}^n)$ is invertible.*
15. *There exists some $\mathbf{D} \in \mathbb{F}^{n\times n}$ such that $\mathbf{AD} = \mathbf{I}_n$.*
16. *There exists some $\mathbf{C} \in \mathbb{F}^{n\times n}$ such that $\mathbf{CA} = \mathbf{I}_n$.*
17. $\det_n(\mathbf{A}) \neq 0$.

Determinants can be applied to find the solution to a nonhomogeneous system of $n$ equations with $n$ unknowns, provided that a unique solution exists.

**Theorem 5.18 (Cramer's Rule).** *Let $\mathbf{a}_1, \dots, \mathbf{a}_n \in \mathbb{F}^n$ such that $\det_n(\mathbf{a}_1, \dots, \mathbf{a}_n) \neq 0$. If $\mathbf{b} \in \mathbb{F}^n$ and $x_1, \dots, x_n$ are scalars such that*

$$x_1\mathbf{a}_1 + \cdots + x_n\mathbf{a}_n = \mathbf{b}, \tag{5.10}$$

*then*

$$x_j = \frac{\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_{j-1}, \mathbf{b}, \mathbf{a}_{j+1}, \ldots, \mathbf{a}_n)}{\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_n)}$$

*for each* $1 \leq j \leq n$.

**Proof.** Suppose that $\mathbf{b} \in \mathbb{F}^n$. Since $\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_n) \neq 0$ it follows from the Invertible Matrix Theorem that there exist unique scalars $x_1, \ldots, x_n$ such that equation (5.10) holds. Fix $1 \leq j \leq n$. Letting

$$\det_n(\mathbf{a}_1, \ldots, \mathbf{b}, \ldots, \mathbf{a}_n) = \det_n(\mathbf{a}_1, \ldots, \mathbf{a}_{j-1}, \mathbf{b}, \mathbf{a}_{j+1}, \ldots, \mathbf{a}_n)$$

for brevity, we obtain

$$\begin{aligned} \det_n(\mathbf{a}_1, \ldots, \mathbf{b}, \ldots, \mathbf{a}_n) &= \det_n\left(\mathbf{a}_1, \ldots, \sum_{k=1}^n x_k \mathbf{a}_k, \ldots, \mathbf{a}_n\right) \\ &= \sum_{k=1}^n x_k \det_n(\mathbf{a}_1, \ldots, \mathbf{a}_k, \ldots, \mathbf{a}_n) \end{aligned} \tag{5.11}$$

by DP1. Now, for each $k \neq j$ we have $\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_k, \ldots, \mathbf{a}_n) = 0$ by DP4, since both the $j$th and $k$th column of the matrix

$$\begin{bmatrix} \mathbf{a}_1 & \cdots & \underbrace{\mathbf{a}_k}_{j\text{th col.}} & \cdots & \mathbf{a}_n \end{bmatrix}$$

is equal to $\mathbf{a}_j$. Hence from (5.11) comes

$$\det_n(\mathbf{a}_1, \ldots, \mathbf{b}, \ldots, \mathbf{a}_n) = x_j \det_n(\mathbf{a}_1, \ldots, \underbrace{\mathbf{a}_j}_{j\text{th col.}}, \ldots, \mathbf{a}_n) = x_j \det_n(\mathbf{a}_1, \ldots, \mathbf{a}_n),$$

and therefore

$$x_j = \frac{\det_n(\mathbf{a}_1, \ldots, \mathbf{b}, \ldots, \mathbf{a}_n)}{\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_n)}$$

as desired. ■

If we let

$$\mathbf{A} = \begin{bmatrix} \mathbf{a}_1 & \mathbf{a}_2 & \cdots & \mathbf{a}_n \end{bmatrix}$$

and

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix},$$

then Cramer's Rule may be given as

$$\mathbf{A}\mathbf{x} = \mathbf{b} \quad \Rightarrow \quad x_j = \frac{\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_{j-1}, \mathbf{b}, \mathbf{a}_{j+1}, \ldots, \mathbf{a}_n)}{\det_n(\mathbf{A})}$$

for each $1 \leq j \leq n$, so long as $\det(\mathbf{A}) \neq 0$.

**Example 5.19.** Solve the system

$$\begin{cases} 2x - \phantom{3}y + \phantom{2}z = 1 \\ \phantom{2}x + 3y - 2z = 0 \\ 4x - 3y + \phantom{2}z = 2 \end{cases}$$

using Cramer's Rule.

**Solution.** Here $\mathbf{A}\mathbf{x} = \mathbf{b}$ with

$$\mathbf{A} = \begin{bmatrix} 2 & -1 & 1 \\ 1 & 3 & -2 \\ 4 & -3 & 1 \end{bmatrix}, \quad \mathbf{x} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad \mathbf{b} = \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}.$$

We have

$$\det(\mathbf{A}) = 2\begin{vmatrix} 3 & -2 \\ -3 & 1 \end{vmatrix} - \begin{vmatrix} -1 & 1 \\ -3 & 1 \end{vmatrix} + 4\begin{vmatrix} -1 & 1 \\ 3 & -2 \end{vmatrix} = 2(-3) - 2 + 4(-1) = -12,$$

so $\det(\mathbf{A}) \neq 0$ and by Cramer's Rule

$$x = \frac{1}{\det(\mathbf{A})}\begin{vmatrix} 1 & -1 & 1 \\ 0 & 3 & -2 \\ 2 & -3 & 1 \end{vmatrix} = -\frac{1}{12}(-5) = \frac{5}{12}$$

$$y = \frac{1}{\det(\mathbf{A})}\begin{vmatrix} 2 & 1 & 1 \\ 1 & 0 & -2 \\ 4 & 2 & 1 \end{vmatrix} = -\frac{1}{12}(1) = -\frac{1}{12}$$

$$z = \frac{1}{\det(\mathbf{A})}\begin{vmatrix} 2 & -1 & 1 \\ 1 & 3 & 0 \\ 4 & -3 & 2 \end{vmatrix} = -\frac{1}{12}(-1) = \frac{1}{12}$$

Therefore the solution to the system, which is unique, is $(5/12, -1/12, 1/12)$. ■

Next, we construct a method for finding the inverse of a square matrix using determinants, provided the matrix is invertible.

**Theorem 5.20.** *Let* $\mathbf{A} = [a_{ij}]_n$*. If* $\det_n(\mathbf{A}) \neq 0$*, then* $\mathbf{X} = [x_{ij}]_n$ *given by*

$$x_{ij} = \frac{(-1)^{i+j}\det_{n-1}(\mathbf{A}_{ji})}{\det_n(\mathbf{A})}$$

*for all* $1 \leq i, j \leq n$ *is the inverse for* $\mathbf{A}$*.*

**Proof.** Suppose that $\det_n(\mathbf{A}) \neq 0$. For any $j \in \{1, \dots, n\}$, let

$$\mathbf{x}_j = \begin{bmatrix} x_{1j} \\ \vdots \\ x_{nj} \end{bmatrix},$$

and recall the $j$th standard unit vector $\mathbf{e}_j$ of $\mathbb{F}^n$. By Cramer's Rule the system of equations corresponding to the matrix equation

$$\mathbf{A}\mathbf{x}_j = \mathbf{e}_j$$

has a unique solution given by

$$x_{ij} = \frac{\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_{i-1}, \mathbf{e}_j, \mathbf{a}_{i+1}, \ldots, \mathbf{a}_n)}{\det_n(\mathbf{A})}$$

for each $1 \leq i \leq n$. Since the $j$th coordinate of $\mathbf{e}_j$ is 1 and all other coordinates are 0, we obtain

$$\det_n(\mathbf{a}_1, \ldots, \mathbf{a}_{i-1}, \mathbf{e}_j, \mathbf{a}_{i+1}, \ldots, \mathbf{a}_n) = (-1)^{i+j} \det_{n-1}(\mathbf{A}_{ji})$$

by expanding the determinant along the $i$th column. Therefore

$$x_{ij} = \frac{(-1)^{i+j} \det_{n-1}(\mathbf{A}_{ji})}{\det_n(\mathbf{A})}$$

for each $1 \leq i \leq n$ and $1 \leq j \leq n$, and if we define $\mathbf{X} = [x_{ij}]_n$, then we readily obtain

$$\mathbf{AX} = \mathbf{I}_n. \tag{5.12}$$

It remains to show that $\mathbf{XA} = \mathbf{I}_n$. Since $\det_n(\mathbf{A}^\top) = \det_n(\mathbf{A}) \neq 0$, we can find a matrix $\mathbf{Y}$ such that $\mathbf{A}^\top\mathbf{Y} = \mathbf{I}_n$, and then

$$\mathbf{A}^\top\mathbf{Y} = \mathbf{I}_n \;\;\Rightarrow\;\; (\mathbf{A}^\top\mathbf{Y})^\top = \mathbf{I}_n^\top \;\;\Rightarrow\;\; \mathbf{Y}^\top\mathbf{A} = \mathbf{I}_n. \tag{5.13}$$

Now, using (5.12) we obtain

$$\mathbf{Y}^\top\mathbf{A} = \mathbf{I}_n \;\;\Rightarrow\;\; (\mathbf{Y}^\top\mathbf{A})\mathbf{X} = \mathbf{I}_n\mathbf{X} \;\;\Rightarrow\;\; \mathbf{Y}^\top(\mathbf{AX}) = \mathbf{X} \;\;\Rightarrow\;\; \mathbf{Y}^\top\mathbf{I}_n = \mathbf{X} \;\;\Rightarrow\;\; \mathbf{X} = \mathbf{Y}^\top,$$

and hence

$$\mathbf{XA} = \mathbf{I}_n$$

by the rightmost equation in (5.13).

Since $\mathbf{XA} = \mathbf{AX} = \mathbf{I}_n$, we conclude that

$$\mathbf{X} = \left[\frac{(-1)^{i+j} \det_{n-1}(\mathbf{A}_{ji})}{\det_n(\mathbf{A})}\right]_n$$

is the inverse for $\mathbf{A}$. ■

Put another way, Theorem 5.20 states that if $\det_n(\mathbf{A}) \neq 0$ then $\mathbf{A}$ is invertible, and the inverse $\mathbf{A}^{-1}$ is given by

$$\mathbf{A}^{-1} = \left[\frac{(-1)^{i+j} \det_{n-1}(\mathbf{A}_{ji})}{\det_n(\mathbf{A})}\right]_n. \tag{5.14}$$

**Example 5.21.** Show that if $\mathbf{D} \in \mathbb{F}^{n\times n}$ is given as a block matrix by

$$\mathbf{D} = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{O} & \mathbf{C} \end{bmatrix},$$

where $\mathbf{A} = [a_{ij}]_\ell$ and $\mathbf{C} = [c_{ij}]_m$ are square matrices, then

$$\det_n(\mathbf{D}) = \det_\ell(\mathbf{A}) \det_m(\mathbf{C}).$$

**Solution.** We must show that, for all $\ell, m \in \mathbb{N}$,

$$\det_{\ell+m}(\mathbf{D}) = \det_{\ell+m}\left(\begin{bmatrix} [a_{ij}]_\ell & \mathbf{B} \\ \mathbf{O} & [c_{ij}]_m \end{bmatrix}\right) = \det_\ell([a_{ij}]_\ell)\det_m([c_{ij}]_m), \tag{5.15}$$

where of course $\mathbf{O} = [0]_{m\times\ell}$ and $\mathbf{B} = [b_{ij}]_{\ell\times m}$.

First consider the case when $\ell = 1$ and $m \in \mathbb{N}$ is arbitrary. Letting $\mathbf{D} = [d_{ij}]_{m+1}$ denote the block matrix and expanding along the first column, we have

$$\det_{m+1}\left(\begin{bmatrix} a & \mathbf{B} \\ \mathbf{O} & [c_{ij}]_m \end{bmatrix}\right) = \sum_{i=1}^{m+1}(-1)^{i+1}d_{i1}\det_m(\mathbf{D}_{i1}).$$

Since $\mathbf{D}_{11} = [c_{ij}]_m$, $d_{11} = a$ and $d_{i1} = 0$ for $i > 1$, let $a_{11} = a$ to obtain

$$\begin{aligned}\det_{m+1}\left(\begin{bmatrix} a & \mathbf{B} \\ \mathbf{O} & [c_{ij}]_m \end{bmatrix}\right) &= (-1)^{1+1}d_{11}\det_m(\mathbf{D}_{11}) = a\det_m([c_{ij}]_m) \\ &= \det_1([a_{ij}]_1)\det_m([c_{ij}]_m).\end{aligned}$$

This establishes the base case of an inductive argument on $\ell$.

Next, fix $\ell \in \mathbb{N}$, and assume that (5.15) is true for $\ell$ and all $m \in \mathbb{N}$. We must show that (5.15) is true for $\ell + 1$ and all $m$. Let $m \in \mathbb{N}$ be arbitrary, and define

$$\mathbf{D} = [d_{ij}]_{\ell+m+1} = \begin{bmatrix} [a_{ij}]_{\ell+1} & \mathbf{B} \\ \mathbf{O} & [c_{ij}]_m \end{bmatrix}.$$

Letting $\mathbf{B}_i$ denote $\mathbf{B}$ with $i$th row deleted, and also setting $\mathbf{A} = [a_{ij}]_{\ell+1}$, we have

$$\begin{aligned}\det_{\ell+m+1}(\mathbf{D}) = \det_{\ell+m+1}\left(\begin{bmatrix} [a_{ij}]_{\ell+1} & \mathbf{B} \\ \mathbf{O} & [c_{ij}]_m \end{bmatrix}\right) &= \sum_{i=1}^{\ell+m+1}(-1)^{i+1}d_{i1}\det_{\ell+m}(\mathbf{D}_{i1}) \\ = \sum_{i=1}^{\ell+1}(-1)^{i+1}a_{i1}\det_{\ell+m}(\mathbf{D}_{i1}).\end{aligned}$$

Since $\mathbf{A}_{i1}$ is an $\ell \times \ell$ matrix for each $1 \le i \le \ell + 1$, by the inductive hypothesis we find that

$$\det_{\ell+m}(\mathbf{D}_{i1}) = \det_{\ell+m}\left(\begin{bmatrix} \mathbf{A}_{i1} & \mathbf{B}_i \\ \mathbf{O} & \mathbf{C} \end{bmatrix}\right) = \det_\ell(\mathbf{A}_{i1})\det_m(\mathbf{C})$$

for each $1 \le i \le \ell + 1$, and hence

$$\det_{\ell+m+1}(\mathbf{D}) = \sum_{i=1}^{\ell+1}(-1)^{i+1}a_{i1}\det_\ell(\mathbf{A}_{i1})\det_m(\mathbf{C}) = \det_{\ell+1}(\mathbf{A})\det_m(\mathbf{C}).$$

By induction we conclude that (5.15) holds for $\ell, m \in \mathbb{N}$, and therefore

$$\det\left(\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{O} & \mathbf{C} \end{bmatrix}\right) = \det(\mathbf{A})\det(\mathbf{C})$$

for any square matrices $\mathbf{A}$ and $\mathbf{C}$. ■

For the next example we define a **minor** of a matrix $\mathbf{A} \in \mathbb{F}^{m\times n}$ to be the determinant of any square submatrix of $\mathbf{A}$. We have encountered minors already: each $\mathbf{A}_{ij}$ that appears in Definition 5.10 is an $(n-1)\times(n-1)$ minor of the $n \times n$ matrix $\mathbf{A}$.

**Example 5.22.** For $\mathbf{A} \in \mathbb{F}^{m \times n}$ let $1 \leq k < \min\{m, n\}$. Show that $\text{rank}(\mathbf{A}) \leq k$ if and only if every $(k+1) \times (k+1)$ minor of $\mathbf{A}$ equals 0.

**Solution.** By Proposition 4.69, $\text{rank}(\mathbf{A}) \leq k$ if and only if every $(k+1) \times (k+1)$ submatrix of $\mathbf{A}$ is noninvertible. By the Invertible Matrix Theorem a $(k+1) \times (k+1)$ submatrix of $\mathbf{A}$ is noninvertible if and only if the determinant of the submatrix equals 0. Therefore $\text{rank}(\mathbf{A}) \leq k$ if and only if every $(k+1) \times (k+1)$ minor of $\mathbf{A}$ equals 0. ■

## Problems

1. Solve the system

$$\begin{cases} x + y + 2z = 1 \\ 2x + 4z = 2 \\ 3y + z = 3 \end{cases}$$

using Cramer's Rule.

## 5.4 – Determinant Formulas

Recall the elementary matrices $\mathbf{M}_{i,j}(c)$ and $\mathbf{M}_{i,j}$ defined in section 2.3. Given a scalar $x$ and an $n \times n$ matrix $\mathbf{A}$ with row vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$, by Proposition 2.16 we have

$$\mathbf{M}_{i,j}(x)\mathbf{A} = \begin{bmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_j + x\mathbf{a}_i \\ \vdots \\ \mathbf{a}_n \end{bmatrix} \}j\text{th row},$$

and so by Proposition 5.11 (recalling DP5 in Theorem 5.4) we find that

$$\det_n(\mathbf{M}_{i,j}(x)\mathbf{A}) = \det_n\left(\begin{bmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_j + x\mathbf{a}_i \\ \vdots \\ \mathbf{a}_n \end{bmatrix}\right) = \det_n\left(\begin{bmatrix} \mathbf{a}_1 \\ \vdots \\ \mathbf{a}_j \\ \vdots \\ \mathbf{a}_n \end{bmatrix}\right) = \det_n(\mathbf{A}). \tag{5.16}$$

By Proposition 2.16 the matrix $\mathbf{M}_{i,j}\mathbf{A}$ is obtained from $\mathbf{A}$ by interchanging the $i$th and $j$th rows, and so by Proposition 5.11 (recalling DP2 in Theorem 5.4) we find that

$$\det_n(\mathbf{M}_{i,j}\mathbf{A}) = -\det_n(\mathbf{A}). \tag{5.17}$$

We use these facts to prove the following.

**Theorem 5.23.** *For any* $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{n\times n}$,

$$\det_n(\mathbf{AB}) = \det_n(\mathbf{A})\det_n(\mathbf{B}).$$

**Proof.** If $\mathbf{A}$ is not invertible, then $\mathbf{AB}$ is not invertible by Proposition 4.68 and we obtain

$$\det_n(\mathbf{A})\det_n(\mathbf{B}) = 0 \cdot \det_n(\mathbf{B}) = 0 = \det_n(\mathbf{AB})$$

by the Invertible Matrix Theorem. If $\mathbf{B}$ is not invertible we obtain a similar result since $\det_n(\mathbf{AB}) = 0$ and $\det_n(\mathbf{B}) = 0$.

Suppose that $\mathbf{A}$ and $\mathbf{B}$ are both invertible, so that $\mathbf{AB}$ is also invertible by Theorem 2.26. By the proof of Theorem 2.30 the matrix $\mathbf{A}$ is row-equivalent via R1 and R2 operations to a diagonal matrix

$$\mathbf{D} = \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix} = \begin{bmatrix} d_1\mathbf{e}_1 \\ \vdots \\ d_n\mathbf{e}_n \end{bmatrix}$$

that is, there exists a sequence of elementary matrices $\mathbf{M}_1, \ldots, \mathbf{M}_k$, of which $\ell$ are of the R2 variety and the rest of the R1 variety, such that

$$\mathbf{A} = \mathbf{M}_k \cdots \mathbf{M}_1\mathbf{D}.$$

Now, if $\mathbf{b}_1, \ldots, \mathbf{b}_n$ are the row vectors of $\mathbf{B}$, then

$$\mathbf{DB} = \begin{bmatrix} d_1\mathbf{b}_1 \\ \vdots \\ d_n\mathbf{b}_n \end{bmatrix}$$

and so, recalling (5.16) and (5.17) as well as Theorem 5.7,

$$\begin{aligned}
\det_n(\mathbf{AB}) &= \det_n\big((\mathbf{M}_k \cdots \mathbf{M}_1\mathbf{D})\mathbf{B}\big) = \det_n\big(\mathbf{M}_k \cdots \mathbf{M}_1(\mathbf{DB})\big) = (-1)^\ell \det_n(\mathbf{DB}) \\
&= (-1)^\ell \det_n\big((\mathbf{DB})^\top\big) = (-1)^\ell \det_n\big(d_1\mathbf{b}_1^\top, \ldots, d_n\mathbf{b}_n^\top\big) \\
&= (-1)^\ell d_1 \cdots d_n \det_n\big(\mathbf{b}_1^\top, \ldots, \mathbf{b}_n^\top\big) = (-1)^\ell d_1 \cdots d_n \det_n\big(\mathbf{B}^\top\big) \\
&= (-1)^\ell d_1 \cdots d_n \det_n(\mathbf{B}) = (-1)^\ell \det_n(\mathbf{D}) \det_n(\mathbf{B}) \\
&= \det_n(\mathbf{M}_k \cdots \mathbf{M}_1\mathbf{D}) \det_n(\mathbf{B}) = \det_n(\mathbf{A}) \det_n(\mathbf{B}).
\end{aligned}$$

Here we use the fact that $\mathbf{D}$ is an upper-triangular matrix and so by Proposition 5.5 has determinant equal to the product of its diagonal entries. ■

**Theorem 5.24.** *If* $\mathbf{A} \in \mathbb{F}^{n\times n}$ *is invertible, then*

$$\det_n(\mathbf{A}^{-1}) = \frac{1}{\det_n(\mathbf{A})}.$$

**Proof.** Suppose that $\mathbf{A} \in \mathbb{F}^{n\times n}$ is invertible. Then there exists some $\mathbf{A}^{-1} \in \mathbb{F}^{n\times n}$ such that $\mathbf{AA}^{-1} = \mathbf{I}_n$, and thus

$$\det_n(\mathbf{A}) \det_n(\mathbf{A}^{-1}) = \det_n(\mathbf{AA}^{-1}) = \det_n(\mathbf{I}_n) = 1. \tag{5.18}$$

by Theorems 5.23 and 5.4(7) . Now, the invertibility of $\mathbf{A}$ implies that $\det_n(\mathbf{A}) \neq 0$ by the Invertible Matrix Theorem, and so from (5.18) we readily obtain

$$\det_n(\mathbf{A}^{-1}) = \frac{1}{\det_n(\mathbf{A})}.$$

as desired. ■

Another way to write the statement of Theorem 5.24 that is particularly elegant is:

$$\det_n(\mathbf{A}^{-1}) = \det_n(\mathbf{A})^{-1}$$

if $\mathbf{A} \in \mathbb{F}^{n\times n}$ is invertible.

Recall Corollary 4.33: given a linear operator $L : V \to V$, bases $\mathcal{B}$ and $\mathcal{B}'$ for $V$, and corresponding matrices $[L]_\mathcal{B}$ and $[L]_{\mathcal{B}'}$, we have

$$[L]_{\mathcal{B}'} = \mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_\mathcal{B}\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}, \tag{5.19}$$

From this matrix equation we obtain an interesting result involving determinants.

**Theorem 5.25.** *Let* $\dim(V) = n$*, let* $L$ *be a linear operator on* $V$*, and let* $\mathcal{B}$ *and* $\mathcal{B}'$ *be bases for* $V$*. If* $[L]_{\mathcal{B}}$ *is the matrix corresponding to* $L$ *with respect to* $\mathcal{B}$ *and* $[L]_{\mathcal{B}'}$ *is the matrix corresponding to* $L$ *with respect to* $\mathcal{B}'$*, then*

$$\det_n([L]_{\mathcal{B}'}) = \det_n([L]_{\mathcal{B}}). \tag{5.20}$$

**Proof.** From equation (5.19) we obtain

$$\det_n([L]_{\mathcal{B}'}) = \det_n(\mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}}\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}).$$

Now, by Theorems 5.23 and 5.24,

$$\begin{aligned}\det_n([L]_{\mathcal{B}'}) &= \det_n(\mathbf{I}_{\mathcal{B}\mathcal{B}'})\det_n([L]_{\mathcal{B}})\det_n(\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}) \\ &= \det_n(\mathbf{I}_{\mathcal{B}\mathcal{B}'})\det_n([L]_{\mathcal{B}})\frac{1}{\det_n(\mathbf{I}_{\mathcal{B}\mathcal{B}'})} \\ &= \det_n([L]_{\mathcal{B}}),\end{aligned}$$

which affirms (5.20) and finishes the proof. ■

Thus the determinant of the matrix corresponding to a linear operator on $V$ is invariant in value under change of bases, so that we can meaningfully speak of the “determinant” of a linear operator.

**Definition 5.26.** *Let* $\dim(V) = n$*, and let* $L$ *be a linear operator on* $V$*. The* ***determinant of*** $L$ *is defined to be*

$$\det_n(L) = \det_n([L]),$$

*where* $[L]$ *is the matrix corresponding to* $L$ *with respect to any basis for* $V$*.*

## 5.5 – Permutations and the Symmetric Group

**Definition 5.27.** *Let $n \in \mathbb{N}$, and let $I_n = \{1, 2, \dots, n\}$. The* ***symmetric group*** *$\mathcal{S}_n$ is the group consisting of all bijections*

$$\sigma : I_n \to I_n$$

*under the operation of function composition $\circ$. Each $\sigma \in \mathcal{S}_n$ is called a* ***permutation****.*

By definition every group must have an identity element. We denote by $\varepsilon$ the **identity** permutation in $\mathcal{S}_n$ that is given by $\varepsilon(k) = k$ for each $k \in I_n$.

A special matrix notation, known as the **two-line notation**, is often used to define a permutation $\sigma \in \mathcal{S}_n$ explicitly. We write

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$$

to indicate that $\sigma$ maps 1 to the value $\sigma(1)$, 2 to the value $\sigma(2)$, and so on. Thus the first row of the matrix lists the "inputs" for the function $\sigma$, and the second row lists the corresponding "outputs."

Since $\sigma \in \mathcal{S}_n$ is a bijection, it has an inverse which we denote (as usual) by $\sigma^{-1}$, and it is easy to see that $\sigma^{-1} \in \mathcal{S}_n$ also. We also define $\sigma^0 = \varepsilon$, $\sigma^1 = \sigma$, $\sigma^2 = \sigma \circ \sigma$, and so on.

**Example 5.28.** One permutation belonging to the group $\mathcal{S}_5$ is $\sigma : I_5 \to I_5$ given by

$$\sigma(1) = 4, \quad \sigma(2) = 2, \quad \sigma(3) = 1, \quad \sigma(4) = 5, \quad \sigma(5) = 3,$$

which we denote by

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{bmatrix}$$

in the two-line notation. ■

**Example 5.29.** Just as there are 6 possible permutations (i.e. ordered arrangements) of a set of 3 distinct objects $\{a, b, c\}$, namely

$$(a, b, c), \quad (a, c, b), \quad (b, a, c), \quad (b, c, a), \quad (c, a, b), \quad (c, b, a),$$

so too are there six permutations in the group $\mathcal{S}_3$. These are

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

The first permutation in the list is the identity permutation $\varepsilon$. ■

If $\sigma, \tau \in \mathcal{S}_n$, then $\tau \circ \sigma \in \mathcal{S}_n$ is given by

$$(\tau \circ \sigma)(i) = \tau(\sigma(i))$$

for each $i \in I_n$ in the usual manner of function composition. Thus

$$\tau \circ \sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & \cdots & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \cdots & \tau(\sigma(n)) \end{bmatrix}.$$

**Example 5.30.** In $\mathcal{S}_3$ we have

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \tag{5.21}$$

Note that the matrix immediately to the *right* of the symbol $\circ$ in (5.21) takes the input *first*, so

$$1 \to \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \to 3 \to \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \to 2,$$

which gives the first column of the matrix to the right of the = symbol in (5.21). ∎

Assuming $n \geq 2$, a **transposition** is a permutation $\tau \in \mathcal{S}_n$ for which there exist $k, \ell \in I_n$ with $k \neq \ell$ such that

$$\tau(i) = \begin{cases} i, & \text{if } i \in I_n \setminus \{k, \ell\} \\ k, & \text{if } i = \ell \\ \ell, & \text{if } i = k. \end{cases}$$

Thus a transposition interchanges precisely two distinct elements of $I_n$ while leaving all other elements fixed. The classic example in $\mathcal{S}_2$ is

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix},$$

and an example in $\mathcal{S}_4$ is

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix}.$$

Any permutation $\sigma \in \mathcal{S}_n$ is uniquely determined by the arrangement of the elements of $I_n$ in the second row of its corresponding matrix. Since the $n$ elements in $I_n$ have $n!$ possible distinct arrangements, it follows that $\mathcal{S}_n$ itself has $n!$ elements. This proves the following.

**Proposition 5.31.** $|\mathcal{S}_n| = n!$ *for all* $n \in \mathbb{N}$.

We now introduce another notation for elements of $\mathcal{S}_n$ called **cycle notation**. For $m \leq n$ let $J = \{j_1, j_2, j_3, \dots, j_m\}$ be a set of distinct elements of $I_n$. Then the symbol

$$(j_1, j_2, j_3, \dots, j_m), \tag{5.22}$$

denotes a permutation in $\mathcal{S}_n$ that performs the mappings

$$j_1 \mapsto j_2 \mapsto j_3 \mapsto \cdots \mapsto j_{m-1} \mapsto j_m \mapsto j_1,$$

and also $i \mapsto i$ for any $i \in I_n \setminus J$. Using function notation, if $\sigma \in \mathcal{S}_n$ is such that

$$\sigma = (j_1, j_2, j_3, \dots, j_m),$$

then

$$\sigma(j_1) = j_2, \quad \sigma(j_2) = j_3, \quad \dots, \quad \sigma(j_{m-1}) = j_m, \quad \sigma(j_m) = j_1,$$

with $\sigma(i) = i$ for any $i \in I_n \setminus J$.

Any permutation expressible in the form (5.22) is called a **cycle**. The entries in (5.22) are ideally envisioned as being written in a circular arrangement, like the numbers on a clock, so that the "last" entry $j_m$ is naturally seen to be followed by $j_1$. In this way

$$(j_m, j_1, j_2, \dots, j_{m-1})$$

is easily recognized as being the same permutation as that given by (5.22).

**Example 5.32.** In $\mathcal{S}_3$ the cycle $(1,3,2)$ is the permutation

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

In $\mathcal{S}_5$ the cycle $(1,3,2)$ is the permutation

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}.$$

Since $(1,3,2) \in \mathcal{S}_5$ does not feature 4 or 5 among its entries, we see that $(1,3,2)$ maps $4 \mapsto 4$ and $5 \mapsto 5$.

In $\mathcal{S}_n$ for any $n \geq 3$ we have

$$(1,3,2) = (2,1,3) = (3,2,1).$$

That is, moving the last entry in a cycle to the first position does not change the corresponding permutation. ■

As with permutations in general, two cycles $\sigma$ and $\tau$ in $\mathcal{S}_n$ may be composed. If

$$\sigma = (j_1, j_2, \dots, j_m) \quad \text{and} \quad \tau = (i_1, i_2, \dots, i_\ell), \tag{5.23}$$

then

$$(j_1, j_2, \dots, j_m) \circ (i_1, i_2, \dots, i_\ell)$$

is the permutation $\sigma \circ \tau$. Typically the symbol $\circ$ is omitted in the cycle notation, and we write

$$\sigma \circ \tau = (j_1, j_2, \dots, j_m)(i_1, i_2, \dots, i_\ell).$$

The **length** of a cycle is simply the number of entries it contains. For instance the cycles $\sigma$ and $\tau$ in (5.23) have lengths $m$ and $\ell$, respectively. We will say a cycle is an ***m*-cycle** if it has length $m$. We now gather a few facts about transpositions.

**Proposition 5.33.** *Let $n \geq 2$.*

1. *$\mathcal{S}_1$ has no transpositions.*
2. *$\tau \in \mathcal{S}_n$ is a transposition if and only if $\tau$ is a 2-cycle.*
3. *If $\tau \in \mathcal{S}_n$ is a transposition, then $\tau \circ \tau = \varepsilon$.*
4. *If $\tau_1, \tau_2 \in \mathcal{S}_n$ are transpositions, then $\tau_1 \circ \tau_2 = \tau_2 \circ \tau_1$.*

**Proof.**
*Proof of (3).* Suppose $\tau \in \mathcal{S}_n$ is a transposition, so $\tau = (a, b)$ for some $a, b \in I_n$ with $a \neq b$ by part (2). Then

$$(\tau \circ \tau)(a) = \tau(\tau(a)) = \tau(b) = a \quad \text{and} \quad (\tau \circ \tau)(b) = \tau(\tau(b)) = \tau(a) = b,$$

and furthermore

$$(\tau \circ \tau)(i) = \tau(\tau(i)) = \tau(i) = i$$

for any $i \in I_n \setminus \{a, b\}$. Therefore $\tau \circ \tau = \varepsilon$. ■

Proofs of the other parts of Proposition 5.33 are left as exercises.

Two cycles $(j_1, \ldots, j_m)$ and $(i_1, \ldots, i_\ell)$ in $\mathcal{S}_n$ are **disjoint** if

$$\{j_1, \ldots, j_m\} \cap \{i_1, \ldots, i_\ell\} = \varnothing,$$

which is to say the cycles have no entries in common. Thus $(1, 6, 3)$ and $(4, 2, 5, 8)$ are disjoint since $\{1, 6, 3\} \cap \{4, 2, 5, 8\} = \varnothing$, but $(5, 2, 1)$ and $(3, 1, 9, 2)$ are not disjoint since $\{5, 2, 1\} \cap \{3, 1, 9, 2\} = \{1, 2\}$.

**Proposition 5.34.** *If $(j_1, \ldots, j_m)$ and $(i_1, \ldots, i_\ell)$ are disjoint cycles in $\mathcal{S}_n$, then*

$$(j_1, \ldots, j_m)(i_1, \ldots, i_\ell) = (i_1, \ldots, i_\ell)(j_1, \ldots, j_m).$$

The proof of Proposition 5.34 is left as an exercise. Another way to state Proposition 5.34 is to say that disjoint cycles commute. Parts (2) and (4) of Proposition 5.33 imply that commutativity always holds in the special case of 2-cycles, even if the 2-cycles under consideration are not disjoint.

The process of expressing a permutation as a composition of two or more cycles is known as **cycle decomposition**. Even a permutation that is itself a cycle we may be interested in expressing anew as a composition of two cycles of lesser length. Indeed, of particular importance to us along our path to a new formulation for determinants in the next section is the process of decomposing a permutation into 2-cycles (i.e. transpositions).

**Example 5.35.** Consider the permutation

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 1 & 2 & 5 & 7 & 4 \end{bmatrix}$$

in $\mathcal{S}_7$. We see that $\sigma$ maps 1 to 3, and also 3 back to 1. We may write this as $1 \mapsto 3 \mapsto 1$. We also have the chain of mappings

$$2 \mapsto 6 \mapsto 7 \mapsto 4 \mapsto 2.$$

The only mapping left is $5 \mapsto 5$. Thus $\sigma$ has the cycle decomposition

$$(1, 3)(2, 6, 7, 4),$$

or equivalently $(2, 6, 7, 4)(1, 3)$. Recall that if a value is absent from a cycle's list of entries, then the cycle returns that value unchanged. Thus

$$5 \to (1, 3) \to 5 \to (2, 6, 7, 4) \to 5,$$

whereas

$$1 \to (1,3) \to 3 \to (2,6,7,4) \to 3.$$

To decompose $\sigma$ into transpositions it is only necessary to decompose $(2,6,7,4)$ into transpositions. In fact we have

$$(2,6,7,4) = (2,6)(2,7)(2,4),$$

where the three transpositions on the right-hand side may be written in any order, and so

$$\sigma = (1,3)(2,6,7,4) = (1,3)(2,6)(2,7)(2,4),$$

where again any order is permissible. ■

It was not mere luck that the permutation $\sigma$ in Example 5.35 was able to be decomposed into transpositions. As the next proposition makes clear, this is true of any permutation in $\mathcal{S}_n$ for $n \geq 2$.

**Proposition 5.36.** *Let $n \geq 2$. If $\sigma \in \mathcal{S}_n$, then for some $k \in \mathbb{N}$ there exist transpositions $\tau_1, \dots, \tau_k \in \mathcal{S}_n$ such that*

$$\sigma = \tau_1 \circ \cdots \circ \tau_k.$$

**Proof.** The proof will employ induction, so we start by showing the $n = 2$ case is true. The symmetric group $\mathcal{S}_2$ has only two elements: $\varepsilon$ and $(1,2)$. Since $(1,2)$ is already a transposition, we need only show that

$$\varepsilon = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$$

can be expressed as a composition of transpositions. But by Proposition 5.33(3) we immediately have $\varepsilon = (1,2)(1,2)$, and so we're done.

Now let $n \geq 2$ be arbitrary, and suppose the statement of the proposition holds for this value $n$. Let $\sigma \in \mathcal{S}_{n+1}$, so that

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n+1 \\ i_1 & i_2 & \cdots & i_{n+1} \end{bmatrix}.$$

Since $\sigma : I_{n+1} \to I_{n+1}$ is a bijection there exists some $m \in I_{n+1}$ such that $\sigma(m) = n+1$. There are two cases to consider: either $m = n+1$ or $m < n+1$.

If $m = n+1$, so that $\sigma(n+1) = n+1$, then $\sigma(i) \in I_n$ for each $i \in I_n$. If we define $\hat{\sigma} : I_n \to I_n$ by $\hat{\sigma}(i) = \sigma(i)$ for each $i \in I_n$, then $\hat{\sigma} \in \mathcal{S}_n$, and by our inductive hypothesis there exist transpositions $\tau_1, \dots, \tau_k \in \mathcal{S}_n$ such that $\hat{\sigma} = \tau_1 \circ \cdots \circ \tau_k$. By Proposition 5.33(2) each transposition $\tau_j$ is a 2-cycle $(a_j, b_j)$, and since $a_j, b_j \in I_n$ and $I_n \subseteq I_{n+1}$, it follows that $(a_j, b_j)$ also defines a 2-cycle in $\mathcal{S}_{n+1}$. Taking $\tau_j = (a_j, b_j)$ to be in $\mathcal{S}_{n+1}$ for each $1 \leq j \leq k$, we find that $\sigma = \tau_1 \circ \cdots \circ \tau_k$, and so $\sigma$ is expressible as a composition of transpositions.

Suppose next that $m < n+1$, so $\sigma(m) = n+1$ for $m \in I_n$. Defining $\sigma_0 \in \mathcal{S}_{n+1}$ by $\sigma_0 = \sigma \circ (m, n+1)$, Proposition 5.33(3) and the known associativity of the function composition operation imply that

$$\begin{aligned} \sigma = \sigma \circ \varepsilon &= \sigma \circ ((m, n+1) \circ (m, n+1)) \\ &= (\sigma \circ (m, n+1)) \circ (m, n+1) = \sigma_0 \circ (m, n+1). \end{aligned} \tag{5.24}$$

Now, since

$$\sigma_0(n+1) = (\sigma \circ (m, n+1))(n+1) = \sigma(m) = n+1,$$

we see that $\sigma_0$ has the property treated in the $m = n+1$ case, and so by the same argument used in that case there exist transpositions $\tau_1, \ldots, \tau_k \in \mathcal{S}_{n+1}$ such that $\sigma_0 = \tau_1 \circ \cdots \circ \tau_k$. Then by (5.24) we find that

$$\sigma = \tau_1 \circ \cdots \circ \tau_k \circ (m, n+1),$$

which shows that $\sigma$ is again expressible as a composition of transpositions. ■

What Proposition 5.36 does not say is that the cycle decomposition of a permutation into transpositions is necessarily unique, and that's because it never is. Even for $(1,2) \in \mathcal{S}_2$ we have

$$(1,2) = (1,2)(1,2)(1,2) = (1,2)(1,2)(1,2)(1,2)(1,2),$$

and in general $(1,2) = (1,2)^{2k-1}$ for any $k \in \mathbb{N}$.

Is there anything more that can be said about the decomposition of a permutation into transpositions, beyond its mere existence? Recall that any integer has a parity, which is to say the integer is either even (divisible by 2) or odd (not divisible by 2). Now we define the **parity** of a particular decomposition of $\sigma \in \mathcal{S}_n$ into transpositions $\tau_1, \ldots, \tau_k$ as being **odd** if $k$ is odd, and **even** if $k$ is even. The next proposition states that no one permutation can have two decompositions of opposite parity.

**Proposition 5.37.** *Let $n \geq 2$. If $\sigma \in \mathcal{S}_n$, then the decompositions of $\sigma$ into transpositions are either all odd or all even.*

**Proof.** The proof will employ induction, so we start by showing the $n = 2$ case is true. The symmetric group $\mathcal{S}_2$ has only two elements, $\varepsilon$ and $(1,2)$, with $(1,2)$ in particular being the only transposition available. Now, for any $k \geq 0$ Proposition 5.33(3) implies that

$$(1,2)^{2k} = [(1,2)(1,2)]^k = \varepsilon^k = \varepsilon,$$

and

$$(1,2)^{2k+1} = (1,2)(1,2)^{2k} = (1,2) \circ \varepsilon = (1,2).$$

Thus all the possible even decompositions equal $\varepsilon$, and all the possible odd decompositions equal $(1,2)$. It follows that $\varepsilon$ has only even decompositions, and $(1,2)$ has only odd decompositions.

Now let $n \geq 2$ be arbitrary, and suppose the statement of the proposition holds for this value $n$. The remainder of the proof we leave as an exercise. ■

It is because of Proposition 5.37 that the following definition is meaningful.

**Definition 5.38.** *Let $n \geq 2$. A permutation $\sigma \in \mathcal{S}_n$ is* ***even*** *if it can be expressed as a composition of an even number of transpositions, and* ***odd*** *if it can be expressed as a composition of an odd number of transpositions. By definition $\varepsilon \in \mathcal{S}_1$ we take to be even.*

*The* ***sign*** *function on $\mathcal{S}_n$ is the function $\operatorname{sgn} : \mathcal{S}_n \to \{-1, 1\}$ given by*

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ is even} \\ -1, & \text{if } \sigma \text{ is odd.} \end{cases}$$

The only element of $\mathcal{S}_1$ is

$$\varepsilon = \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

which cannot be expressed as a composition of transpositions since there are no transpositions in $\mathcal{S}_1$. Nonetheless it will be convenient to *define* $\varepsilon \in \mathcal{S}_1$ to be even, and therefore $\text{sgn}(\varepsilon) = 1$.

**Remark.** Since $(-1)^m$ is 1 if $m$ is even and $-1$ if $m$ is odd, we see from Definition 5.38 that if a permutation $\sigma$ can be expressed as a composition of $m$ transpositions, then $\text{sgn}(\sigma) = (-1)^m$.

It is straightforward to check that the composition of two even permutations is again even, and so if $\mathcal{A}_n$ is the set of all even permutations in $\mathcal{S}_n$, then $\mathcal{A}_n$ is in fact a subgroup of $\mathcal{S}_n$ called the **antisymmetric group**. In contrast the composition of two odd permutations is even, and so the set $\mathcal{S}_n \setminus \mathcal{A}_n$ of all odd permutations in $\mathcal{S}_n$ is not a group since it is not closed under the operation $\circ$ of function composition.

## 5.6 – The Leibniz Formula

In §5.2 we found that, for each $n \in \mathbb{N}$, the functions $\det_{n,i}$ and $\det'_{n,j}$ were equal for all $1 \le i, j \le n$; that is,

$$\det_{n,1} = \cdots = \det_{n,n} = \det'_{n,1} = \cdots = \det'_{n,n}.$$

That all these functions are the same ultimately derives from the fact that they all possess the six properties given in Theorem 5.4. A close look at these properties, however, reveals that not all of them are fundamental. That is, some of the properties are an immediate consequence of one or more of the others. In particular, analyzing the details of the theorem's proof, it can be seen that properties DP1, DP2, and DP3 are independent (i.e. no two can be used to derive the third), and yet taken together they readily imply DP4, DP5, and DP6.

While all the "different" determinants defined in §5.2 turned out to be the same, it is reasonable to wonder whether there is some way to define the determinant of a square matrix $\mathbf{A}$ so that it possesses the properties in Theorem 5.4 and yet is genuinely different. Put another way, if the minimum qualifications that a function must satisfy in order for it to be called a "determinant" are that it possess the multilinearity, alternating, and normalization properties in Theorem 5.4, does that *uniquely* characterize the function? The answer is yes.

**Theorem 5.39** (**Uniqueness of the Determinant**). *For $n \in \mathbb{N}$ suppose $D : \mathbb{F}^{n\times n} \to \mathbb{F}$ has the following properties:*

DP1. ***Multilinearity.*** *For any $1 \le j \le n$ and $x \in \mathbb{F}$,*

$$D(\ldots, \mathbf{a}_j, \ldots) + D(\ldots, \mathbf{b}_j, \ldots) = D(\ldots, \mathbf{a}_j + \mathbf{b}_j, \ldots),$$

*and*

$$D(\ldots, x\mathbf{a}_j, \ldots) = xD(\ldots, \mathbf{a}_j, \ldots).$$

DP2. ***Alternating.*** *For any $1 \le j < k \le n$,*

$$D(\ldots, \mathbf{a}_j, \ldots, \mathbf{a}_k, \ldots) = -D(\ldots, \underbrace{\mathbf{a}_k}_{j}, \ldots, \underbrace{\mathbf{a}_j}_{k}, \ldots).$$

DP3. ***Normalization.***

$$D(\mathbf{I}_n) = 1.$$

*Then $D = \det_n$.*

**Proof.** Applying DP2 in the case when $\mathbf{a}_j = \mathbf{a}_k = \mathbf{u}$ gives

$$D(\ldots, \mathbf{u}, \ldots, \mathbf{u}, \ldots) = -D(\ldots, \mathbf{u}, \ldots, \mathbf{u}, \ldots),$$

and hence

$$D(\ldots, \mathbf{u}, \ldots, \mathbf{u}, \ldots) = 0.$$

That is, $D(\mathbf{A}) = 0$ whenever $\mathbf{A} \in \mathbb{F}^{n\times n}$ has two identical columns.

Let $\mathbf{A} = [\mathbf{a}_1 \ \cdots \ \mathbf{a}_n] \in \mathbb{F}^{n\times n}$ be arbitrary. By DP1,

$$D(\mathbf{A}) = D(\mathbf{a}_1, \ldots, \mathbf{a}_n) = D\left(\sum_{i_1=1}^{n} a_{i_1 1}\mathbf{e}_{i_1}, \ldots, \sum_{i_n=1}^{n} a_{i_n n}\mathbf{e}_{i_n}\right)$$

$$= \sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} D\big(a_{i_1 1}\mathbf{e}_{i_1}, \ldots, a_{i_n n}\mathbf{e}_{i_n}\big)$$

$$= \sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} a_{i_1 1} \cdots a_{i_n n} D(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_n}). \tag{5.25}$$

It remains to evaluate $D(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_n})$ in (5.25). In fact we have $D(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_n}) = 0$ whenever $i_k = i_\ell$ for some $k \neq \ell$, since the matrix $[\mathbf{e}_{i_1} \ \cdots \ \mathbf{e}_{i_n}]$ then has two identical columns, and it follows that only those terms in the sum (5.25) for which the list of values $i_1, \ldots, i_n$ represents a permutation $\sigma \in \mathcal{S}_n$ are all that's left. In particular, for each such term we take $\sigma$ to be given by $\sigma(k) = i_k$ for $1 \leq k \leq n$, and since there is a one-to-one correspondence between the remaining terms in (5.25) and the elements of $\mathcal{S}_n$, we obtain

$$D(\mathbf{A}) = \sum_{\sigma \in \mathcal{S}_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n} D(\mathbf{e}_{\sigma(1)}, \ldots, \mathbf{e}_{\sigma(n)}). \tag{5.26}$$

Now, for any $\sigma \in \mathcal{S}_n$ there exist, by Proposition 5.36, transpositions $\tau_1, \ldots, \tau_m$ such that $\sigma = \tau_m \circ \cdots \circ \tau_1$. By DP2,

$$\begin{aligned} D(\mathbf{e}_1, \ldots, \mathbf{e}_n) &= -D(\mathbf{e}_{\tau_1(1)}, \ldots, \mathbf{e}_{\tau_1(n)}) = (-1)^2 D\big(\mathbf{e}_{\tau_2(\tau_1(1))}, \ldots, \mathbf{e}_{\tau_2(\tau_1(n))}\big) \\ &= (-1)^3 D\big(\mathbf{e}_{\tau_3(\tau_2(\tau_1(1)))}, \ldots, \mathbf{e}_{\tau_3(\tau_2(\tau_1(n)))}\big) \\ &\ \ \vdots \\ &= (-1)^m D\big(\mathbf{e}_{(\tau_m \circ \cdots \circ \tau_1)(1)}, \ldots, \mathbf{e}_{(\tau_m \circ \cdots \circ \tau_1)(n)}\big) \\ &= \operatorname{sgn}(\sigma) D(\mathbf{e}_{\sigma(1)}, \ldots, \mathbf{e}_{\sigma(n)}), \end{aligned}$$

and so by DP3, noting that $1/\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma)$,

$$D(\mathbf{e}_{\sigma(1)}, \ldots, \mathbf{e}_{\sigma(n)}) = \operatorname{sgn}(\sigma) D(\mathbf{e}_1, \ldots, \mathbf{e}_n) = \operatorname{sgn}(\sigma) D(\mathbf{I}_n) = \operatorname{sgn}(\sigma).$$

Putting this result into (5.26) gives

$$D(\mathbf{A}) = \sum_{\sigma \in \mathcal{S}_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n} \operatorname{sgn}(\sigma). \tag{5.27}$$

The expression at right in (5.27) is entirely independent of $D$. Indeed, if we assume $\hat{D}$ is another function on $\mathbb{F}^{n \times n}$ that satisfies the properties DP1, DP2, and DP3, then an identical argument will lead to $\hat{D}(\mathbf{A})$ equalling the same expression, and hence $\hat{D}(\mathbf{A}) = D(\mathbf{A})$. Since $\det_n$ has the properties DP1, DP2, and DP3, we conclude that $\det_n(\mathbf{A}) = D(\mathbf{A})$. ■

The proof of Theorem 5.39 immediately gives the following result, which is a formula for the determinant function that is explicit rather than recursive.

**Theorem 5.40 (Leibniz Formula).** *For any $n \in \mathbb{N}$ and $\mathbf{A} \in \mathbb{F}^{n \times n}$,*

$$\det_n(\mathbf{A}) = \sum_{\sigma \in \mathcal{S}_n} \operatorname{sgn}(\sigma) a_{\sigma(1),1} a_{\sigma(2),2} \cdots a_{\sigma(n),n}.$$

**Proposition 5.41.** *Let $n \geq 2$. For any $1 \leq k < \ell \leq n$,*

$$\sum_{\sigma \in \mathcal{S}_n} \operatorname{sgn}(\sigma)\left(a_{\sigma(k),k} a_{\sigma(\ell),k} \prod_{i \in I_n \setminus \{k,\ell\}} a_{\sigma(i),i}\right) = 0. \tag{5.28}$$

**Proof.** Fix $1 \leq k < \ell \leq n$, and let $\Sigma_\sigma$ denote the sum in (5.28). Then

$$\Sigma_\sigma = \sum_{\pi \in \mathcal{A}_n}\left(a_{\pi(k),k} a_{\pi(\ell),k} \prod_{i \in I_n \setminus \{k,\ell\}} a_{\pi(i),i}\right) - \sum_{\nu \in \mathcal{S}_n \setminus \mathcal{A}_n}\left(a_{\nu(k),k} a_{\nu(\ell),k} \prod_{i \in I_n \setminus \{k,\ell\}} a_{\nu(i),i}\right). \tag{5.29}$$

Fix $\pi_0 \in \mathcal{A}_n$. Then $\nu_0 = \pi_0 \circ (k, \ell) \in \mathcal{S}_n \setminus \mathcal{A}_n$ is given by

$$\nu_0(i) = \begin{cases} \pi_0(i), & \text{if } i \in I_n \setminus \{k, n\} \\ \pi_0(\ell), & \text{if } i = k \\ \pi_0(k), & \text{if } i = \ell, \end{cases}$$

so that

$$a_{\nu_0(\ell),k} a_{\nu_0(k),k} \prod_{i \in I_n \setminus \{k,\ell\}} a_{\nu_0(i),i} = a_{\pi_0(k),k} a_{\pi_0(\ell),k} \prod_{i \in I_n \setminus \{k,\ell\}} a_{\pi_0(i),i}.$$

This shows that the term in the sum $\sum_{\pi \in \mathcal{A}_n}$ that corresponds to $\pi_0$ is canceled by the term in $\sum_{\nu \in \mathcal{S}_n \setminus \mathcal{A}_n}$ that corresponds to $\nu_0$ at right in (5.29). In a similar way, for any $\nu_1 \in \mathcal{S}_n \setminus \mathcal{A}_n$ we have $\pi_1 = \nu_1 \circ (k, \ell) \in \mathcal{A}_n$, and the terms in $\sum_{\pi \in \mathcal{A}_n}$ and $\sum_{\nu \in \mathcal{S}_n \setminus \mathcal{A}_n}$ corresponding to $\pi_1$ and $\nu_1$ will cancel in (5.29). Therefore the sum $\sum_\sigma$ must equal zero. ■

# 6

# Eigen Theory

## 6.1 – Eigenvectors and Eigenvalues

Throughout this chapter we assume that all vector spaces are finite-dimensional with dimension at least 1 unless otherwise specified.

**Definition 6.1.** *Let $V$ be a vector space over $\mathbb{F}$ and $L : V \to V$ a linear operator. An **eigenvector** of $L$ is a nonzero vector $\mathbf{v} \in V$ such that*

$$L(\mathbf{v}) = \lambda\mathbf{v}$$

*for some $\lambda \in \mathbb{F}$. The scalar $\lambda$ is an **eigenvalue** of $L$, and $\mathbf{v}$ is said to be an eigenvector corresponding to $\lambda$. The set*

$$E_L(\lambda) = \{\mathbf{v} \in V : L(\mathbf{v}) = \lambda\mathbf{v}\}$$

*is the **eigenspace** of $L$ corresponding to $\lambda$.*

The symbol $\sigma(L)$ will occasionally be used to denote the set of eigenvalues possessed by a linear operator $L$, so that $|\sigma(L)|$ denotes the number of distinct eigenvalues of $L$.

A careful examination of Definition 6.1 should make it clear that, while the zero vector $\mathbf{0} \in V$ cannot be an eigenvector, the zero scalar $0 \in \mathbb{F}$ can be an eigenvalue. Despite not being an eigenvector, however, it is always true that $\mathbf{0}$ is an element of $E_L(\lambda)$ since

$$L(\mathbf{0}) = \mathbf{0} = \lambda\mathbf{0}$$

holds for any linear operator $L$

**Proposition 6.2.** *Let $V$ be a vector space. If $L : V \to V$ is a linear operator with eigenvalue $\lambda$, then $E_L(\lambda)$ is a subspace of $V$.*

**Proof.** Suppose $L : V \to V$ is linear with eigenvalue $\lambda$. It has already been established that $\mathbf{0} \in E_L(\lambda)$. Given $\mathbf{u}, \mathbf{v} \in E_L(\lambda)$ and scalar $c$ we have

$$L(\mathbf{u} + \mathbf{v}) = L(\mathbf{u}) + L(\mathbf{v}) = \lambda\mathbf{u} + \lambda\mathbf{v} = \lambda(\mathbf{u} + \mathbf{v})$$

and

$$L(c\mathbf{v}) = cL(\mathbf{v}) = c(\lambda\mathbf{v}) = \lambda(c\mathbf{v}),$$

which shows that $\mathbf{u} + \mathbf{v} \in E_L(\lambda)$ and $c\mathbf{v} \in E_L(\lambda)$. ■

**Example 6.3.** Let $V$ be a vector space and consider the identity operator $I_V : V \to V$ given by $I_V(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v} \in V$. It is clear that $\lambda = 1$ is the only eigenvalue of $I_V$, and all nonzero vectors in $V$ are corresponding eigenvectors. Indeed,

$$E_{I_V}(1) = \{\mathbf{v} \in V : I_V(\mathbf{v}) = \mathbf{v}\} = V$$

is the corresponding eigenspace. ■

**Example 6.4.** Let $V$ be a vector space and consider the zero operator $O_V : V \to V$ given by $O_V(\mathbf{v}) = \mathbf{0}$ for all $\mathbf{v} \in V$. For any $\mathbf{v} \neq \mathbf{0}$, then, we have

$$O_V(\mathbf{v}) = \mathbf{0} = 0\mathbf{v},$$

which shows that 0 is an eigenvalue of $O_V$. Moreover

$$E_{O_V}(0) = \{\mathbf{v} \in V : O_V(\mathbf{v}) = 0\mathbf{v}\} = V$$

is the corresponding eigenspace. There are no other eigenvalues. ■

In addition to eigenvectors, eigenvalues, and eigenspaces of linear mappings, there are related notions for square matrices.

**Definition 6.5.** *Let $\mathbf{A} \in \mathbb{F}^{n\times n}$. An* ***eigenvector*** *of $\mathbf{A}$ is a nonzero vector $\mathbf{x} \in \mathbb{F}^n$ such that*

$$\mathbf{A}\mathbf{x} = \lambda\mathbf{x}$$

*for some $\lambda \in \mathbb{F}$. The scalar $\lambda$ is an* ***eigenvalue*** *of $\mathbf{A}$, and $\mathbf{x}$ is said to be an eigenvector corresponding to $\lambda$. The set*

$$E_{\mathbf{A}}(\lambda) = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{A}\mathbf{x} = \lambda\mathbf{x}\}$$

*is the* ***eigenspace*** *of $\mathbf{A}$ corresponding to $\lambda$.*

The symbol $\sigma(\mathbf{A})$ will occasionally be used to denote the set of eigenvalues possessed by a square matrix $\mathbf{A}$, so that $|\sigma(\mathbf{A})|$ denotes the number of distinct eigenvalues of $\mathbf{A}$.

**Remark.** A careful reading of Definition 6.5 should make it clear that any eigenvector corresponding to an eigenvalue of $\mathbf{A} \in \mathbb{F}^{n\times n}$ must be an element of $\mathbb{F}^n$. Thus, if we are given that $\mathbf{A} \in \mathbb{R}^{n\times n}$, then we would discount any $\mathbf{z} \in \mathbb{C}^n \setminus \mathbb{R}^n$ for which $\mathbf{A}\mathbf{z} = \lambda\mathbf{z}$ for some $\lambda \in \mathbb{R}$.

**Proposition 6.6.** *If $\lambda$ is an eigenvalue of $\mathbf{A} \in \mathbb{F}^{n\times n}$, then $E_{\mathbf{A}}(\lambda)$ is a subspace of $\mathbb{F}^n$.*

**Proof.** Suppose that $\lambda$ is an eigenvalue of $\mathbf{A}$. By Definitions 6.5 and 3.15,

$$\begin{aligned}\mathbf{x} \in E_{\mathbf{A}}(\lambda) \;&\Leftrightarrow\; \mathbf{A}\mathbf{x} = \lambda\mathbf{x} \;\Leftrightarrow\; \mathbf{A}\mathbf{x} - \lambda\mathbf{x} = \mathbf{0} \;\Leftrightarrow\; \mathbf{A}\mathbf{x} - \lambda\mathbf{I}_n\mathbf{x} = \mathbf{0}\\ &\Leftrightarrow\; (\mathbf{A} - \lambda\mathbf{I}_n)\mathbf{x} = \mathbf{0} \;\Leftrightarrow\; \mathbf{x} \in \mathrm{Nul}(\mathbf{A} - \lambda\mathbf{I}_n).\end{aligned}$$

That is,

$$E_{\mathbf{A}}(\lambda) = \mathrm{Nul}(\mathbf{A} - \lambda\mathbf{I}_n), \tag{6.1}$$

the null space of $\mathbf{A} - \lambda\mathbf{I}_n$. By Proposition 3.16 $\mathrm{Nul}(\mathbf{A} - \lambda\mathbf{I}_n)$ is a subspace of $\mathbb{F}^n$, and hence so too is $E_{\mathbf{A}}(\lambda)$. ■

**Proposition 6.7.** *Let $V$ be a vector space over $\mathbb{F}$, and suppose $L \in \mathcal{L}(V)$ has eigenvalues $\lambda_1, \lambda_2$ with corresponding eigenvectors $\mathbf{v}_1, \mathbf{v}_2$, respectively.*

1. *If $\lambda_1 \neq \lambda_2$, then $\mathbf{v}_1 \neq \mathbf{v}_2$.*
2. *$E_L(\lambda_1) \cap E_L(\lambda_2) = \{\mathbf{0}\}$ if and only if $\lambda_1 \neq \lambda_2$.*

**Proof.**
*Proof of Part (1).* We will prove the contrapositive: "If $\mathbf{v}_1 = \mathbf{v}_2$, then $\lambda_1 = \lambda_2$." Suppose that $\mathbf{v}_1 = \mathbf{v}_2 = \mathbf{v}$, so

$$\lambda_1\mathbf{v} = \lambda_1\mathbf{v}_1 = L(\mathbf{v}_1) = L(\mathbf{v}_2) = \lambda_2\mathbf{v}_2 = \lambda_2\mathbf{v},$$

and then

$$(\lambda_1 - \lambda_2)\mathbf{v} = \lambda_1\mathbf{v} - \lambda_2\mathbf{v} = \mathbf{0}.$$

By Proposition 3.2(3) either $\lambda_1 - \lambda_2 = 0$ or $\mathbf{v} = \mathbf{0}$. But $\mathbf{v} \neq \mathbf{0}$ since an eigenvector is nonzero by definition, and so it must be that $\lambda_1 - \lambda_2$. Therefore $\lambda_1 = \lambda_2$.

*Proof of Part (2).* Suppose $\lambda_1 = \lambda_2 = \lambda$, so that $\lambda$ is an eigenvalue of $L$ with corresponding eigenvectors $\mathbf{v}_1$ and $\mathbf{v}_2$. In particular

$$\mathbf{v}_1 \in E_L(\lambda) = E_L(\lambda_1) = E_L(\lambda_2),$$

and thus

$$\mathbf{v}_1 \in E_L(\lambda_1) \cap E_L(\lambda_2).$$

Since $\mathbf{v}_1 \neq \mathbf{0}$, it follows that $E_L(\lambda_1) \cap E_L(\lambda_2) \neq \{\mathbf{0}\}$.

For the converse, suppose $\lambda_1 \neq \lambda_2$. Let $\mathbf{v} \in E_L(\lambda_1) \cap E_L(\lambda_2)$. Then $L(\mathbf{v}) = \lambda_1\mathbf{v}$ and $L(\mathbf{v}) = \lambda_2\mathbf{v}$, and thus $\lambda_1\mathbf{v} = \lambda_2\mathbf{v}$. Now,

$$\lambda_1\mathbf{v} = \lambda_2\mathbf{v} \;\Rightarrow\; (\lambda_1 - \lambda_2)\mathbf{v} = \mathbf{0},$$

and since $\lambda_1 - \lambda_2 \neq 0$, Proposition 3.2(3) implies that $\mathbf{v} = \mathbf{0}$. Therefore $E_L(\lambda_1) \cap E_L(\lambda_2) = \{\mathbf{0}\}$. ■

The converse of Proposition 6.7(1) is not true in general; that is, if $L \in \mathcal{L}(V)$ has eigenvalues $\lambda_1, \lambda_2$ with corresponding eigenvectors $\mathbf{v}_1, \mathbf{v}_2$, then $\mathbf{v}_1 \neq \mathbf{v}_2$ does not necessarily imply that $\lambda_1 \neq \lambda_2$. Consider for example $\mathbf{v}_2 = 2\mathbf{v}_1$: certainly $\mathbf{v}_1 \neq \mathbf{v}_2$ since we know $\mathbf{v}_1 \neq \mathbf{0}$, but

$$L(\mathbf{v}_2) = L(2\mathbf{v}_1) = 2L(\mathbf{v}_1) = 2(\lambda_1\mathbf{v}_1) = \lambda_1(2\mathbf{v}_1) = \lambda_1\mathbf{v}_2$$

shows that $\lambda_1 = \lambda_2$.

**Theorem 6.8.** *Let $V$ be a vector space over $\mathbb{F}$, and let $L \in \mathcal{L}(V)$ have distinct eigenvalues $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$. If $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are eigenvectors corresponding to $\lambda_1, \ldots, \lambda_n$, respectively, then the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is linearly independent.*

**Proof.** An eigenvector is nonzero by definition, so if $n = 1$ then certainly the set $\{\mathbf{v}_1\}$ is linearly independent. This establishes the base case of an inductive argument.

Suppose the theorem is true when $n = m$, where $m$ is some arbitrary positive integer (this is our "inductive hypothesis"). Let $L$ be a linear operator on $V$ with distinct eigenvalues $\lambda_1, \ldots, \lambda_{m+1}$ and corresponding eigenvectors $\mathbf{v}_1, \ldots, \mathbf{v}_{m+1}$, so that $L(\mathbf{v}_k) = \lambda_k \mathbf{v}_k$ for each $1 \leq k \leq m+1$. Suppose $c_1, \ldots, c_{m+1} \in \mathbb{F}$ are such that

$$\sum_{k=1}^{m+1} c_k \mathbf{v}_k = \mathbf{0}. \tag{6.2}$$

Since the eigenvalues $\lambda_1, \ldots, \lambda_{m+1}$ are distinct, there exists some $1 \leq k_0 \leq m+1$ such that $\lambda_{k_0} \neq 0$. Since the eigenvalues may be indexed in any convenient way, we can assume $k_0 = m+1$ so that $\lambda_{m+1} \neq 0$. Multiplying (6.2) by $\lambda_{m+1}$ gives

$$\sum_{k=1}^{m+1} c_k \lambda_{m+1} \mathbf{v}_k = \mathbf{0}, \tag{6.3}$$

and we also have

$$L\left(\sum_{k=1}^{m+1} c_k \mathbf{v}_k\right) = L(\mathbf{0}) \quad \Rightarrow \quad \sum_{k=1}^{m+1} c_k L(\mathbf{v}_k) = \mathbf{0} \quad \Rightarrow \quad \sum_{k=1}^{m+1} c_k \lambda_k \mathbf{v}_k = \mathbf{0}. \tag{6.4}$$

Subtracting (6.3) from the rightmost equation in (6.4), we obtain

$$\sum_{k=1}^{m+1} c_k \lambda_k \mathbf{v}_k - \sum_{k=1}^{m+1} c_k \lambda_{m+1} \mathbf{v}_k = \mathbf{0},$$

so that

$$\sum_{k=1}^{m+1} c_k (\lambda_k - \lambda_{m+1}) \mathbf{v}_k = \mathbf{0}. \tag{6.5}$$

Of course

$$c_k (\lambda_k - \lambda_{m+1}) \mathbf{v}_k = \mathbf{0}$$

if $k = m+1$, and so (6.5) becomes

$$\sum_{k=1}^{m} c_k (\lambda_k - \lambda_{m+1}) \mathbf{v}_k = \mathbf{0}. \tag{6.6}$$

Now, $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are the eigenvectors corresponding to the distinct eigenvalues $\lambda_1, \ldots, \lambda_m$, and so by our inductive hypothesis the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is linearly independent. From (6.6) it follows that

$$c_k (\lambda_k - \lambda_{m+1}) = 0$$

for $1 \leq k \leq m$, which in turn implies that $c_k = 0$ for $1 \leq k \leq m$ since $\lambda_1, \ldots, \lambda_m$ do not equal $\lambda_{m+1}$. Now (6.2) becomes $c_{m+1}\mathbf{v}_{m+1} = \mathbf{0}$, which immediately yields $c_{m+1} = 0$. Since (6.2) results only in the trivial solution

$$c_1 = \cdots = c_{m+1} = 0$$

we conclude that $\mathbf{v}_1, \ldots, \mathbf{v}_{m+1}$ are linearly independent.

We see now that the theorem holds for $n = m + 1$ when we assume that it holds for $n = m$, and therefore by induction it holds for all $n \in \mathbb{N}$. ■

**Corollary 6.9.** *If $V$ is a finite-dimensional vector space and $L \in \mathcal{L}(V)$, then $L$ has at most $\dim(V)$ distinct eigenvalues.*

**Proof.** Suppose that $V$ is an $n$-dimensional vector space and $L \in \mathcal{L}(V)$. Suppose $\lambda_1, \ldots, \lambda_{n+1}$ are distinct eigenvalues of $L$ with corresponding eigenvectors $\mathbf{v}_1, \ldots, \mathbf{v}_{n+1}$. Then $\{\mathbf{v}_1, \ldots, \mathbf{v}_{n+1}\}$ is a basis for $V$ by Theorem 6.8 and we are led to conclude that the dimension of $V$ is $n + 1$, which is a contradiction. Therefore $L$ has at most $n$ distinct eigenvalues. ■

**Example 6.10.** Let $\mathbf{A} \in \mathbb{F}^{n\times n}$ be the diagonal matrix

$$\mathbf{A} = \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{bmatrix}$$

having distinct diagonal entries $\lambda_1, \ldots, \lambda_n$ (i.e. $\lambda_i \neq \lambda_j$ whenever $i \neq j$). If $\mathbf{e}_1, \ldots, \mathbf{e}_n$ are the standard basis vectors for $\mathbb{F}^n$, so that

$$\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \quad \ldots, \quad \mathbf{e}_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix},$$

then for each $1 \leq k \leq n$ we find that $\mathbf{A}\mathbf{e}_k = \lambda_k \mathbf{e}_k$, and so $\lambda_k$ is an eigenvalue of $\mathbf{A}$.

If $L$ is the linear operator on $\mathbb{F}^n$ having $\mathbf{A}$ as its corresponding matrix with respect to the standard basis $\mathcal{E} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$, then clearly $\lambda_1, \ldots, \lambda_n$ are distinct eigenvalues of $L$, with $\mathbf{e}_1, \ldots, \mathbf{e}_n$ being corresponding eigenvectors:

$$L(\mathbf{e}_k) = \mathbf{A}\mathbf{e}_k = \lambda_k \mathbf{e}_k.$$

Of course the eigenvectors $\mathbf{e}_1, \ldots, \mathbf{e}_n$ are linearly independent as predicted by Theorem 6.8. ■

**Proposition 6.11.** *An operator $L \in \mathcal{L}(V)$ is not invertible if and only if $0$ is an eigenvalue of $L$. A matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$ is not invertible if and only if $0$ is an eigenvalue of $\mathbf{A}$.*

**Proof.** By the Invertible Operator Theorem (Theorem 4.65), $L$ is not invertible if and only if $\text{Nul}(L) \neq \{\mathbf{0}\}$, and $\text{Nul}(L) \neq \{\mathbf{0}\}$ if and only if there exists some $\mathbf{v} \neq \mathbf{0}$ such that $L(\mathbf{v}) = \mathbf{0}$, which is to say 0 is an eigenvalue of $L$ since $\mathbf{0} = 0\mathbf{v}$.

By the Invertible Matrix Theorem (Theorem 5.17), $\mathbf{A}$ is not invertible if and only if $\text{Nul}(\mathbf{A}) \neq \{\mathbf{0}\}$, and $\text{Nul}(\mathbf{A}) \neq \{\mathbf{0}\}$ if and only if there exists some $\mathbf{x} \neq \mathbf{0}$ such that $\mathbf{A}\mathbf{x} = \mathbf{0}$, which is to say 0 is an eigenvalue of $\mathbf{A}$ since $\mathbf{0} = 0\mathbf{x}$. ■

**Proposition 6.12.** *Let $L \in \mathcal{L}(V)$ and $\mathbf{A} \in \mathbb{F}^{n\times n}$.*

1. *Let $n \in \mathbb{N}$. If $\lambda$ is an eigenvalue of $L$ (resp. $\mathbf{A}$) with corresponding eigenvector $\mathbf{v}$, then $\lambda^n$ is an eigenvalue of $L^n$ (resp. $\mathbf{A}^n$) with eigenvector $\mathbf{v}$.*
2. *Suppose $L$ and $\mathbf{A}$ are invertible. If $\lambda$ is an eigenvalue of $L$ (resp. $\mathbf{A}$) with corresponding eigenvector $\mathbf{v}$, then $\lambda^{-1}$ is an eigenvalue of $L^{-1}$ (resp. $\mathbf{A}^{-1}$) with eigenvector $\mathbf{v}$.*

The proof will consider only the statements about an operator $L : V \to V$, since the arguments are much the same for a square matrix $\mathbf{A}$.

**Proof.**
*Proof of Part (1):* The $n = 1$ case is trivially true. Suppose the statement of Part (1) is true for some arbitrary $n \in \mathbb{N}$. Let $\lambda$ be an eigenvalue of $L$ with corresponding eigenvector $\mathbf{v}$. Then $L(\mathbf{v}) = \lambda\mathbf{v}$, and by our inductive hypothesis $L^n(\mathbf{v}) = \lambda^n\mathbf{v}$. Now,

$$L^{n+1}(\mathbf{v}) = L^n(L(\mathbf{v})) = L^n(\lambda\mathbf{v}) = \lambda L^n(\mathbf{v}) = \lambda(\lambda^n\mathbf{v}) = \lambda^{n+1}\mathbf{v},$$

and Part (1) is proven for all $n \in \mathbb{N}$ by the principle of induction.

*Proof of Part (2):* Suppose that $\lambda$ is an eigenvalue of $L$ with corresponding eigenvector $\mathbf{v}$, so that $L(\mathbf{v}) = \lambda\mathbf{v}$. By Proposition 4.55 we obtain $L^{-1}(\lambda\mathbf{v}) = \mathbf{v}$, and since $\lambda \neq 0$ by Proposition 6.11, it follows that

$$L^{-1}(\lambda\mathbf{v}) = \mathbf{v} \;\;\Rightarrow\;\; \lambda L^{-1}(\mathbf{v}) = \mathbf{v} \;\;\Rightarrow\;\; L^{-1}(\mathbf{v}) = \lambda^{-1}\mathbf{v}.$$

Hence $\lambda^{-1}$ is an eigenvalue of $L^{-1}$. ■

## 6.2 – The Characteristic Polynomial

**Definition 6.13.** *Let* $\mathbf{A} \in \mathbb{F}^{n\times n}$*. The* ***characteristic polynomial*** *of* $\mathbf{A}$ *is the polynomial function* $P_{\mathbf{A}} : \mathbb{F} \to \mathbb{F}$ *given by*

$$P_{\mathbf{A}}(t) = \det_n(\mathbf{A} - t\mathbf{I}_n).$$

Some books define the characteristic polynomial of $\mathbf{A}$ to be $\det(t\mathbf{I}_n - \mathbf{A})$ instead of $\det(\mathbf{A} - t\mathbf{I}_n)$, but whichever way it is done will have no impact on either the theory of characteristic polynomials or any application involving them. This is because only the zeros of the characteristic polynomial will be of any concern. Setting $Q_{\mathbf{A}}(t) = \det(t\mathbf{I}_n - \mathbf{A})$, observe that $P_{\mathbf{A}} = Q_{\mathbf{A}}$ if $n$ is even, and $P_{\mathbf{A}} = -Q_{\mathbf{A}}$ if $n$ is odd. In either case $P_{\mathbf{A}}$ and $Q_{\mathbf{A}}$ will have the same zeros.

**Proposition 6.14.** *Let* $V$ *be a vector space over* $\mathbb{F}$ *with* $\dim(V) = n$*, and let* $L \in \mathcal{L}(V)$*. Then the following statements are equivalent.*

1. $\lambda$ *is an eigenvalue of* $L$ *with corresponding eigenvector* $\mathbf{u}$*.*
2. *There exists some basis* $\mathcal{B}$ *for* $V$ *such that* $\lambda$ *is an eigenvalue of* $[L]_{\mathcal{B}}$ *with corresponding eigenvector* $[\mathbf{u}]_{\mathcal{B}}$*.*
3. *For all bases* $\mathcal{B}$ *for* $V$*,* $\lambda$ *is an eigenvalue of* $[L]_{\mathcal{B}}$ *with corresponding eigenvector* $[\mathbf{u}]_{\mathcal{B}}$*.*

**Proof.**
*(1)* $\Rightarrow$ *(3):* Suppose that $\lambda$ is an eigenvalue of $L$, so there exists some $\mathbf{u} \neq \mathbf{0}$ such that $L(\mathbf{u}) = \lambda\mathbf{u}$. Let $\mathcal{B}$ be any basis for $V$, and let $[L]_{\mathcal{B}} \in \mathbb{F}^{n\times n}$ be the matrix corresponding to $L$ with respect to $\mathcal{B}$, so that

$$[L]_{\mathcal{B}}[\mathbf{v}]_{\mathcal{B}} = [L(\mathbf{v})]_{\mathcal{B}}$$

for all $\mathbf{v} \in V$. Recall that by Theorem 4.11 the coordinate map $V \to \mathbb{F}^n$ given by $\mathbf{v} \mapsto [\mathbf{v}]_{\mathcal{B}}$ is an isomorphism, so $[\mathbf{u}]_{\mathcal{B}} \in \mathbb{F}^n$ is not the zero vector since $\mathrm{Nul}([\,\cdot\,]_{\mathcal{B}}) = \{\mathbf{0}\}$. Thus, from

$$[L]_{\mathcal{B}}[\mathbf{u}]_{\mathcal{B}} = [L(\mathbf{u})]_{\mathcal{B}} = [\lambda\mathbf{u}]_{\mathcal{B}} = \lambda[\mathbf{u}]_{\mathcal{B}}$$

we conclude that $\lambda$ is an eigenvalue of $[L]_{\mathcal{B}}$ with corresponding eigenvector $[\mathbf{u}]_{\mathcal{B}}$.

*(3)* $\Rightarrow$ *(2):* This is obvious.

*(2)* $\Rightarrow$ *(1):* Suppose there exists some basis $\mathcal{B}$ for $V$ such that $\lambda$ is an eigenvalue of $[L]_{\mathcal{B}}$ with corresponding eigenvector $[\mathbf{u}]_{\mathcal{B}}$. Again, the coordinate map $[\,\cdot\,]_{\mathcal{B}} : V \to \mathbb{F}^n$ is an isomorphism, so

$$[L]_{\mathcal{B}}[\mathbf{u}]_{\mathcal{B}} = \lambda[\mathbf{u}]_{\mathcal{B}} \;\;\Rightarrow\;\; [L(\mathbf{u})]_{\mathcal{B}} = [\lambda\mathbf{u}]_{\mathcal{B}} \;\;\Rightarrow\;\; L(\mathbf{u}) = \lambda\mathbf{u},$$

where the last implication follows from the fact that $[\,\cdot\,]_{\mathcal{B}} : V \to \mathbb{F}^n$ is injective. Therefore $\lambda$ is an eigenvalue of $L$ with corresponding eigenvector $\mathbf{u}$. ∎

We see from the proposition that if we consider two different bases $\mathcal{B}$ and $\mathcal{B}'$ for $V$, then the matrices corresponding to $L$ with respect to these bases, $[L]_{\mathcal{B}}$ and $[L]_{\mathcal{B}'}$, have the same eigenvalues as $L$. The only thing that changes is the corresponding eigenvector: $[\mathbf{v}]_{\mathcal{B}}$ is an eigenvector of $[L]_{\mathcal{B}}$ corresponding to eigenvalue $\lambda$ if and only if $[\mathbf{v}]_{\mathcal{B}'}$ is an eigenvector of $[L]_{\mathcal{B}'}$ corresponding to eigenvalue $\lambda$.

But there's something more: the characteristic polynomials of $[L]_{\mathcal{B}}$ and $[L]_{\mathcal{B}'}$ will be found to be the same! To see this, recall $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$, the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$. By Corollary 4.33 we have

$$[L]_{\mathcal{B}'} = \mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}}\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}.$$

Now, noting that $\mathbf{I}_n = \mathbf{I}_{\mathcal{B}\mathcal{B}'}\mathbf{I}_n\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}$ and

$$\det(\mathbf{I}_{\mathcal{B}\mathcal{B}'})\det(\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}) = \det(\mathbf{I}_{\mathcal{B}\mathcal{B}'}) \cdot \frac{1}{\det(\mathbf{I}_{\mathcal{B}\mathcal{B}'})} = 1$$

by Theorem 5.24, for any $t \in \mathbb{F}$ we have

$$\begin{aligned}
P_{[L]_{\mathcal{B}'}}(t) &= \det([L]_{\mathcal{B}'} - t\mathbf{I}_n) = \det\big(\mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}}\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1} - t(\mathbf{I}_{\mathcal{B}\mathcal{B}'}\mathbf{I}_n\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1})\big) \\
&= \det\big((\mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}} - t(\mathbf{I}_{\mathcal{B}\mathcal{B}'}\mathbf{I}_n))\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}\big) = \det\big((\mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}} - \mathbf{I}_{\mathcal{B}\mathcal{B}'}(t\mathbf{I}_n))\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}\big) \\
&= \det\big(\mathbf{I}_{\mathcal{B}\mathcal{B}'}([L]_{\mathcal{B}} - t\mathbf{I}_n)\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}\big) = \det(\mathbf{I}_{\mathcal{B}\mathcal{B}'})\det([L]_{\mathcal{B}} - t\mathbf{I}_n)\det(\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}) \\
&= \det([L]_{\mathcal{B}} - t\mathbf{I}_n) = P_{[L]_{\mathcal{B}}}(t)
\end{aligned}$$

by Theorem 5.23. That is, $P_{[L]_{\mathcal{B}'}} = P_{[L]_{\mathcal{B}}}$, which is to say that the characteristic polynomial of a linear operator's associated matrix is invariant under change of basis. We have proven the following.

**Proposition 6.15.** *Let $L : V \to V$ be a linear operator, and let $\mathcal{B}$ and $\mathcal{B}'$ be bases for $V$. If $[L]_{\mathcal{B}}$ and $[L]_{\mathcal{B}'}$ are the matrices corresponding to $L$ with respect to $\mathcal{B}$ and $\mathcal{B}'$, then $P_{[L]_{\mathcal{B}}} = P_{[L]_{\mathcal{B}'}}$.*

Because of Proposition 6.15, it makes sense to speak of the "characteristic polynomial" of a linear operator on $V$ without reference to any specific basis for $V$.

**Definition 6.16.** *Let $L$ be a linear operator on $V$. The **characteristic polynomial of** $L$ is the polynomial function $P_L : \mathbb{F} \to \mathbb{F}$ given by*

$$P_L(t) = P_{[L]}(t),$$

*where $[L]$ is the matrix corresponding to $L$ with respect to any basis for $V$.*

While the idea of an eigenvalue is simple, it can be quite difficult to find eigenvalues of either a linear operator or a matrix by direct means. To help find the eigenvalue of a linear operator we have the following.

**Theorem 6.17.** *Let $L : V \to V$ be a linear operator. Then $\lambda$ is an eigenvalue of $L$ if and only if $L - \lambda I_V$ is not invertible.*

**Proof.** Suppose that $\lambda$ is an eigenvalue of $L$. Then there exists some $\mathbf{v} \in V$ such that $\mathbf{v} \neq \mathbf{0}$ and $L(\mathbf{v}) = \lambda\mathbf{v}$. Now,

$$(L - \lambda I_V)(\mathbf{v}) = L(\mathbf{v}) - (\lambda I_V)(\mathbf{v}) = \lambda\mathbf{v} - \lambda I_V(\mathbf{v}) = \lambda\mathbf{v} - \lambda\mathbf{v} = \mathbf{0},$$

which shows that $\mathbf{v} \in \text{Nul}(L - \lambda I_V)$ and so $\text{Nul}(L - \lambda I_V) \neq \{\mathbf{0}\}$. Hence $L - \lambda I_V$ is not invertible by the Invertible Operator Theorem.

For the converse, suppose that $L - \lambda I_V$ is not invertible. Then $\text{Nul}(L - \lambda I_V) \neq \{\mathbf{0}\}$ by the Invertible Operator Theorem, and it follows that there exists some $\mathbf{v} \neq \mathbf{0}$ such that $(L - \lambda I_V)(\mathbf{v}) = \mathbf{0}$. Now,

$$(L - \lambda I_V)(\mathbf{v}) = \mathbf{0} \;\Leftrightarrow\; L(\mathbf{v}) - \lambda I_V(\mathbf{v}) = \mathbf{0} \;\Leftrightarrow\; L(\mathbf{v}) - \lambda \mathbf{v} = \mathbf{0} \;\Leftrightarrow\; L(\mathbf{v}) = \lambda \mathbf{v},$$

and therefore $\lambda$ is an eigenvalue of $L$. ■

The next theorem plainly reduces the problem of finding eigenvalues of an $n \times n$ matrix to that of finding the zeros of an $n$th-degree polynomial function. We begin to see the utility of characteristic polynomials at this point.

**Theorem 6.18.** *Let $\mathbf{A} \in \mathbb{F}^{n \times n}$. Then $\lambda$ is an eigenvalue of $\mathbf{A}$ if and only if $P_{\mathbf{A}}(\lambda) = 0$.*

**Proof.** Suppose that $\lambda$ is an eigenvalue of $\mathbf{A}$, so that $\mathbf{A}\mathbf{x}_0 = \lambda \mathbf{x}_0$ for some $\mathbf{x}_0 \in \mathbb{F}^n$. Define the linear mapping $L : \mathbb{F}^n \to \mathbb{F}^n$ by $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$. Then

$$L(\mathbf{x}_0) = \mathbf{A}\mathbf{x}_0 = \lambda \mathbf{x}_0$$

shows that $\lambda$ is an eigenvalue of $L$, and so by Theorem 6.17 the mapping

$$L - \lambda I_{\mathbb{F}^n} : \mathbb{F}^n \to \mathbb{F}^n$$

is not invertible. Let $I = I_{\mathbb{F}^n}$, and observe that the matrix associated with $L - \lambda I$ is $\mathbf{A} - \lambda \mathbf{I}_n$:

$$(L - \lambda I)(\mathbf{x}) = L(\mathbf{x}) - \lambda I(\mathbf{x}) = \mathbf{A}\mathbf{x} - \lambda \mathbf{x} = \mathbf{A}\mathbf{x} - \lambda \mathbf{I}_n \mathbf{x} = (\mathbf{A} - \lambda \mathbf{I}_n)\mathbf{x}$$

for all $\mathbf{x} \in \mathbb{F}^n$. Thus, since the operator $L - \lambda I$ is not invertible, by Corollary 4.59 its associated square matrix $\mathbf{A} - \lambda \mathbf{I}_n$ is also not invertible, and so $\det(\mathbf{A} - \lambda \mathbf{I}_n) = 0$ by the Invertible Matrix Theorem. That is, $P_{\mathbf{A}}(\lambda) = 0$.

Conversely, suppose that $P_{\mathbf{A}}(\lambda) = 0$. Then $\det(\mathbf{A} - \lambda \mathbf{I}_n) = 0$, so by the Invertible Matrix Theorem $\mathbf{A} - \lambda \mathbf{I}_n$ is not invertible. Define $L : \mathbb{F}^n \to \mathbb{F}^n$ by $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$. Then $\mathbf{A} - \lambda \mathbf{I}_n$ is the matrix corresponding to the linear operator $L - \lambda I : \mathbb{F}^n \to \mathbb{F}^n$, and by Corollary 4.59 $L - \lambda I$ is not invertible. So $\lambda$ is an eigenvalue of $L$ by Theorem 6.17, which is to say there exists some nonzero $\mathbf{x}_0 \in \mathbb{F}^n$ such that $L(\mathbf{x}_0) = \lambda \mathbf{x}_0$. Hence $\mathbf{A}\mathbf{x}_0 = \lambda \mathbf{x}_0$ and we conclude that $\lambda$ is an eigenvalue of $\mathbf{A}$. ■

**Example 6.19.** Find the characteristic polynomial $P_{\mathbf{A}} : \mathbb{R} \to \mathbb{R}$ of

$$\mathbf{A} = \begin{bmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{bmatrix},$$

find the eigenvalues of $\mathbf{A}$, and find a basis for each eigenspace as a subspace of $\mathbb{R}^3$.

**Solution.** We have

$$P_{\mathbf{A}}(t) = \det(\mathbf{A} - t\mathbf{I}_3) = \det\left(\begin{bmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{bmatrix} - \begin{bmatrix} t & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & t \end{bmatrix}\right) = \begin{vmatrix} 1-t & -3 & 3 \\ 3 & -5-t & 3 \\ 6 & -6 & 4-t \end{vmatrix}$$

$$\xlongequal{c_1+c_2 \to c_2} \begin{vmatrix} 1-t & -2-t & 3 \\ 3 & -2-t & 3 \\ 6 & 0 & 4-t \end{vmatrix} \xlongequal{-r_1+r_2 \to r_2} \begin{vmatrix} 1-t & -2-t & 3 \\ t+2 & 0 & 0 \\ 6 & 0 & 4-t \end{vmatrix}.$$

Expanding the determinant according to the 2nd row then gives

$$P_{\mathbf{A}}(t) = (-1)^{2+1}(t+2)\begin{vmatrix} -2-t & 3 \\ 0 & 4-t \end{vmatrix} = (t+2)^2(t-4),$$

and so we see that $P_{\mathbf{A}}(t) = 0$ for $t = -2, 4$. Thus by Theorem 6.18 the eigenvalues of $\mathbf{A}$ are $\lambda = -2, 4$.

By (6.1) the eigenspace of $\mathbf{A}$ corresponding to $\lambda = -2$ is

$$\begin{aligned} E_{\mathbf{A}}(-2) &= \mathrm{Nul}(\mathbf{A} + 2\mathbf{I}_3) = \{\mathbf{x} \in \mathbb{R}^3 : (\mathbf{A} + 2\mathbf{I}_3)\mathbf{x} = \mathbf{0}\} \\ &= \left\{ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \in \mathbb{R}^3 : \begin{bmatrix} 3 & -3 & 3 \\ 3 & -3 & 3 \\ 6 & -6 & 6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\}. \end{aligned}$$

Writing the matrix equation—which is a homogeneous system of equations—as an augmented matrix, we have

$$\left[\begin{array}{ccc|c} 3 & -3 & 3 & 0 \\ 3 & -3 & 3 & 0 \\ 6 & -6 & 6 & 0 \end{array}\right] \xrightarrow[-2r_1+r_3 \to r_3]{-r_1+r_2 \to r_2} \left[\begin{array}{ccc|c} 3 & -3 & 3 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] \xrightarrow{\frac{1}{3}r_1 \to r_1} \left[\begin{array}{ccc|c} 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]. \tag{6.7}$$

Hence $x_1 - x_2 + x_3 = 0$, which implies that $x_3 = x_2 - x_1$ and so

$$E_{\mathbf{A}}(-2) = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \in \mathbb{R}^3 : x_1 - x_2 + x_3 = 0 \right\} = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ x_2 - x_1 \end{bmatrix} : x_1, x_2 \in \mathbb{R} \right\}.$$

Observing that

$$\begin{bmatrix} x_1 \\ x_2 \\ x_2 - x_1 \end{bmatrix} = \begin{bmatrix} x_1 \\ 0 \\ -x_1 \end{bmatrix} + \begin{bmatrix} 0 \\ x_2 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} x_1 + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} x_2,$$

we have

$$E_{\mathbf{A}}(-2) = \left\{ \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} x_1 + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} x_2 : x_1, x_2 \in \mathbb{R} \right\}$$

and so it is clear that

$$\mathcal{B}_{-2} = \left\{ \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \right\}$$

is a linearly independent set of vectors that spans $E_{\mathbf{A}}(-2)$ and therefore must be a basis for $E_{\mathbf{A}}(-2)$. Notice that the elements of $\mathcal{B}_{-2}$ are in fact eigenvectors of $\mathbf{A}$ corresponding to the eigenvalue $-2$, as are all the vectors belonging to $E_{\mathbf{A}}(-2)$.

Next, the eigenspace of $\mathbf{A}$ corresponding to $\lambda = 4$ is

$$\begin{aligned} E_{\mathbf{A}}(4) &= \text{Nul}(\mathbf{A} - 4\mathbf{I}_3) = \{\mathbf{x} \in \mathbb{R}^3 : (\mathbf{A} - 4\mathbf{I}_3)\mathbf{x} = \mathbf{0}\} \\ &= \left\{ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \in \mathbb{R}^3 : \begin{bmatrix} -3 & -3 & 3 \\ 3 & -9 & 3 \\ 6 & -6 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\}. \end{aligned}$$

Applying Gaussian Elimination to the corresponding augmented matrix yields

$$\left[\begin{array}{rrr|r} -3 & -3 & 3 & 0 \\ 3 & -9 & 3 & 0 \\ 6 & -6 & 0 & 0 \end{array}\right] \xrightarrow[2r_1+r_3\to r_3]{r_1+r_2\to r_2} \left[\begin{array}{rrr|r} -3 & -3 & 3 & 0 \\ 0 & -12 & 6 & 0 \\ 0 & -12 & 6 & 0 \end{array}\right] \xrightarrow[-\frac{1}{2}r_2+r_1\to r_1]{-r_2+r_3\to r_3} \left[\begin{array}{rrr|r} -3 & 3 & 0 & 0 \\ 0 & -12 & 6 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

From the top row we obtain $x_2 = x_1$, and from the middle row we obtain $x_3 = 2x_2$ and thus $x_3 = 2x_1$. Now,

$$E_{\mathbf{A}}(4) = \left\{ \begin{bmatrix} x_1 \\ x_1 \\ 2x_1 \end{bmatrix} : x_1 \in \mathbb{R} \right\} = \left\{ \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} x_1 : x_1 \in \mathbb{R} \right\}.$$

Clearly

$$\mathcal{B}_4 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} \right\}$$

is a linearly independent set that spans $E_{\mathbf{A}}(4)$ and so qualifies as a basis for $E_{\mathbf{A}}(4)$. The vector belonging to $\mathcal{B}_4$ is an eigenvector of $\mathbf{A}$ corresponding to the eigenvalue 4, as is any real scalar multiple of the vector. ■

In Example 6.19 we found in (6.7) that $\mathbf{A} + 2\mathbf{I}_3$ is row-equivalent to

$$\mathbf{B} = \begin{bmatrix} 1 & -1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

which clearly has rank 1, and so

$$\text{rank}(\mathbf{A} + 2\mathbf{I}_3) = \text{rank}(\mathbf{B}) = 1$$

by Theorem 3.66. Then by the Rank-Nullity Theorem for Matrices we have

$$\dim(E_{\mathbf{A}}(-2)) = \text{nullity}(\mathbf{A} + 2\mathbf{I}_3) = \dim(\mathbb{R}^3) - \text{rank}(\mathbf{A} + 2\mathbf{I}_3) = 3 - 1 = 2. \tag{6.8}$$

Then, employing the equation $x_1 - x_2 + x_3 = 0$ obtained at right in (6.7), we could have easily obtained the two solutions

$$\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$$

Since these two vectors in $E_{\mathbf{A}}(-2)$ are linearly independent and we know from (6.8) that $E_{\mathbf{A}}(-2)$ has dimension 2, we can conclude by Theorem 3.54(1) that the two vectors must be a basis for $E_{\mathbf{A}}(-2)$. We mention this here in order to suggest an alternative means of finding a basis for an eigenspace which makes use of earlier theoretical developments.

In the next example, for variety's sake, eigenspaces will be found using Definition 6.5 directly, rather than equation (6.1).

**Example 6.20.** Find the eigenvalues of the matrix

$$\mathbf{A} = \begin{bmatrix} -1 & 4 & -2 \\ -3 & 4 & 0 \\ -3 & 1 & 3 \end{bmatrix},$$

and also find a basis for each eigenspace as a subspace of $\mathbb{R}^3$.

**Solution.** Expanding the determinant according to the second row, we have

$$\begin{aligned} P_{\mathbf{A}}(t) = \det(\mathbf{A} - t\mathbf{I}_3) &= \begin{vmatrix} -1-t & 4 & -2 \\ -3 & 4-t & 0 \\ -3 & 1 & 3-t \end{vmatrix} \\ &= (-1)^{2+1}(-3)\begin{vmatrix} 4 & -2 \\ 1 & 3-t \end{vmatrix} + (-1)^{2+2}(4-t)\begin{vmatrix} -1-t & -2 \\ -3 & 3-t \end{vmatrix} \\ &= -t^3 + 6t^2 - 11t + 6, \end{aligned}$$

and so

$$P_{\mathbf{A}}(t) = 0 \quad \Leftrightarrow \quad t^3 - 6t^2 + 11t - 6 = 0.$$

By the Rational Zeros Theorem of algebra, the only rational numbers that may be zeros of $P_{\mathbf{A}}$ are $\pm 1$, $\pm 2$, $\pm 3$ and $\pm 6$. It's an easy matter to verify that 1 is in fact a zero, and so by the Factor Theorem of algebra $t - 1$ must be a factor of $P_{\mathbf{A}}(t)$. Now,

$$\frac{t^3 - 6t^2 + 11t - 6}{t - 1} = t^2 - 5t + 6,$$

whence we obtain

$$t^3 - 6t^2 + 11t - 6 = 0 \quad \Leftrightarrow \quad (t-1)(t^2 - 5t + 6) = 0 \quad \Leftrightarrow \quad (t-1)(t-2)(t-3) = 0,$$

and therefore $P_{\mathbf{A}}(t) = 0$ if and only if $t = 1, 2, 3$. By Theorem 6.18 the eigenvalues of $\mathbf{A}$ are $\lambda = 1, 2, 3$.

The eigenspace of $\mathbf{A}$ corresponding to $\lambda = 1$ is

$$E_{\mathbf{A}}(1) = \{\mathbf{x} \in \mathbb{R}^3 : \mathbf{A}\mathbf{x} = \mathbf{x}\} = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3 : \begin{bmatrix} -1 & 4 & -2 \\ -3 & 4 & 0 \\ -3 & 1 & 3 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \right\}.$$

The matrix equation yields the system of equations

$$\begin{cases} -x + 4y - 2z = x \\ -3x + 4y \phantom{{}-2z} = y \\ -3x + \phantom{4}y + 3z = z \end{cases}$$

or equivalently

$$\begin{cases} -x + 2y - 1z = 0 \\ -x + \ \ y \qquad\ = 0 \\ -3x + \ \ y + 2z = 0 \end{cases}$$

Apply Gaussian elimination on the corresponding augmented matrix:

$$\left[\begin{array}{rrr|r} -1 & 2 & -1 & 0 \\ -1 & 1 & 0 & 0 \\ -3 & 1 & 2 & 0 \end{array}\right] \xrightarrow[-3r_1+r_3\to r_3]{-r_1+r_2\to r_2} \left[\begin{array}{rrr|r} -1 & 2 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & -5 & 5 & 0 \end{array}\right] \xrightarrow{-5r_2+r_3\to r_3} \left[\begin{array}{rrr|r} -1 & 2 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right],$$

so from the second row we have $y = z$, and from the first row we have $x = 2y - z = 2z - z = z$. Replacing $z$ with $t$, so that $x = y = z = t$, we have

$$E_{\mathbf{A}}(1) = \left\{ \begin{bmatrix} t \\ t \\ t \end{bmatrix} : t \in \mathbb{R} \right\} = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} t : t \in \mathbb{R} \right\}.$$

From this we see that the set

$$\mathcal{B}_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}$$

is a basis for $E_{\mathbf{A}}(1)$.

The eigenspace of $\mathbf{A}$ corresponding to $\lambda = 2$ is

$$E_{\mathbf{A}}(2) = \{\mathbf{x} \in \mathbb{R}^3 : \mathbf{A}\mathbf{x} = 2\mathbf{x}\} = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3 : \begin{bmatrix} -1 & 4 & -2 \\ -3 & 4 & 0 \\ -3 & 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2x \\ 2y \\ 2z \end{bmatrix} \right\}.$$

The matrix equation yields the system of equations

$$\begin{cases} -3x + 4y - 2z = 0 \\ -3x + 2y \qquad\ = 0 \\ -3x + \ \ y + \ \ z = 0 \end{cases}$$

Apply Gaussian elimination on the corresponding augmented matrix:

$$\left[\begin{array}{rrr|r} -3 & 4 & -2 & 0 \\ -3 & 2 & 0 & 0 \\ -3 & 1 & 1 & 0 \end{array}\right] \xrightarrow[-r_1+r_3\to r_3]{-r_1+r_2\to r_2} \left[\begin{array}{rrr|r} -3 & 4 & -2 & 0 \\ 0 & -2 & 2 & 0 \\ 0 & -3 & 3 & 0 \end{array}\right] \xrightarrow{-\frac{3}{2}r_2+r_3\to r_3} \left[\begin{array}{rrr|r} -3 & 4 & -2 & 0 \\ 0 & -2 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right],$$

so from the second row we have $y = z$, and from the first row we have

$$x = \frac{4}{3}y - \frac{2}{3}z = \frac{4}{3}z - \frac{2}{3}z = \frac{2}{3}z.$$

Hence

$$E_{\mathbf{A}}(2) = \left\{ \begin{bmatrix} 2z/3 \\ z \\ z \end{bmatrix} : z \in \mathbb{R} \right\} = \left\{ \begin{bmatrix} 2/3 \\ 1 \\ 1 \end{bmatrix} z : z \in \mathbb{R} \right\}.$$

If we replace $z$ with $3t$, we obtain an equivalent rendition of $E_2$ that features no fractions:

$$E_{\mathbf{A}}(2) = \left\{ \begin{bmatrix} 2 \\ 3 \\ 3 \end{bmatrix} t \,:\, t \in \mathbb{R} \right\}.$$

The set

$$\mathcal{B}_2 = \left\{ \begin{bmatrix} 2 \\ 3 \\ 3 \end{bmatrix} \right\}$$

is a basis for $E_2$.

Finally, the eigenspace of $\mathbf{A}$ corresponding to $\lambda = 3$ is

$$E_{\mathbf{A}}(3) = \{\mathbf{x} \in \mathbb{R}^3 : \mathbf{A}\mathbf{x} = 3\mathbf{x}\} = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3 \,:\, \begin{bmatrix} -1 & 4 & -2 \\ -3 & 4 & 0 \\ -3 & 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3x \\ 3y \\ 3z \end{bmatrix} \right\}.$$

The matrix equation yields the system of equations

$$\begin{cases} -4x + 4y - 2z = 0 \\ -3x + \phantom{4}y \phantom{{}-2z} = 0 \\ -3x + \phantom{4}y \phantom{{}-2z} = 0 \end{cases}$$

Once more we apply Gaussian elimination to the augmented matrix:

$$\left[\begin{array}{ccc|c} -4 & 4 & -2 & 0 \\ -3 & 1 & 0 & 0 \\ -3 & 1 & 0 & 0 \end{array}\right] \xrightarrow[\frac{1}{2}r_1 \to r_1]{-r_2 + r_3 \to r_3} \left[\begin{array}{ccc|c} -2 & 2 & -1 & 0 \\ -3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right],$$

so $y = 3x$ and $-2x + 2y - z = 0$, where

$$-2x + 2y - z = 0 \;\Rightarrow\; z = -2x + 2y \;\Rightarrow\; z = 4x.$$

Therefore, replacing $x$ with $t$ so that $y = 3t$ and $z = 4t$, we have

$$E_{\mathbf{A}}(3) = \left\{ \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} t \,:\, t \in \mathbb{R} \right\}.$$

The set

$$\mathcal{B}_3 = \left\{ \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \right\}$$

is a basis for $E_{\mathbf{A}}(3)$. ■

**Example 6.21.** Find the eigenvalues of the matrix

$$\mathbf{A} = \begin{bmatrix} 2 & 3 \\ -1 & 4 \end{bmatrix},$$

and also find a basis for each eigenspace as a subspace of $\mathbb{C}^2$.

**Solution.** We have

$$P_{\mathbf{A}}(t)=\det(\mathbf{A}-t\mathbf{I}_2)=\begin{vmatrix}2-t & 3\\ -1 & 4-t\end{vmatrix}=t^2-6t+11,$$

and so

$$P_{\mathbf{A}}(t)=0 \quad\Leftrightarrow\quad t^2-6t+11=0 \quad\Leftrightarrow\quad t=3\pm i\sqrt{2}.$$

That is, $\mathbf{A}$ has two complex-valued eigenvalues. Let $\lambda=3-i\sqrt{2}$. The eigenspace corresponding to $\lambda$ is

$$E_{\mathbf{A}}(\lambda)=\{\mathbf{z}\in\mathbb{C}^2:\mathbf{A}\mathbf{z}=\lambda\mathbf{z}\}=\left\{\begin{bmatrix}z_1\\ z_2\end{bmatrix}\in\mathbb{C}^2 : \begin{bmatrix}2 & 3\\ -1 & 4\end{bmatrix}\begin{bmatrix}z_1\\ z_2\end{bmatrix}=\begin{bmatrix}\lambda z_1\\ \lambda z_2\end{bmatrix}\right\}.$$

Now,

$$\begin{bmatrix}2 & 3\\ -1 & 4\end{bmatrix}\begin{bmatrix}z_1\\ z_2\end{bmatrix}=\begin{bmatrix}\lambda z_1\\ \lambda z_2\end{bmatrix}$$

corresponds to the system of equations

$$\begin{cases}(2-\lambda)z_1+ \quad 3z_2=0\\ \quad -z_1+(4-\lambda)z_2=0\end{cases}$$

We apply Gaussian elimination to the augmented matrix,

$$\left[\begin{array}{cc|c}2-\lambda & 3 & 0\\ -1 & 4-\lambda & 0\end{array}\right]\xrightarrow{r_1\leftrightarrow r_2}\left[\begin{array}{cc|c}-1 & 4-\lambda & 0\\ 2-\lambda & 3 & 0\end{array}\right]\xrightarrow{(2-\lambda)r_1+r_2\to r_2}\left[\begin{array}{cc|c}-1 & 4-\lambda & 0\\ 0 & 0 & 0\end{array}\right],$$

observing that

$$(2-\lambda)(4-\lambda)+3=(\lambda^2-6\lambda+8)+3=\big(3-i\sqrt{2}\big)^2-6\big(3-i\sqrt{2}\big)+11=0.$$

Thus

$$z_1=\big(-1-i\sqrt{2}\big)z_2,$$

and so we obtain

$$E_{\mathbf{A}}(\lambda)=\left\{\begin{bmatrix}\big(-1-i\sqrt{2}\big)z_2\\ z_2\end{bmatrix}: z_2\in\mathbb{C}\right\}=\left\{\begin{bmatrix}-1-i\sqrt{2}\\ 1\end{bmatrix}z : z\in\mathbb{C}\right\},$$

where for simplicity we replace $z_2$ with $z$ in the end. Hence the eigenvector

$$\begin{bmatrix}-1-i\sqrt{2}\\ 1\end{bmatrix}$$

corresponding to the eigenvalue $3-i\sqrt{2}$ constitutes a basis for the eigenspace $E_{\mathbf{A}}(\lambda)$.

The analysis of the other eigenvalue $3+i\sqrt{2}$ is quite similar (with eigenspace also of dimension 1) and so is left as a problem. ■

**Example 6.22.** We will show that, for all $n\in\mathbb{N}$, if $\mathbf{A}\in\mathbb{F}$ is given by

$$\mathbf{A}=\begin{bmatrix}0 & 0 & 0 & \cdots & 0 & -a_0\\ 1 & 0 & 0 & \cdots & 0 & -a_1\\ 0 & 1 & 0 & \cdots & 0 & -a_2\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2}\\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1}\end{bmatrix}, \tag{6.9}$$

then

$$P_{\mathbf{A}}(t) = (-1)^n(a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + t^n). \tag{6.10}$$

In the case when $n = 1$ we take $\mathbf{A} = [-a_0]$, whereupon we obtain

$$P_{\mathbf{A}}(t) = \det_1(\mathbf{A} - t\mathbf{I}_1) = \det_1([-a_0 - t]) = -a_0 - t = (-1)(a_0 + t).$$

This establishes the base case of an inductive argument. Fix $n \in \mathbb{N}$, and suppose any matrix of the form (6.9) has characteristic polynomial (6.10); that is, $\det_n(\mathbf{A} - t\mathbf{I}_n)$ is given by

$$\begin{vmatrix} -t & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & -t & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & -t & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -t & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} - t \end{vmatrix} = (-1)^n(a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + t^n).$$

Now, define $\mathbf{A} \in \mathbb{F}^{(n+1)\times(n+1)}$ by

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 0 & 0 & \cdots & 1 & -a_n \end{bmatrix},$$

so

$$\mathbf{A} - t\mathbf{I}_{n+1} = \begin{bmatrix} -t & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & -t & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & -t & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -t & -a_{n-1} \\ 0 & 0 & 0 & \cdots & 1 & -a_n - t \end{bmatrix}.$$

Letting $\mathbf{B} = \mathbf{A} - t\mathbf{I}_{n+1}$,

$$\begin{aligned} P_{\mathbf{A}}(t) = \det_{n+1}(\mathbf{B}) &= \sum_{j=1}^{n+1}(-1)^{1+j}a_{1j}\det_n(\mathbf{B}_{1j}) \\ &= -t\det_n(\mathbf{B}_{11}) + (-1)^{n+2}(-a_0)\det_n(\mathbf{B}_{1(n+1)}), \end{aligned}$$

where

$$\mathbf{B}_{11} = \begin{bmatrix} -t & 0 & 0 & \cdots & 0 & -a_1 \\ 1 & -t & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & -t & \cdots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -t & -a_{n-1} \\ 0 & 0 & 0 & \cdots & 1 & -a_n - t \end{bmatrix} \quad \text{and} \quad \mathbf{B}_{1(n+1)} = \begin{bmatrix} 1 & -t & 0 & \cdots & 0 & 0 \\ 0 & 1 & -t & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -t \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Clearly $\det_n(\mathbf{B}_{1(n+1)}) = 1$, and by the inductive hypothesis we have

$$\det_n(\mathbf{B}_{11}) = (-1)^n(a_1 + a_2t + \cdots + a_nt^{n-1} + t^n),$$

so that

$$\begin{aligned} P_{\mathbf{A}}(t) &= -t(-1)^n(a_1 + a_2t + \cdots + a_nt^{n-1} + t^n) - (-1)^n a_0 \\ &= (-1)^{n+1}(a_1t + a_2t^2 + \cdots + a_nt^n + t^{n+1}) + (-1)^{n+1}a_0 \\ &= (-1)^{n+1}(a_0 + a_1t + \cdots + a_nt^n + t^{n+1}), \end{aligned}$$

as desired. ∎

## Problems

1. For each of the $2 \times 2$ matrices below, do the following:
   (i) Find the characteristic equation.
   (ii) Find all real eigenvalues.
   (iii) Find a basis for the eigenspace corresponding to each real eigenvalue.

$$\text{(a)} \begin{bmatrix} 3 & 0 \\ 8 & -1 \end{bmatrix} \qquad \text{(b)} \begin{bmatrix} 0 & 3 \\ 4 & 0 \end{bmatrix} \qquad \text{(c)} \begin{bmatrix} -2 & -7 \\ 1 & 2 \end{bmatrix} \qquad \text{(d)} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

2. For each of the $3 \times 3$ matrices below, do the following:
   (i) Find the characteristic equation.
   (ii) Find all real eigenvalues.
   (iii) Find a basis for the eigenspace corresponding to each real eigenvalue.

$$\text{(a)} \begin{bmatrix} 4 & 0 & 1 \\ -2 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix} \qquad \text{(b)} \begin{bmatrix} 3 & 0 & -5 \\ \frac{1}{5} & -1 & 0 \\ 1 & 1 & -2 \end{bmatrix} \qquad \text{(c)} \begin{bmatrix} 5 & 6 & 2 \\ 0 & -1 & -8 \\ 1 & 0 & -2 \end{bmatrix}$$

3. For each of the $4 \times 4$ matrices below, do the following:
   (i) Find the characteristic equation.
   (ii) Find all real eigenvalues.
   (iii) Find a basis for the eigenspace corresponding to each real eigenvalue.

$$\text{(a)} \begin{bmatrix} 0 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad \text{(b)} \begin{bmatrix} 10 & -9 & 0 & 0 \\ 4 & -2 & 0 & 0 \\ 0 & 0 & -2 & -7 \\ 0 & 0 & 1 & 2 \end{bmatrix}$$

## 6.3 – Applications of the Characteristic Polynomial

Recall that $\mathcal{P}_n(\mathbb{F})$ denotes the set of polynomials of degree $n$ with coefficients in $\mathbb{F}$. That is, for $n \in \mathbb{W}$,

$$\mathcal{P}_n(\mathbb{F}) = \left\{ \sum_{k=0}^{n} a_k x^k : a_0, \ldots, a_n \in \mathbb{F} \text{ and } a_n \neq 0 \right\}.$$

We regard 0 to be the polynomial of degree $-1$ and define $\mathcal{P}_{-1}(\mathbb{F}) = \{0\}$. If $\mathbb{F}$ is an infinite field such as $\mathbb{R}$ or $\mathbb{C}$, it is common to treat a polynomial as a function $f : \mathbb{F} \to \mathbb{F}$ given by

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

for all $x \in \mathbb{F}$, in which case it is called a polynomial function. For $n \geq -1$, a polynomial function $p$ is said to have degree $n$ if $f(x) \in \mathcal{P}_n(\mathbb{F})$, in which case we write $\deg(p) = n$. Thus, we may just as well regard $\mathcal{P}_n(\mathbb{F})$ as the set of all polynomial functions of degree $n$, so that it makes as much sense to write $f \in \mathcal{P}_n(\mathbb{F})$ as $f(x) \in \mathcal{P}_n(\mathbb{F})$. Finally, we define

$$\mathcal{P}(\mathbb{F}) = \bigcup_{n=0}^{\infty} \mathcal{P}_{n-1}(\mathbb{F}).$$

In what follows we will have need of the following theorem, which is proven in §5.1 of the Complex Analysis Notes.

**Theorem 6.23** (**Fundamental Theorem of Algebra**). *If*

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

*is a polynomial function of degree $n \geq 1$ with coefficients $a_0, \ldots, a_n \in \mathbb{C}$, then there exists some $z_0 \in \mathbb{C}$ such that $p(z_0) = 0$.*

**Theorem 6.24** (**Division Algorithm for Polynomials**). *Let $f \in \mathcal{P}_n(\mathbb{F})$, and let $g \in \mathcal{P}_m(\mathbb{F})$ for some $m \geq 0$. Then there exist unique polynomial functions $q$ and $r$ such that*

$$f(x) = q(x)g(x) + r(x)$$

*for all $x \in \mathbb{F}$, where $\deg(r) \leq m$.*

**Theorem 6.25** (**Factor Theorem**). *Let $f \in \mathcal{P}_n(\mathbb{F})$ for some $n \geq 1$, and let $c \in \mathbb{F}$. Then $f(c) = 0$ if and only if $x - c$ is a factor of $f(x)$.*

**Lemma 6.26.** *Suppose $\mathbf{P}(t) = [p_{ij}(t)]_n \in \mathbb{F}^{n \times n}$ is such that $p_{ij}$ is a polynomial function for all $1 \leq i, j \leq n$. If*

$$\deg(p_{ij}) \leq \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

*then $\deg(\det_n(\mathbf{P}(t))) \leq n$.*

**Proof.** The statement of the lemma is clearly true in the case when $n = 1$. Suppose that it is true for some arbitrary $n \in \mathbb{N}$. Let $\mathbf{P}(t) = [p_{ij}(t)]_{n+1}$. Then, expanding along the first row, we have

$$\det_{n+1}(\mathbf{P}(t)) = \sum_{j=1}^{n+1}(-1)^{1+j} p_{1j}(t) \det_n(\mathbf{P}_{1j}(t)).$$

For each $1 \leq j \leq n+1$ we find that the $n \times n$ submatrix $\mathbf{P}_{1j}$ is such that all non-diagonal entries are degree 0 polynomial functions (i.e. constants), and all diagonal entries are polynomial functions of either degree 0 or degree 1. Thus $\deg(\det_n(\mathbf{P}_{1j})) \leq n$ by our inductive hypothesis, and since $p_{1j}(t)$ is a constant for $2 \leq j \leq n+1$, it follows that

$$\deg\big((-1)^{1+j} p_{1j}(t) \det_n(\mathbf{P}_{1j}(t))\big) \leq n$$

for $2 \leq j \leq n+1$. In the case when $j = 1$ we have

$$(-1)^{1+j} p_{1j}(t) \det_n(\mathbf{P}_{1j}(t)) = p_{11}(t) \det_n(\mathbf{P}_{11}(t)),$$

where $p_{11}(t)$ has degree at most 1, and $\det_n(\mathbf{P}_{11}(t))$ has degree at most $n$. Hence

$$\deg\big(p_{11}(t) \det_n(\mathbf{P}_{11}(t))\big) \leq n+1,$$

and therefore $\deg(\det_n(\mathbf{P}(t))) \leq n+1$ since $\det_{n+1}(\mathbf{P}(t))$ is the sum of polynomials of degree at most $n+1$. Thus the lemma holds true in the $n+1$ case, and so it must hold for all $n \in \mathbb{N}$ by induction. ■

**Proposition 6.27.** *If* $\mathbf{A} \in \mathbb{F}^{n\times n}$, *then* $\deg(P_{\mathbf{A}}) = n$ *and the lead coefficient of* $P_{\mathbf{A}}$ *is* $(-1)^n$.

**Proof.** In the case when $n = 1$ we have $\mathbf{A} = [a]$, so that

$$P_{\mathbf{A}}(t) = \det_1([a] - [t]) = \det_1([a - t]) = a - t = -t + a,$$

and we clearly that $\deg(P_{\mathbf{A}}) = 1$ and the lead coefficient of $P_{\mathbf{A}}$ is $(-1)^1$.

Suppose the proposition is true for some $n \in \mathbb{N}$. Let $\mathbf{A} = [a_{ij}]_{n+1} \in \mathbb{F}^{(n+1)\times(n+1)}$, and define $\mathbf{P}(t) = \mathbf{A} - t\mathbf{I}_{n+1}$ so that $\mathbf{P}(t) = [p_{ij}(t)]_{n+1}$ with

$$\deg(p_{ij}) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

Now,

$$P_{\mathbf{A}}(t) = \det_{n+1}(\mathbf{P}(t)) = \sum_{k=1}^{n+1}(-1)^{1+k} p_{1k}(t) \det_n(\mathbf{P}_{1k}(t)),$$

where for each $k$ we have $\mathbf{P}_{1k}(t) = [p_{k,ij}(t)]_n$ such that

$$\deg(p_{k,ij}) \leq \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

and so $\deg(\det_n(\mathbf{P}_{1k}(t))) \leq n$ by Lemma 6.26. Since $p_{1k}(t)$ is a constant for $2 \leq k \leq n+1$, it follows that

$$\deg\big((-1)^{1+k} p_{1k}(t) \det_n(\mathbf{P}_{1k}(t))\big) \leq n$$

for $2 \leq k \leq n+1$. In the case when $k=1$ we have

$$(-1)^{1+k} p_{1k}(t) \det_n(\mathbf{P}_{1k}(t)) = p_{11}(t) \det_n(\mathbf{P}_{11}(t)),$$

where

$$\det_n(\mathbf{P}_{11}(t)) = \det_n(\mathbf{A}_{11} - t\mathbf{I}_n) = P_{\mathbf{A}_{11}}(t)$$

has degree $n$ and lead coefficient $(-1)^n$ by our inductive hypothesis. That is,

$$\det_n(\mathbf{P}_{11}(t)) = (-1)^n t^n + b_{n-1}t^{n-1} + \cdots + b_1 t + b_0$$

for some $b_{n-1}, \ldots, b_0 \in \mathbb{F}$, and since $p_{11}(t) = a_{11} - t$ we obtain

$$\begin{aligned} p_{11}(t) \det_n(\mathbf{P}_{11}(t)) &= (-t + a_{11})\big((-1)^n t^n + b_{n-1}t^{n-1} + \cdots + b_1 t + b_0\big) \\ &= (-1)^{n+1} t^{n+1} + c_n t^n + \cdots + c_1 t + c_0 \end{aligned}$$

for some $c_n, \ldots, c_0 \in \mathbb{F}$. Hence $Q(t) = p_{11}(t) \det_n(\mathbf{P}_{11}(t))$ has degree $n+1$ with lead coefficient $(-1)^{n+1}$. Since $P_{\mathbf{A}}(t) = \det_{n+1}(\mathbf{P}(t))$ is the sum of $Q(t)$ with other polynomials of degree at most $n$, it follows that $P_{\mathbf{A}}$ likewise has degree $n+1$ with lead coefficient $(-1)^{n+1}$.

We conclude by the principle of induction that the proposition holds for all $n \in \mathbb{N}$, which finishes the proof. ■

**Corollary 6.28.** *If $V$ is a nontrivial finite-dimensional vector space over $\mathbb{F}$ and $L \in \mathcal{L}(V)$, then* $\deg(P_L) = \dim(V)$ *and the lead coefficient of $P_L$ is $(-1)^{\dim(V)}$.*

**Proof.** Suppose $V$ is a nontrivial finite-dimensional vector space over $\mathbb{F}$ and $L \in \mathcal{L}(V)$. Let $\mathcal{B}$ be any basis for $V$. Since $[L]_{\mathcal{B}} \in \mathbb{F}^{\dim(V)\times\dim(V)}$, by Proposition 6.27 we have $\deg(P_{[L]_{\mathcal{B}}}) = \dim(V)$ and the lead coefficient of $P_{[L]_{\mathcal{B}}}$ is $(-1)^n$. Now, $P_L = P_{[L]_{\mathcal{B}}}$ by Definition 6.16, and so the proof is done. ■

**Proposition 6.29.** *Let $n \in \mathbb{N}$.*

1. *If $\mathbf{A} \in \mathbb{C}^{n\times n}$, then $1 \leq |\sigma(\mathbf{A})| \leq n$.*
2. *Let $V$ be an $n$-dimensional vector space over $\mathbb{C}$. If $L \in \mathcal{L}(V)$, then $1 \leq |\sigma(L)| \leq n$.*

**Proof.**
*Proof of Part (1):* Let $\mathbf{A} \in \mathbb{C}^{n\times n}$. By Proposition 6.27 the polynomial function $P_{\mathbf{A}}$ is of degree $n \in \mathbb{N}$, so by the Fundamental Theorem of Algebra $P_{\mathbf{A}}$ has at least one zero in $\mathbb{C}$, and by the Factor Theorem $P_{\mathbf{A}}$ has at most $n$ zeros in $\mathbb{C}$. Since, by Theorem 6.18, $\lambda$ is an eigenvalue of $\mathbf{A}$ if and only if $P_{\mathbf{A}}(\lambda) = 0$, it follows that $\mathbf{A}$ possesses at least one and at most $n$ distinct eigenvalues. That is, $1 \leq |\sigma(\mathbf{A})| \leq n$.

*Proof of Part (2):* Suppose $L \in \mathcal{L}(V)$, and let $\mathcal{B}$ be an ordered basis for $V$. Then $[L]_{\mathcal{B}} \in \mathbb{C}^{n\times n}$, and by Part (1) we have $1 \leq |\sigma([L]_{\mathcal{B}})| \leq n$. Now, because $\lambda$ is an eigenvalue of $L$ if and only if it is an eigenvalue of $[L]_{\mathcal{B}}$ by Proposition 6.14, we conclude that $1 \leq |\sigma(L)| \leq n$. ■

**Definition 6.30.** *If $\mathbf{A} \in \mathbb{F}^{n\times n}$, then the* ***algebraic multiplicity*** $\alpha_{\mathbf{A}}(\lambda)$ *of an eigenvalue* $\lambda \in \sigma(\mathbf{A})$ *is given by*

$$\alpha_{\mathbf{A}}(\lambda) = \max\{j : (t-\lambda)^j \text{ is a factor of } P_{\mathbf{A}}(t)\}. \tag{6.11}$$

*The* ***geometric multiplicity*** *of* $\lambda$ *is* $\gamma_{\mathbf{A}}(\lambda) = \dim(E_{\mathbf{A}}(\lambda))$.

*If* $L \in \mathcal{L}(V)$, *then the* ***algebraic multiplicity*** $\alpha_L(\lambda)$ *of an eigenvalue* $\lambda \in \sigma(L)$ *is given by*

$$\alpha_L(\lambda) = \alpha_{[L]}(\lambda),$$

*where* $[L]$ *denotes the matrix corresponding to* $L$ *with respect to any basis for* $V$. *The* ***geometric multiplicity*** *of* $\lambda$ *is* $\gamma_L(\lambda) = \dim(E_L(\lambda))$.

Proposition 6.15 ensures that the algebraic multiplicity of any eigenvalue $\lambda$ of an operator $L \in \mathcal{L}(V)$ is independent of the choice of basis for $V$. That is, $\alpha_L(\lambda)$ is invariant under change of bases.

It must be stressed that if a matrix $\mathbf{A}$ is regarded as being an element of $\mathbb{F}^{n\times n}$, then in general we consider only eigenvalues that are elements of $\mathbb{F}$. Thus, if $\mathbf{A} \in \mathbb{R}^{n\times n}$, then $\sigma(\mathbf{A}) \subseteq \mathbb{R}$, and we discount any value in $\mathbb{C} \setminus \mathbb{R}$ as being an eigenvalue. A similar convention is observed in the case when $L \in \mathcal{L}(V)$, where $V$ is given to be a vector space over the field $\mathbb{F}$; that is, we take $\sigma(L) \subseteq \mathbb{F}$.

An easy consequence of the Factor Theorem is that the multiplicities of the distinct complex zeros of an $n$th-degree polynomial function must sum to $n$. Thus, since the characteristic polynomial of a matrix $\mathbf{A} \in \mathbb{C}^{n\times n}$ has degree $n$ by Proposition 6.27, it readily follows from Theorem 6.18 that the sum of the algebraic multiplicities of the distinct complex eigenvalues $\lambda_1, \ldots, \lambda_m$ of $\mathbf{A}$ must be $n$:

$$\sum_{k=1}^{m} \alpha_{\mathbf{A}}(\lambda_k) = n. \tag{6.12}$$

It is in this sense (i.e. counting multiplicities) that it can be said that an $n \times n$ matrix $\mathbf{A}$ with complex-valued entries has "$n$ eigenvalues," which we may sometimes denote by $\lambda_1, \ldots, \lambda_n$. The same applies to any linear operator $L$ on an $n$-dimensional vector space over $\mathbb{C}$.

**Theorem 6.31.** *If* $\mathbf{A} \in \mathbb{C}^{n\times n}$ *has distinct complex eigenvalues* $\lambda_1, \ldots, \lambda_m$, *then*

$$\det_n(\mathbf{A}) = \prod_{k=1}^{m} \lambda_k^{\alpha_{\mathbf{A}}(\lambda_k)}$$

**Proof.** Suppose $\mathbf{A} \in \mathbb{C}^{n\times n}$ has distinct complex eigenvalues $\lambda_1, \ldots, \lambda_m$. Then $\lambda_1, \ldots, \lambda_m$ are precisely the zeros of $P_{\mathbf{A}}$ by Theorem 6.18, and so

$$P_{\mathbf{A}}(t) = (-1)^n (t-\lambda_1)^{\alpha_{\mathbf{A}}(\lambda_1)} \cdots (t-\lambda_m)^{\alpha_{\mathbf{A}}(\lambda_m)}$$

by the Factor Theorem and (6.11), along with Proposition 6.27 which tells us that the lead coefficient of $P_{\mathbf{A}}$ is $(-1)^n$. Now, since

$$\det_n(\mathbf{A}) = \det_n(\mathbf{A} - 0\mathbf{I}_n) = P_{\mathbf{A}}(0),$$

from (6.12) we obtain

$$\det_n(\mathbf{A}) = (-1)^n (-\lambda_1)^{\alpha_{\mathbf{A}}(\lambda_1)} \cdots (-\lambda_m)^{\alpha_{\mathbf{A}}(\lambda_m)}$$

$$= (-1)^n(-1)^{\alpha_{\mathbf{A}}(\lambda_1)+\cdots+\alpha_{\mathbf{A}}(\lambda_m)}\lambda_1^{\alpha_{\mathbf{A}}(\lambda_1)}\cdots\lambda_m^{\alpha_{\mathbf{A}}(\lambda_m)}$$
$$= (-1)^n(-1)^n\lambda_1^{\alpha_{\mathbf{A}}(\lambda_1)}\cdots\lambda_m^{\alpha_{\mathbf{A}}(\lambda_m)}$$
$$= \lambda_1^{\alpha_{\mathbf{A}}(\lambda_1)}\cdots\lambda_m^{\alpha_{\mathbf{A}}(\lambda_m)}$$

as desired. ■

**Proposition 6.32.** *Let $\mathbf{A} \in \mathbb{F}^{n\times n}$. If $\lambda$ is an eigenvalue of $\mathbf{A}$, then it is also an eigenvalue of $\mathbf{A}^\top$*

**Proof.** Suppose that $\lambda \in \mathbb{F}$ is an eigenvalue of $\mathbf{A}$. Then $P_{\mathbf{A}}(\lambda) = 0$ by Theorem 6.18, and thus

$$\det_n(\mathbf{A} - \lambda\mathbf{I}_n) = 0.$$

Now, by Theorem 5.7

$$\det_n\big((\mathbf{A} - \lambda\mathbf{I}_n)^\top\big) = \det_n(\mathbf{A} - \lambda\mathbf{I}_n),$$

and since

$$(\mathbf{A} - \lambda\mathbf{I}_n)^\top = \mathbf{A}^\top - \lambda\mathbf{I}_n^\top = \mathbf{A}^\top - \lambda\mathbf{I}_n,$$

it follows that

$$\det_n(\mathbf{A}^\top - \lambda\mathbf{I}_n) = 0.$$

That is, $P_{\mathbf{A}^\top}(\lambda) = 0$, and so by Theorem 6.18 we conclude that $\lambda$ is an eigenvalue of $\mathbf{A}^\top$. ■

## 6.4 – Similar Matrices

**Definition 6.33.** *Let* $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{n\times n}$. *We say* $\mathbf{A}$ *is* ***similar*** *to* $\mathbf{B}$, *written* $\mathbf{A} \overset{s}{\sim} \mathbf{B}$, *if there exists an invertible matrix* $\mathbf{Q} \in \mathbb{F}^{n\times n}$ *such that* $\mathbf{B} = \mathbf{QAQ}^{-1}$.

**Theorem 6.34.** *The similarity relation* $\overset{s}{\sim}$ *is an equivalence relation on the class of square matrices over* $\mathbb{F}$.

**Proof.** For any $\mathbf{A} \in \mathbb{F}^{n\times n}$ we have $\mathbf{A} = \mathbf{I}_n\mathbf{A}\mathbf{I}_n^{-1}$, so that $\mathbf{A} \overset{s}{\sim} \mathbf{A}$ and hence $\overset{s}{\sim}$ is reflexive.

Suppose that $\mathbf{A} \overset{s}{\sim} \mathbf{B}$. Then $\mathbf{B} = \mathbf{QAQ}^{-1}$ for some invertible matrix $\mathbf{Q}$, and since

$$\mathbf{B} = \mathbf{QAQ}^{-1} \quad\Rightarrow\quad \mathbf{A} = \mathbf{Q}^{-1}\mathbf{BQ} \quad\Rightarrow\quad \mathbf{A} = \mathbf{Q}^{-1}\mathbf{B}(\mathbf{Q}^{-1})^{-1},$$

it follows that $\mathbf{B} \overset{s}{\sim} \mathbf{A}$ and therefore $\overset{s}{\sim}$ is symmetric.

Suppose $\mathbf{A} \overset{s}{\sim} \mathbf{B}$ and $\mathbf{B} \overset{s}{\sim} \mathbf{C}$, so that

$$\mathbf{B} = \mathbf{QAQ}^{-1} \quad \text{and} \quad \mathbf{C} = \mathbf{PBP}^{-1}$$

for some invertible matrices $\mathbf{Q}$ and $\mathbf{P}$. Then by the associativity of matrix multiplication and Theorem 2.26 we obtain

$$\mathbf{C} = \mathbf{P}(\mathbf{QAQ}^{-1})\mathbf{P}^{-1} = (\mathbf{PQ})\mathbf{A}(\mathbf{Q}^{-1}\mathbf{P}^{-1}) = (\mathbf{PQ})\mathbf{A}(\mathbf{PQ})^{-1},$$

which shows that $\mathbf{A} \overset{s}{\sim} \mathbf{C}$ and therefore $\overset{s}{\sim}$ is transitive. ∎

**Remark.** Because the relation $\overset{s}{\sim}$ is symmetric, when two matrices $\mathbf{A}$ and $\mathbf{B}$ are said to be similar it does not matter whether we take that to mean $\mathbf{A} \overset{s}{\sim} \mathbf{B}$ (i.e. $\mathbf{B} = \mathbf{QAQ}^{-1}$) or $\mathbf{B} \overset{s}{\sim} \mathbf{A}$ (i.e. $\mathbf{A} = \mathbf{QBQ}^{-1}$).

**Proposition 6.35.** *Suppose that* $\mathbf{A}$ *and* $\mathbf{B}$ *are similar matrices.*

1. $\mathbf{A}$ *is invertible if and only if* $\mathbf{B}$ *is invertible.*
2. $\det(\mathbf{A}) = \det(\mathbf{B})$.
3. $P_{\mathbf{A}} = P_{\mathbf{B}}$.
4. $\sigma(\mathbf{A}) = \sigma(\mathbf{B})$.
5. $\operatorname{rank}(\mathbf{A}) = \operatorname{rank}(\mathbf{B})$.

**Proof.**
*Proof of Part (1):* If $\mathbf{A}$ is invertible, then there exists an invertible matrix $\mathbf{Q}$ such that $\mathbf{B} = \mathbf{QAQ}^{-1}$, and therefore $\mathbf{B}$ is invertible by Theorem 2.26. The converse follows from the symmetric property of $\overset{s}{\sim}$.

*Proof of Part (2):* There exists an invertible matrix $\mathbf{Q}$ such that $\mathbf{B} = \mathbf{QAQ}^{-1}$. Now,

$$\det(\mathbf{B}) = \det(\mathbf{QAQ}^{-1}) = \det(\mathbf{Q})\det(\mathbf{A})\det(\mathbf{Q}^{-1}) = \det(\mathbf{Q})\det(\mathbf{A})\frac{1}{\det(\mathbf{Q})} = \det(\mathbf{A})$$

by Theorems 5.23 and 5.24.

*Proof of Part (3):* There exists an invertible matrix $\mathbf{Q}$ such that $\mathbf{B} = \mathbf{QAQ}^{-1}$, and so

$$\begin{aligned} P_{\mathbf{B}}(t) &= \det(\mathbf{B} - t\mathbf{I}) = \det(\mathbf{QAQ}^{-1} - t\mathbf{QIQ}^{-1}) = \det\big(\mathbf{Q}(\mathbf{A} - t\mathbf{I})\mathbf{Q}^{-1}\big) \\ &= \det(\mathbf{Q})\det(\mathbf{A} - t\mathbf{I})\det(\mathbf{Q}^{-1}) = \det(\mathbf{Q})\det(\mathbf{A} - t\mathbf{I})\det(\mathbf{Q})^{-1} \\ &= \det(\mathbf{A} - t\mathbf{I}) = P_{\mathbf{A}}(t) \end{aligned}$$

for any $t \in \mathbb{F}$. Therefore $P_{\mathbf{A}} = P_{\mathbf{B}}$.

*Proof of Part (4):* Applying Theorem 6.18 and Part (3), we have

$$\lambda \in \sigma(\mathbf{A}) \quad \Leftrightarrow \quad P_{\mathbf{A}}(\lambda) = 0 \quad \Leftrightarrow \quad P_{\mathbf{B}}(\lambda) = 0 \quad \Leftrightarrow \quad \lambda \in \sigma(\mathbf{B}),$$

and therefore $\sigma(\mathbf{A}) = \sigma(\mathbf{B})$.

*Proof of Part (5):* This is an immediate consequence of Theorem 4.47(4). ■

The following proposition is a direct consequence of Corollary 4.33 and will prove useful later on.

**Proposition 6.36.** *Suppose $V$ is a finite-dimensional vector space and $L \in \mathcal{L}(V)$. If $\mathcal{B}$ and $\mathcal{B}'$ are ordered bases for $V$, then $[L]_{\mathcal{B}}$ and $[L]_{\mathcal{B}'}$ are similar matrices.*

**Proposition 6.37.** *Suppose that $V$ is a finite-dimensional vector space, $L \in \mathcal{L}(V)$, and $\mathbf{A} \in \mathbb{F}^{n\times n}$. If there is an ordered basis $\mathcal{B}$ for $V$ such that $[L]_{\mathcal{B}} \overset{s}{\sim} \mathbf{A}$, then there exists a basis $\mathcal{B}'$ such that $[L]_{\mathcal{B}'} = \mathbf{A}$.*

**Proof.** Suppose $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ is an ordered basis for $V$ such that $[L]_{\mathcal{B}} \overset{s}{\sim} \mathbf{A}$. Thus there exists an invertible matrix

$$\mathbf{Q} = [q_{ij}]_n = \begin{bmatrix} \mathbf{q}_1 & \cdots & \mathbf{q}_n \end{bmatrix}$$

such that $[L]_{\mathcal{B}} = \mathbf{QAQ}^{-1}$. Let $\mathcal{B}' = \{\mathbf{v}'_1, \dots, \mathbf{v}'_n\}$ be the set of vectors for which

$$\mathbf{v}'_k = q_{1k}\mathbf{v}_1 + \cdots + q_{nk}\mathbf{v}_n$$

for each $1 \le k \le n$, so that

$$[\mathbf{v}'_k]_{\mathcal{B}} = \begin{bmatrix} q_{1k} \\ \vdots \\ q_{nk} \end{bmatrix} = \mathbf{q}_k.$$

Since $\mathbf{Q}$ is invertible, by the Invertible Matrix Theorem the column vectors $\mathbf{q}_1, \dots, \mathbf{q}_n$ of $\mathbf{Q}$ are linearly independent, which is to say $[\mathbf{v}'_1]_{\mathcal{B}}, \dots, [\mathbf{v}'_n]_{\mathcal{B}}$ are linearly independent vectors in $\mathbb{F}^n$. Thus, since the mapping $\varphi_{\mathcal{B}}^{-1} : \mathbb{F}^n \to V$ (the inverse of the $\mathcal{B}$-coordinate map) is an isomorphism and

$$\varphi_{\mathcal{B}}^{-1}\big([\mathbf{v}'_k]_{\mathcal{B}}\big) = \mathbf{v}'_k$$

for $1 \le k \le n$, it follows by Proposition 4.16 that $\mathbf{v}'_1, \dots, \mathbf{v}'_n$ are linearly independent and therefore $\mathcal{B}'$ is a basis for $V$. We give it the natural order: $\mathcal{B}' = (\mathbf{v}'_1, \dots, \mathbf{v}'_n)$.

Now, by Theorem 4.27,

$$\mathbf{I}_{\mathcal{B}'\mathcal{B}} = \Big[[\mathbf{v}'_1]_{\mathcal{B}} \quad \cdots \quad [\mathbf{v}'_n]_{\mathcal{B}}\Big] = \big[\mathbf{q}_1 \quad \cdots \quad \mathbf{q}_n\big] = \mathbf{Q},$$

and so

$$[L]_{\mathcal{B}} = \mathbf{QAQ}^{-1} = \mathbf{I}_{\mathcal{B}'\mathcal{B}}\mathbf{A}\mathbf{I}_{\mathcal{B}'\mathcal{B}}^{-1} = \mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1}\mathbf{A}\mathbf{I}_{\mathcal{B}\mathcal{B}'}$$

by Proposition 4.31. Finally, by Corollary 4.33 we obtain

$$\mathbf{A} = \mathbf{I}_{\mathcal{B}\mathcal{B}'}[L]_{\mathcal{B}}\mathbf{I}_{\mathcal{B}\mathcal{B}'}^{-1} = [L]_{\mathcal{B}'}$$

as desired. ■

We will often have need to raise matrix expressions of the form $\mathbf{QAQ}^{-1}$ and $\mathbf{Q}^{-1}\mathbf{AQ}$ to an arbitrary positive integer power, for which the following proposition will prove invaluable.

**Proposition 6.38.** *If* $\mathbf{A}, \mathbf{Q} \in \mathbb{F}^{n\times n}$ *and* $\mathbf{Q}$ *is invertible, then*

$$(\mathbf{Q}^{-1}\mathbf{AQ})^k = \mathbf{Q}^{-1}\mathbf{A}^k\mathbf{Q} \tag{6.13}$$

*and*

$$(\mathbf{QAQ}^{-1})^k = \mathbf{QA}^k\mathbf{Q}^{-1} \tag{6.14}$$

*for all* $k \in \mathbb{N}$.

**Proof.** First we prove that (6.13) holds for all $k \geq 1$. Certainly the equation holds when $k = 1$. Suppose it holds for some arbitrary $k \geq 1$. Then, exploiting the associativity of matrix multiplication, we obtain

$$\begin{aligned}(\mathbf{Q}^{-1}\mathbf{AQ})^{k+1} &= (\mathbf{Q}^{-1}\mathbf{AQ})^k(\mathbf{Q}^{-1}\mathbf{AQ}) = (\mathbf{Q}^{-1}\mathbf{A}^k\mathbf{Q})(\mathbf{Q}^{-1}\mathbf{AQ})\\ &= \mathbf{Q}^{-1}\mathbf{A}^k(\mathbf{QQ}^{-1})\mathbf{AQ} = \mathbf{Q}^{-1}\mathbf{A}^k(\mathbf{I}_k)\mathbf{AQ} = \mathbf{Q}^{-1}\mathbf{A}^k\mathbf{AQ}\\ &= \mathbf{Q}^{-1}(\mathbf{A}^k\mathbf{A})\mathbf{Q} = \mathbf{Q}^{-1}\mathbf{A}^{k+1}\mathbf{Q},\end{aligned}$$

which shows the equation holds for $k + 1$. By the Principle of Induction we conclude that (6.13) holds for all $k \in \mathbb{N}$.

Equation (6.14) is a symmetrical result that is easily derived from (6.13) merely by replacing $\mathbf{Q}$ with $\mathbf{Q}^{-1}$. ■

## 6.5 – The Theory of Diagonalization

**Definition 6.39.** *Suppose $V$ is a nontrivial finite-dimensional vector space over $\mathbb{F}$, and let $L \in \mathcal{L}(V)$. An ordered basis for $V$ consisting of the eigenvectors of $L$ is called a* ***spectral basis*** *for $L$. We say $L$ is* ***diagonalizable*** *if there exists a spectral basis for $L$. Any procedure that finds a spectral basis for $L$ is called* ***diagonalization****.*

*A matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$ is* ***diagonalizable*** *in $\mathbb{F}$ if it is similar to a diagonal matrix $\mathbf{D} \in \mathbb{F}^{n\times n}$.*

**Theorem 6.40.** *Suppose $V$ is a finite-dimensional vector space over $\mathbb{F}$, $L \in \mathcal{L}(V)$, and $\lambda_1, \dots, \lambda_m$ are the distinct eigenvalues of $L$. Then the following statements are equivalent.*

1. *$L$ is diagonalizable.*
2. *There exists some ordered basis $\mathcal{B}$ for $V$ such that $[L]_{\mathcal{B}}$ is a diagonal matrix.*
3. *There exists some ordered basis $\mathcal{B}$ for $V$ such that $[L]_{\mathcal{B}}$ is diagonalizable in $\mathbb{F}$.*
4. *$V$ decomposes as*
$$V = E_L(\lambda_1) \oplus \cdots \oplus E_L(\lambda_m).$$
5. *The dimension of $V$ is*
$$\dim(V) = \dim(E_L(\lambda_1)) + \cdots + \dim(E_L(\lambda_m)).$$

**Proof.**
*(1) ⇒ (2):* Suppose $L$ is diagonalizable. Then there exists some ordered basis $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ consisting of eigenvectors of $L$, so that $L(\mathbf{v}_k) = \lambda_k \mathbf{v}_k$ for each $1 \le k \le n$. By Corollary 4.21 the matrix corresponding to $L$ with respect to $\mathcal{B}$ is

$$[L]_{\mathcal{B}} = \Big[ \big[L(\mathbf{v}_1)\big]_{\mathcal{B}} \ \cdots \ \big[L(\mathbf{v}_n)\big]_{\mathcal{B}} \Big] = \Big[ \big[\lambda_1\mathbf{v}_1\big]_{\mathcal{B}} \ \cdots \ \big[\lambda_n\mathbf{v}_n\big]_{\mathcal{B}} \Big]$$
$$= \Big[ \lambda_1\big[\mathbf{v}_1\big]_{\mathcal{B}} \ \cdots \ \lambda_n\big[\mathbf{v}_n\big]_{\mathcal{B}} \Big] = \left[ \lambda_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \ \cdots \ \lambda_n \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \right] = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix},$$

and so we see that $[L]_{\mathcal{B}}$ is a diagonal matrix as desired.

*(2) ⇒ (1):* Suppose there exists some ordered basis $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ such that $[L]_{\mathcal{B}} \in \mathbb{F}^{n\times n}$ is a diagonal matrix:

$$[L]_{\mathcal{B}} = \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix}.$$

Since $[\mathbf{v}_k]_{\mathcal{B}} = [\delta_{ik}]_{n\times 1}$ for each $1 \le k \le n$, we have

$$[L]_{\mathcal{B}}[\mathbf{v}_k]_{\mathcal{B}} = d_k[\mathbf{v}_k]_{\mathcal{B}},$$

and so $d_k$ is an eigenvalue of $[L]_{\mathcal{B}}$ with corresponding eigenvector $[\mathbf{v}_k]_{\mathcal{B}}$. By Proposition 6.14 we conclude that, for each $1 \le k \le n$, $d_k$ is an eigenvalue of $L$ with corresponding eigenvector $\mathbf{v}_k$, and therefore $\mathcal{B}$ is an ordered basis for $V$ consisting of eigenvectors of $L$.

*(2) ⇒ (3):* This is trivial since equal matrices are similar matrices.

*(3) ⇒ (2):* If there is an ordered basis $\mathcal{B}$ such that $[L]_{\mathcal{B}}$ is similar to a diagonal matrix $\mathbf{D}$, then by Proposition 6.37 there is an ordered basis $\mathcal{B}'$ such that $[L]_{\mathcal{B}'} = \mathbf{D}$.

*(1) ⇒ (4):* Suppose $L$ is diagonalizable, so there is an ordered basis $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ consisting of eigenvectors of $L$. We may take the order to be such that $\mathbf{v}_1, \dots, \mathbf{v}_m$ have the distinct eigenvalues $\lambda_1, \dots, \lambda_m$. Let $\lambda_{m+1}, \dots, \lambda_n$ be the eigenvalues corresponding to $\mathbf{v}_{m+1}, \dots, \mathbf{v}_n$. For any $\mathbf{u} \in V$ there exist $c_1, \dots, c_n \in \mathbb{F}$ such that $\mathbf{u} = c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n$, and so

$$L(\mathbf{u}) = \sum_{k=1}^{n} c_k L(\mathbf{v}_k) = \sum_{k=1}^{n} c_k \lambda_k \mathbf{v}_k. \tag{6.15}$$

Now,

$$E_L(\lambda_k) = \{\mathbf{v} \in V : L(\mathbf{v}) = \lambda_k \mathbf{v}\}$$

is the eigenspace of $L$ corresponding to $\lambda_k$, and since

$$\lambda_{m+1}, \dots, \lambda_n \in \{\lambda_1, \dots, \lambda_m\},$$

it is clear that we may recast (6.15) as

$$L(\mathbf{u}) = \sum_{k=1}^{m} c_k' \lambda_k \mathbf{v}_k'$$

by combining terms with matching eigenvalues. For each $1 \le k \le m$ we have

$$L(c_k'\mathbf{v}_k') = c_k' L(\mathbf{v}_k') = c_k' \lambda_k \mathbf{v}_k' = \lambda_k(c_k'\mathbf{v}_k'),$$

so that $c_k'\mathbf{v}_k' \in E_L(\lambda_k)$, and thus

$$\mathbf{u} = \sum_{k=1}^{n} c_k \mathbf{v}_k = \sum_{k=1}^{m} c_k' \mathbf{v}_k' \in \sum_{k=1}^{m} E_L(\lambda_k).$$

This establishes that $V = E_L(\lambda_1) + \cdots + E_L(\lambda_m)$.

Next, suppose that

$$\sum_{k=1}^{m} \mathbf{u}_k = \mathbf{u} \quad \text{and} \quad \sum_{k=1}^{m} \mathbf{u}_k' = \mathbf{u}$$

for $\mathbf{u}_k, \mathbf{u}_k' \in E_L(\lambda_k)$. Then

$$\sum_{k=1}^{m} (\mathbf{u}_k - \mathbf{u}_k') = \mathbf{0}, \tag{6.16}$$

where $\mathbf{u}_k - \mathbf{u}_k' \in E_L(\lambda_k)$ for each $1 \le k \le m$. Suppose that $\mathbf{u}_{k_j} - \mathbf{u}_{k_j}' \neq \mathbf{0}$ for some values

$$1 \le k_1 < k_2 < \cdots < k_\ell \le m,$$

with $\mathbf{u}_k - \mathbf{u}'_k = \mathbf{0}$ for all $k \notin \{k_1, \ldots, k_\ell\}$. Then (6.16) becomes

$$\sum_{j=1}^{\ell} (\mathbf{u}_{k_j} - \mathbf{u}'_{k_j}) = \mathbf{0}. \tag{6.17}$$

However, each $\mathbf{u}_{k_j} - \mathbf{u}'_{k_j}$ (being nonzero) is an eigenvalue of $L$ with corresponding eigenvalue $\lambda_{k_j}$, and since the eigenvalues $\lambda_{k_1}, \ldots, \lambda_{k_\ell}$ are distinct, it follows by Theorem 6.8 that the set

$$\{\mathbf{u}_{k_1} - \mathbf{u}'_{k_1}, \ldots, \mathbf{u}_{k_\ell} - \mathbf{u}'_{k_\ell}\}$$

is linearly independent. Now (6.17) forces us to conclude that $\mathbf{u}_{k_j} - \mathbf{u}'_{k_j} = \mathbf{0}$ for some $1 \leq j \leq \ell$, which is a contradiction. We must conclude that $\mathbf{u}_k - \mathbf{u}'_k = \mathbf{0}$ for all $1 \leq k \leq m$, or equivalently

$$\mathbf{u}_1 = \mathbf{u}'_1, \ldots \mathbf{u}_m = \mathbf{u}'_m.$$

Hence any $\mathbf{u} \in V$ has a unique representation $\mathbf{u}_1 + \cdots + \mathbf{u}_m$ such that each $\mathbf{u}_k$ is an element of $E_L(\lambda_k)$, and therefore $V = E_L(\lambda_1) \oplus \cdots \oplus E_L(\lambda_m)$.

*(4) ⇒ (5):* That

$$V = \bigoplus_{k=1}^{m} E_L(\lambda_k) \quad \Rightarrow \quad \dim(V) = \sum_{k=1}^{m} \dim(E_L(\lambda_k))$$

is an immediate consequence of Theorem 4.45.

*(5) ⇒ (1):* Suppose that

$$\dim(V) = \dim(E_L(\lambda_1)) + \cdots + \dim(E_L(\lambda_m)),$$

with $\dim(E_L(\lambda_i)) = n_i$ for each $1 \leq i \leq m$. Let

$$\mathcal{B}_i = \{\mathbf{v}_{i1}, \ldots, \mathbf{v}_{in_i}\}$$

be a basis for $E_L(\lambda_i)$. Suppose

$$\sum_{i=1}^{m} \sum_{j=1}^{n_i} a_{ij}\mathbf{v}_{ij} = \sum_{j=1}^{n_1} a_{1j}\mathbf{v}_{1j} + \cdots + \sum_{j=1}^{n_m} a_{mj}\mathbf{v}_{mj} = \mathbf{0}, \tag{6.18}$$

where

$$\mathbf{v}_i = \sum_{j=1}^{n_i} a_{ij}\mathbf{v}_{ij} \in E_L(\lambda_i)$$

and so

$$\mathbf{v}_1 + \cdots + \mathbf{v}_m = \mathbf{0}. \tag{6.19}$$

For each $1 \leq i \leq m$ the nonzero elements of $E_L(\lambda_i)$ are eigenvectors of $L$ with corresponding eigenvalue $\lambda_i$, and since $\lambda_1, \ldots, \lambda_m$ are distinct we conclude by Theorem 6.8 that if $\mathbf{v}_1, \ldots, \mathbf{v}_m \neq \mathbf{0}$, then $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent. However, (6.19) implies that $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are not linearly independent, and so at least one of the vectors must be the zero vector. In fact, if we suppose that

$$\mathbf{v}_{k_1}, \ldots, \mathbf{v}_{k_\ell} \in \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$$

are the nonzero vectors, then (6.19) becomes

$$\mathbf{v}_{k_1} + \cdots + \mathbf{v}_{k_\ell} = \mathbf{0}$$

and we are compelled to conclude—just as before—that at least one term on the left-hand side must be $\mathbf{0}$! Hence

$$\sum_{j=1}^{n_i} a_{ij}\mathbf{v}_{ij} = \mathbf{v}_i = \mathbf{0}$$

for all $1 \le i \le m$, and since $\mathbf{v}_{i1}, \ldots, \mathbf{v}_{in_i}$ are linearly independent it follows that

$$a_{i1} = 0, \ldots, a_{in_i} = 0$$

for all $1 \le i \le m$. It is now clear that (6.18) admits only the trivial solution, so that the set

$$\mathcal{B} = \bigcup_{i=1}^{m} \mathcal{B}_i$$

of eigenvectors of $L$ is linearly independent; and because

$$|\mathcal{B}| = \sum_{i=1}^{m} |\mathcal{B}_i| = \sum_{i=1}^{m} n_i = \sum_{i=1}^{m} \dim(E_L(\lambda_i)) = \dim(V)$$

(Proposition 6.7 ensures that $\mathcal{B}_i \cap \mathcal{B}_j = \varnothing$ for any $i \neq j$), Theorem 3.51(1) implies that $\mathcal{B}$ must in fact be a basis for $V$ consisting of eigenvectors of $L$. Assigning any order to $\mathcal{B}$ that we wish, we conclude that $L$ is diagonalizable. ■

From the details of the proof of Theorem 6.40 (specifically that the first statement implies the second statement) we immediately obtain the following result.

**Corollary 6.41.** *Suppose $V$ is a finite-dimensional vector space over $\mathbb{F}$. If $L \in \mathcal{L}(V)$ is diagonalizable, $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ is a spectral basis for $L$, and $\lambda_k$ is the eigenvalue corresponding to eigenvector $\mathbf{v}_k$, then $[L]_\mathcal{B} \in \mathbb{F}^{n\times n}$ is a diagonal matrix with $kk$-entry $\lambda_k$ for $1 \le k \le n$. That is, $[L]_\mathcal{B} = \operatorname{diag}[\lambda_1, \ldots, \lambda_n]$.*

**Definition 6.42.** *A polynomial function $p \in \mathcal{P}_n(\mathbb{F})$* ***splits over*** *$\mathbb{F}$ if there exist $c, a_1, \ldots, a_n \in \mathbb{F}$ such that*

$$p(t) = c\prod_{k=1}^{n}(t - a_k)$$

*for all $t \in \mathbb{F}$.*

**Proposition 6.43.** *Suppose $V$ is a finite-dimensional vector space over $\mathbb{F}$. If $L \in \mathcal{L}(V)$ is diagonalizable, then $P_L$ splits over $\mathbb{F}$.*

**Proof.** Suppose $L \in \mathcal{L}(V)$ is diagonalizable, with $\dim(V) = n$. Let $\mathcal{B}$ be a spectral basis for $L$, so that $[L]_\mathcal{B}$ is a diagonal matrix

$$[L]_\mathcal{B} = \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix}$$

for some $d_1, \ldots, d_n \in \mathbb{F}$ by Theorem 6.40. Now,

$$P_L(t) = P_{[L]_{\mathcal{B}}}(t) = \det_n([L]_{\mathcal{B}} - t\mathbf{I}_n) = \begin{vmatrix} d_1 - t & & 0 \\ & \ddots & \\ 0 & & d_n - t \end{vmatrix} = (-1)^n \prod_{k=1}^{n}(t - d_k),$$

and therefore $P_L$ splits over $\mathbb{F}$. ■

The first part of the following theorem tells us that the algebraic multiplicity of an eigenvalue of a diagonalizable linear operator on a finite-dimensional vector space is always equal to its geometric multiplicity.

The following theorem will, in the next section, show itself to be the workhorse that yields a practical method for diagonalizing linear operators and square matrices alike.

**Theorem 6.44.** *Suppose $V$ is a finite-dimensional vector space over $\mathbb{F}$, $L \in \mathcal{L}(V)$, and $\lambda_1, \ldots, \lambda_m$ are the distinct eigenvalues of $L$. Assuming that $P_L$ splits over $\mathbb{F}$, then:*

1. *$L$ is diagonalizable if and only if $\alpha_L(\lambda_k) = \gamma_L(\lambda_k)$ for all $1 \leq k \leq m$.*
2. *If $L$ is diagonalizable and $\mathcal{B}_k$ is a basis for $E_L(\lambda_k)$ for each $1 \leq k \leq m$, then $\bigcup_{k=1}^m \mathcal{B}_k$ is a spectral basis for $L$.*

**Proof.**
*Proof of Part (1).* Let $n = \dim(V)$. Suppose that

$$\max\{j : (t - \lambda_k)^j \text{ is a factor of } P_L(t)\} = \alpha_L(\lambda_k) = \gamma_L(\lambda_k) = \dim(E_L(\lambda_k))$$

for each $1 \leq k \leq m$. Then

$$P_L(t) = p(t) \prod_{k=1}^{m}(t - \lambda_k)^{\dim(E_L(\lambda_k))}$$

for some polynomial function $p$ for which $\lambda_1, \ldots, \lambda_m$ are not zeros. However, $P_L$ splits over $\mathbb{F}$ by hypothesis, and so $\deg(p)$ is either 0 or 1. If $\deg(p) = 1$, so that $p(t) = c(t - \lambda)$ for some $\lambda, c \in \mathbb{F}$, then $P_L(\lambda) = 0$ and we conclude that $\lambda \neq \lambda_1, \ldots, \lambda_m$ must be an eigenvalue of $L$. This is a contradiction since $\lambda_1, \ldots, \lambda_m$ represent all the distinct eigenvalues of $L$. Hence $\deg(p) = 0$, which is to say $p(t) = c$ for some $c \in \mathbb{F}$ and we have

$$P_L(t) = c \prod_{k=1}^{m}(t - \lambda_k)^{\dim(E_L(\lambda_k))}. \tag{6.20}$$

Now, since $\deg(P_L) = n$ by Corollary 6.28, it follows from (6.20) that

$$\sum_{k=1}^{m} \dim(E_L(\lambda_k)) = n = \dim(V),$$

and therefore $L$ is diagonalizable by Theorem 6.40.

Suppose that $L$ is diagonalizable, and let $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a spectral basis for $L$ such that $L(\mathbf{v}_k) = \lambda_k \mathbf{v}_k$ for each $1 \leq k \leq n$. By Corollary 6.41, $[L]_{\mathcal{B}} \in \mathbb{F}^{n \times n}$ is a diagonal matrix with $kk$-entry $\lambda_k$:

$$[L]_{\mathcal{B}} = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}.$$

Let $r_k = \alpha_L(\lambda_k)$ for each $1 \leq k \leq m$; that is,

$$r_k = \max\{i : (t - \lambda_k)^i \text{ is a factor of } P_L(t)\},$$

and so

$$\begin{aligned} P_L(t) = \det_n([L]_{\mathcal{B}} - t\mathbf{I}_n) &= \begin{vmatrix} \lambda_1 - t & & 0 \\ & \ddots & \\ 0 & & \lambda_n - t \end{vmatrix} \\ &= \prod_{k=1}^{n}(\lambda_k - t) = (-1)^n \prod_{k=1}^{n}(t - \lambda_k) = (-1)^n \prod_{k=1}^{m}(t - \lambda_k)^{r_k}. \end{aligned} \tag{6.21}$$

The last equality holds since $\lambda_k \in \{\lambda_1, \ldots, \lambda_m\}$ for all $1 \leq k \leq n$, so there can be no factor of $P_L(t)$ of the form $t - \lambda$ such that $\lambda \neq \lambda_1, \ldots, \lambda_m$. Corollary 6.28 and (6.21) now imply that

$$\dim(V) = \deg(P_L) = \sum_{k=1}^{m} r_k. \tag{6.22}$$

From (6.21) we also see that, for each $1 \leq k \leq m$, the scalar $\lambda_k$ must occur precisely $r_k$ times on the diagonal of $[L]_{\mathcal{B}}$; that is, for each $1 \leq k \leq m$ there exist

$$1 \leq i_1 < i_2 < \cdots < i_{r_k} \leq n$$

such that

$$\lambda_{i_1} = \lambda_{i_2} = \cdots = \lambda_{i_{r_k}} = \lambda_k,$$

and therefore

$$S = \{\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \ldots, \mathbf{v}_{i_{r_k}}\} \subseteq E_L(\lambda_k).$$

Now Theorem 3.56(2) implies that

$$\dim(E_L(\lambda_k)) \geq r_k \tag{6.23}$$

since $\operatorname{Span}(S)$ is a subspace of $E_L(\lambda_k)$ of dimension $r_k$.

Since $L$ is diagonalizable,

$$\dim(V) = \sum_{k=1}^{m} \dim(E_L(\lambda_k)) \tag{6.24}$$

by Theorem 6.40. If we suppose that $\dim(E_{\lambda_j}(L)) > r_j$ for some $1 \leq j \leq m$, then by equations (6.24), (6.23), and (6.22), in turn, we obtain

$$\dim(V) = \sum_{k=1}^{m} \dim(E_L(\lambda_k)) > \sum_{k=1}^{m} r_k = \dim(V),$$

which is an egregious contradiction. Hence $\dim(E_L(\lambda_k)) \leq r_k$ for all $1 \leq k \leq m$, which together with (6.23) leads to the conclusion that

$$\alpha_L(\lambda_k) = r_k = \dim(E_L(\lambda_k)) = \gamma_L(\lambda_k)$$

for all $1 \leq k \leq m$.

*Proof of Part (2).* Suppose that $L$ is diagonalizable and $\mathcal{B}_k$ is a basis for $E_L(\lambda_k)$ for each $1 \leq k \leq m$. Statement (5) of Theorem 6.40 is true, and in the proof that statement (5) implies statement (1) we immediately see that $\mathcal{B} = \bigcup_{k=1}^m \mathcal{B}_k$ is a basis for $V$ consisting of eigenvectors of $L$. That is, $\mathcal{B}$ is a spectral basis for $L$. ■

## 6.6 – Diagonalization Methods and Applications

In general, if a square matrix $\mathbf{A}$ is given to be in $\mathbb{F}^{n\times n}$, then to say $\mathbf{A}$ is "diagonalizable" means in particular "diagonalizable in $\mathbb{F}$."

**Theorem 6.45** (**Matrix Diagonalization Procedure**). *Let $\mathbf{A} \in \mathbb{F}^{n\times n}$ have distinct eigenvalues $\lambda_1, \ldots, \lambda_m$, with $\mathcal{B}_k$ a basis for $E_{\mathbf{A}}(\lambda_k)$ for each $1 \le k \le m$. If $P_{\mathbf{A}}$ splits over $\mathbb{F}$ and $\alpha_{\mathbf{A}}(\lambda_k) = \gamma_{\mathbf{A}}(\lambda_k)$ for each $k$, then $\mathbf{A}$ is diagonalizable in $\mathbb{F}$ with diagonal matrix $\mathbf{D} \in \mathbb{F}^{n\times n}$ given by*

$$\mathbf{D} = \mathbf{I}_{\mathcal{E}\mathcal{B}}\mathbf{A}\mathbf{I}_{\mathcal{E}\mathcal{B}}^{-1},$$

*where $\mathcal{E}$ is the standard basis for $\mathbb{F}^n$ and $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ is an ordered basis formed from the elements of $\bigcup_{k=1}^m \mathcal{B}_k$. Therefore*

$$\mathbf{A} = \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{bmatrix} \operatorname{diag}\big[\mu_1, \ldots, \mu_n\big] \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{bmatrix}^{-1}, \tag{6.25}$$

*where $\mu_k$ is an eigenvalue corresponding to $\mathbf{v}_k$ for each $1 \le k \le n$.*

**Proof.** Suppose $P_{\mathbf{A}}$ splits over $\mathbb{F}$, and $\alpha_{\mathbf{A}}(\lambda_k) = \gamma_{\mathbf{A}}(\lambda_k)$ for each $1 \le k \le m$. Define $L \in \mathcal{L}(\mathbb{F}^n)$ by $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$ in the standard basis $\mathcal{E}$, which is to say $[L]_{\mathcal{E}} = \mathbf{A}$. It is immediate that $\lambda_1, \ldots, \lambda_m$ are the distinct eigenvalues of $L$, and since $P_L = P_{\mathbf{A}}$ by Definition 6.16, it follows that $P_L$ splits over $\mathbb{F}$. By Definition 6.30 $\alpha_L(\lambda_k) = \alpha_{\mathbf{A}}(\lambda_k)$ for each $k$, and since $E_L(\lambda_k) = E_{\mathbf{A}}(\lambda_k)$,

$$\gamma_L(\lambda_k) = \dim(E_L(\lambda_k)) = \dim(E_{\mathbf{A}}(\lambda_k)) = \gamma_{\mathbf{A}}(\lambda_k).$$

Hence $\alpha_L(\lambda_k) = \gamma_L(\lambda_k)$ for all $1 \le k \le m$, and so $L$ is diagonalizable by Theorem 6.44(1). Since each $\mathcal{B}_k$ that is a basis for $E_{\mathbf{A}}(\lambda_k)$ is also a basis for $E_L(\lambda_k)$, by Theorem 6.44(2) the set

$$\mathcal{B} = \bigcup_{k=1}^m \mathcal{B}_k$$

is a spectral basis for $L$. We order the elements of $\mathcal{B}$, where $|\mathcal{B}| = n$ since $\mathcal{B}$ is a basis for $\mathbb{F}^n$, so that $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ is an ordered basis for $\mathbb{F}^n$. Then $\mathbf{D} = [L]_{\mathcal{B}}$ is a diagonal matrix by Corollary 6.41, and by Corollary 4.33

$$\mathbf{I}_{\mathcal{E}\mathcal{B}}\mathbf{A}\mathbf{I}_{\mathcal{E}\mathcal{B}}^{-1} = \mathbf{I}_{\mathcal{E}\mathcal{B}}[L]_{\mathcal{E}}\mathbf{I}_{\mathcal{E}\mathcal{B}}^{-1} = [L]_{\mathcal{B}} = \mathbf{D}$$

as desired.

To obtain (6.25), observe that if $\mu_k$ is the eigenvalue corresponding to eigenvector $\mathbf{v}_k$ for each $1 \le k \le n$, then

$$\mathbf{D} = [L]_{\mathcal{B}} = \operatorname{diag}\big[\mu_1, \ldots, \mu_n\big]$$

by Corollary 6.41, and so from $\mathbf{D} = \mathbf{I}_{\mathcal{E}\mathcal{B}}\mathbf{A}\mathbf{I}_{\mathcal{E}\mathcal{B}}^{-1}$ we having, recalling Proposition 4.31 and Theorem 4.27,

$$\begin{aligned}
\mathbf{A} = \mathbf{I}_{\mathcal{E}\mathcal{B}}^{-1}\mathbf{D}\mathbf{I}_{\mathcal{E}\mathcal{B}} &= \mathbf{I}_{\mathcal{B}\mathcal{E}} \operatorname{diag}\big[\mu_1, \ldots, \mu_n\big] \mathbf{I}_{\mathcal{B}\mathcal{E}}^{-1} \\
&= \Big[[\mathbf{v}_1]_{\mathcal{E}} \ \cdots \ [\mathbf{v}_n]_{\mathcal{E}}\Big] \operatorname{diag}\big[\mu_1, \ldots, \mu_n\big] \Big[[\mathbf{v}_1]_{\mathcal{E}} \ \cdots \ [\mathbf{v}_n]_{\mathcal{E}}\Big]^{-1} \\
&= \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{bmatrix} \operatorname{diag}\big[\mu_1, \ldots, \mu_n\big] \begin{bmatrix} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{bmatrix}^{-1},
\end{aligned}$$

where the last equality is due to the simple fact that each symbol $\mathbf{v}_k$ already represents the $\mathcal{E}$-coordinates of a vector in $\mathbb{F}^n$, so that $[\mathbf{v}_k]_{\mathcal{E}} = \mathbf{v}_k$. ∎

One particularly appealing feature of diagonal matrices is that, for any $n \in \mathbb{N}$, their $n$th powers are found simply by taking the $n$th powers of their entries.

**Proposition 6.46.** *If* $\mathbf{D} = [d_{ij}]_n$ *is a diagonal matrix, then* $\mathbf{D}^k = [d_{ij}^k]_n$ *for all* $k \in \mathbb{N}$.

**Proof.** The statement of the proposition is certainly true in the case when $k = 1$. Suppose it is true for some arbitrary $k \in \mathbb{N}$, so that $\mathbf{D}^k = [d_{ij}^k]_n$. Since $\mathbf{D}$ is diagonal we have $d_{ij} = 0$ whenever $i \neq j$. Fix $1 \leq i, j \leq n$. By Definition 2.4,

$$\left[\mathbf{D}^{k+1}\right]_{ij} = \left[\mathbf{D}^k\mathbf{D}\right]_{ij} = \sum_{\ell=1}^{n} d_{i\ell}^k d_{\ell j} = 0 = d_{ij}^{k+1}$$

if $i \neq j$, and

$$\left[\mathbf{D}^{k+1}\right]_{ij} = \left[\mathbf{D}^k\mathbf{D}\right]_{jj} = \sum_{\ell=1}^{n} d_{j\ell}^k d_{\ell j} = d_{jj}^k d_{jj} = d_{jj}^{k+1}$$

if $i = j$. In either case we see that the $ij$-entry of $\mathbf{D}^{k+1}$ is $d_{ij}^{k+1}$, and so $\mathbf{D}^{k+1} = [d_{ij}^{k+1}]_n$.

Therefore the statement of the proposition holds for all $k \in \mathbb{N}$ by the Principle of Induction and the proof is done. ∎

**Example 6.47.** Determine whether

$$\mathbf{A} = \begin{bmatrix} -1 & 4 & -2 \\ -3 & 4 & 0 \\ -3 & 1 & 3 \end{bmatrix}$$

is diagonalizable in $\mathbb{R}$. If it is, then find an invertible matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$.

**Solution.** In Example 6.20 we found that the characteristic polynomial $P_{\mathbf{A}}$ splits over $\mathbb{R}$ by direct factorization:

$$P_{\mathbf{A}}(t) = -t^3 + 6t^2 - 11t + 6 = -(t-1)(t-2)(t-3).$$

In this way we determined that the eigenvalues of $\mathbf{A}$ are 1, 2, and 3, and by inspection we see that

$$\alpha_{\mathbf{A}}(1) = \alpha_{\mathbf{A}}(2) = \alpha_{\mathbf{A}}(3) = 1.$$

We also determined a basis for the eigenspace corresponding to each eigenvalue: for eigenspaces $E_{\mathbf{A}}(1)$, $E_{\mathbf{A}}(2)$, and $E_{\mathbf{A}}(3)$ we found bases

$$\mathcal{B}_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}, \quad \mathcal{B}_2 = \left\{ \begin{bmatrix} 2 \\ 3 \\ 3 \end{bmatrix} \right\}, \quad \text{and} \quad \mathcal{B}_3 = \left\{ \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \right\},$$

respectively. Since $|\mathcal{B}_1| = |\mathcal{B}_2| = |\mathcal{B}_3| = 1$, we see that

$$\gamma_{\mathbf{A}}(1) = \gamma_{\mathbf{A}}(2) = \gamma_{\mathbf{A}}(3) = 1.$$

Hence $\alpha_{\mathbf{A}}(\lambda) = \gamma_{\mathbf{A}}(\lambda)$ for every eigenvalue $\lambda$ of $\mathbf{A}$. Therefore $\mathbf{A}$ is diagonalizable in $\mathbb{R}$ by Theorem 6.45.

Letting

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 2 \\ 3 \\ 3 \end{bmatrix}, \quad \text{and} \quad \mathbf{v}_3 = \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix},$$

then $\mathcal{B} = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ is an ordered set formed from the elements of $\mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$ which Theorem 6.45 implies is an ordered basis for $\mathbb{R}^3$. Now, since eigenvalues 1, 2, and 3 correspond to eigenvectors $\mathbf{v}_1$, $\mathbf{v}_2$, and $\mathbf{v}_3$, respectively, by (6.25) we easily find that

$$\mathbf{A} = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{v}_3 \end{bmatrix} \operatorname{diag}[1, 2, 3] \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{v}_3 \end{bmatrix}^{-1}.$$

Thus if we let

$$\mathbf{P} = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{v}_3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 3 & 3 \\ 1 & 3 & 4 \end{bmatrix} \quad \text{and} \quad \mathbf{D} = \operatorname{diag}[1, 2, 3] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix},$$

then we have $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$ as desired. ■

In Example 6.47 there are other possible solutions. If we had chosen the ordered basis $(\mathbf{v}_3, \mathbf{v}_2, \mathbf{v}_1)$ instead of $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$, then we would have

$$\mathbf{A} = \begin{bmatrix} \mathbf{v}_3 & \mathbf{v}_2 & \mathbf{v}_1 \end{bmatrix} \operatorname{diag}[3, 2, 1] \begin{bmatrix} \mathbf{v}_3 & \mathbf{v}_2 & \mathbf{v}_1 \end{bmatrix}^{-1},$$

which is to say $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$ for

$$\mathbf{P} = \begin{bmatrix} 1 & 2 & 1 \\ 3 & 3 & 1 \\ 4 & 3 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{D} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

One great use for diagonalization is that it makes it possible to calculate high powers of square matrices with relative ease, as illustrated in the following example.

**Example 6.48.** Given

$$\mathbf{A} = \begin{bmatrix} -1 & 4 & -2 \\ -3 & 4 & 0 \\ -3 & 1 & 3 \end{bmatrix},$$

Find a formula for $\mathbf{A}^n$, and use it to calculate $\mathbf{A}^{10}$.

**Solution.** From Example 6.47 we have $\mathbf{A} = \mathbf{P}\mathbf{D}\mathbf{P}^{-1}$, with

$$\mathbf{P} = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 3 & 3 \\ 1 & 3 & 4 \end{bmatrix}, \quad \mathbf{D} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}, \quad \mathbf{P}^{-1} = \begin{bmatrix} 3 & -5 & 3 \\ -1 & 3 & -2 \\ 0 & -1 & 1 \end{bmatrix},$$

and so by Propositions 6.38 and 6.46, respectively,

$$\mathbf{A}^n = (\mathbf{P}\mathbf{D}\mathbf{P}^{-1})^n = \mathbf{P}\mathbf{D}^n\mathbf{P}^{-1} = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 3 & 3 \\ 1 & 3 & 4 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2^n & 0 \\ 0 & 0 & 3^n \end{bmatrix} \begin{bmatrix} 3 & -5 & 3 \\ -1 & 3 & -2 \\ 0 & -1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 3-2^{n+1} & -5+3\cdot 2^{n+1}-3^n & 3-2^{n+2}+3^n \\ 3-3\cdot 2^n & -5+9\cdot 2^n-3^{n+1} & 3-3\cdot 2^{n+1}+3^{n+1} \\ 3-3\cdot 2^n & -5+9\cdot 2^n-4\cdot 3^n & 3-3\cdot 2^{n+1}+4\cdot 3^n \end{bmatrix}.$$

Therefore

$$\mathbf{A}^{10} = \begin{bmatrix} 3-2^{11} & -5+3\cdot 2^{11}-3^{10} & 3-2^{12}+3^{10} \\ 3-3\cdot 2^{10} & -5+9\cdot 2^{10}-3^{11} & 3-3\cdot 2^{11}+3^{11} \\ 3-3\cdot 2^{10} & -5+9\cdot 2^{10}-4\cdot 3^{10} & 3-3\cdot 2^{11}+4\cdot 3^{10} \end{bmatrix}$$

$$= \begin{bmatrix} -2045 & -52,910 & 54,956 \\ -3069 & -167,936 & 171,006 \\ -3069 & -226,985 & 230,055 \end{bmatrix},$$

a result far more easily obtained than calculating $\mathbf{A}^{10}$ directly! ■

**Example 6.49.** Determine whether the linear operator $L \in \mathcal{L}(\mathbb{R}^{2\times 2})$ given by $L(\mathbf{A}) = \mathbf{A}^\top$ is diagonalizable. If it is, then find a spectral basis for $L$, and find the matrix corresponding to $L$ with respect to the spectral basis.

**Solution.** In Example 4.23 we found that the matrix corresponding to $L$ with respect to the standard basis $\mathcal{E} = (\mathbf{E}_{11}, \mathbf{E}_{12}, \mathbf{E}_{21}, \mathbf{E}_{22})$ is

$$[L]_{\mathcal{E}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The characteristic polynomial of $L$ is thus

$$P_L(t) = P_{[L]_{\mathcal{E}}}(t) = \det_4\left([L]_{\mathcal{E}} - t\mathbf{I}_4\right) = \begin{vmatrix} 1-t & 0 & 0 & 0 \\ 0 & -t & 1 & 0 \\ 0 & 1 & -t & 0 \\ 0 & 0 & 0 & 1-t \end{vmatrix} = (t-1)^3(t+1),$$

which makes clear that $P_L$ splits over $\mathbb{R}$, and the eigenvalues of $L$ are $\pm 1$ with $\alpha_L(-1) = 1$ and $\alpha_L(1) = 3$.

Next we find bases for the eigenspaces of $L$. For the eigenvalue 1 we have

$$E_L(1) = \left\{\mathbf{X} \in \mathbb{R}^{2\times 2} : L(\mathbf{X}) = \mathbf{X}\right\},$$

where

$$\mathbf{X} = L(\mathbf{X}) \;\Leftrightarrow\; \mathbf{X} = \mathbf{X}^\top \;\Leftrightarrow\; \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} x & z \\ y & w \end{bmatrix}$$

for $x, y, z, w \in \mathbb{R}$, implying that $y = z$ and thus

$$E_L(1) = \left\{\begin{bmatrix} x & y \\ z & w \end{bmatrix} \in \mathbb{R}^{2\times 2} \,:\, y = z\right\} = \left\{\begin{bmatrix} x & y \\ y & w \end{bmatrix} \,:\, x, y, w \in \mathbb{R}\right\}.$$

Letting $x = s_1$, $y = s_2$, and $w = s_3$, we finally obtain

$$E_L(1) = \left\{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} s_1 + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} s_2 + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} s_3 \,:\, s_1, s_2, s_3 \in \mathbb{R}\right\},$$

which shows that $E_L(1)$ has basis

$$\mathcal{B}_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\} = \{\mathbf{E}_{11},\, \mathbf{E}_{12} + \mathbf{E}_{21},\, \mathbf{E}_{22}\}$$

and therefore $\gamma_L(1) = 3$.

For the eigenvalue $-1$,

$$E_L(-1) = \left\{ \mathbf{X} \in \mathbb{R}^{2\times 2} \,:\, L(\mathbf{X}) = -\mathbf{X} \right\},$$

where

$$-\mathbf{X} = L(\mathbf{X}) \quad \Leftrightarrow \quad -\mathbf{X} = \mathbf{X}^\top \quad \Leftrightarrow \quad \begin{bmatrix} -x & -y \\ -z & -w \end{bmatrix} = \begin{bmatrix} x & z \\ y & w \end{bmatrix}$$

for $x, y, z, w \in \mathbb{R}$, implying that $x = -x$, $z = -y$, $-z = y$, and $w = -w$. Thus $x = w = 0$, and $z = -y$, so that

$$E_L(-1) = \left\{ \begin{bmatrix} 0 & y \\ -y & 0 \end{bmatrix} : y \in \mathbb{R} \right\}.$$

Letting $y = s$, we obtain

$$E_L(-1) = \left\{ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} s \,:\, s \in \mathbb{R} \right\},$$

which shows that $E_L(-1)$ has basis

$$\mathcal{B}_2 = \left\{ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\} = \{\mathbf{E}_{12} - \mathbf{E}_{21}\},$$

and therefore $\gamma_L(-1) = 1$.

By Theorem 6.44(1), since $P_L$ splits over $\mathbb{R}$, $\alpha_L(1) = \gamma_L(1)$, and $\alpha_L(-1) = \gamma_L(-1)$, the operator $L$ is diagonalizable. By Theorem 6.44(2) the ordered set

$$\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4) = (\mathbf{E}_{11},\, \mathbf{E}_{12} + \mathbf{E}_{21},\, \mathbf{E}_{22}, \mathbf{E}_{12} - \mathbf{E}_{21})$$

is a spectral basis for $L$. By Corollary 6.41 the $\mathcal{B}$-matrix of $L$ is a diagonal matrix with $kk$-entry the eigenvalue corresponding to the $k$th vector $\mathbf{v}_k$ in $\mathcal{B}$. Since $\mathbf{v}_1 = \mathbf{E}_{11}$, $\mathbf{v}_2 = \mathbf{E}_{12} + \mathbf{E}_{21}$, and $\mathbf{v}_3 = \mathbf{E}_{22}$ are eigenvectors corresponding to 1, and $\mathbf{v}_4 = \mathbf{E}_{12} - \mathbf{E}_{21}$ is an eigenvector corresponding to $-1$, we have

$$[L]_{\mathcal{B}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

It is in this sense that $L$ is "diagonalized" by finding a spectral basis. ■

### Problems

1. The matrix
$$\mathbf{A} = \begin{bmatrix} 3 & 2 \\ 2 & 3 \end{bmatrix}$$
is diagonalizable.
   (a) Find the characteristic polynomial of $\mathbf{A}$, and use it to find the eigenvalues of $\mathbf{A}$.
   (b) For each eigenvalue of $\mathbf{A}$ find the basis for the corresponding eigenspace.
   (c) Find an invertible matrix $\mathbf{P}$ and a diagonal matrix $\mathbf{D}$ such that $\mathbf{A} = \mathbf{PDP}^{-1}$.
   (d) Find $\mathbf{A}^{50}$ and $\mathbf{A}^{1/2}$.

2. Determine whether the matrix
$$\mathbf{A} = \begin{bmatrix} 7 & -15 \\ 2 & -4 \end{bmatrix}$$
is diagonalizable in $\mathbb{R}$. If it is, then find an invertible matrix $\mathbf{P}$ and diagonal matrix $\mathbf{D}$ such that $\mathbf{A} = \mathbf{PDP}^{-1}$.

3. Determine whether the matrix
$$\mathbf{A} = \begin{bmatrix} 4 & 0 & 4 \\ 0 & 4 & 4 \\ 4 & 4 & 8 \end{bmatrix}$$
is diagonalizable in $\mathbb{R}$. If it is, then find an invertible matrix $\mathbf{P}$ and diagonal matrix $\mathbf{D}$ such that $\mathbf{A} = \mathbf{PDP}^{-1}$.

4. Determine whether the matrix
$$\mathbf{A} = \begin{bmatrix} 2 & 0 & -2 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$
is diagonalizable in $\mathbb{R}$. If it is, then find an invertible matrix $\mathbf{P}$ and diagonal matrix $\mathbf{D}$ such that $\mathbf{A} = \mathbf{PDP}^{-1}$.

## 6.7 – Matrix Limits and Markov Chains

## 6.8 – The Cayley-Hamilton Theorem

**Proposition 6.50.** *Let $V$ be a finite-dimensional vector space over $\mathbb{F}$ with subspace $W$. If $W$ is invariant under $L \in \mathcal{L}(V)$, then the characteristic polynomial of $L|_W$ divides the characteristic polynomial of $L$.*

**Proof.** Let $\mathcal{C} = \{\mathbf{v}_1, \dots, \mathbf{v}_m\}$ be a basis for $W$. By Theorem 3.55 we can extend $\mathcal{C}$ to a basis

$$\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{v}_{m+1}, \dots, \mathbf{v}_n\}$$

for $V$. Since $W$ is $L$-invariant, for each $\mathbf{v}_j$ with $1 \le j \le m$ we have $L(\mathbf{v}_j) \in W$, and so there exist $a_{1j}, \dots, a_{mj} \in \mathbb{F}$ such that

$$L(\mathbf{v}_j) = \sum_{i=1}^{m} a_{ij}\mathbf{v}_i.$$

For $m + 1 \le j \le n$ we have

$$L(\mathbf{v}_j) = \sum_{i=1}^{n} a_{ij}\mathbf{v}_i.$$

Defining

$$\mathbf{A} = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} a_{1(m+1)} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m(m+1)} & \cdots & a_{mn} \end{bmatrix}, \quad \mathbf{C} = \begin{bmatrix} a_{(m+1)(m+1)} & \cdots & a_{(m+1)n} \\ \vdots & \ddots & \vdots \\ a_{n(m+1)} & \cdots & a_{nn} \end{bmatrix},$$

by Corollary 4.21 the $\mathcal{B}$-matrix for $L$ is

$$[L]_{\mathcal{B}} = \Big[ \big[L(\mathbf{v}_1)\big]_{\mathcal{B}} \ \cdots \ \big[L(\mathbf{v}_n)\big]_{\mathcal{B}} \Big] = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{O} & \mathbf{C} \end{bmatrix}$$

and the $\mathcal{C}$-matrix for $L|_W$ is

$$[L|_W]_{\mathcal{C}} = \Big[ \big[L|_W(\mathbf{v}_1)\big]_{\mathcal{C}} \ \cdots \ \big[L|_W(\mathbf{v}_m)\big]_{\mathcal{C}} \Big] = \Big[ \big[L(\mathbf{v}_1)\big]_{\mathcal{C}} \ \cdots \ \big[L(\mathbf{v}_m)\big]_{\mathcal{C}} \Big] = \mathbf{A}.$$

Now by Example 5.21,

$$\begin{aligned} P_L(t) &= \det_n\big([L]_{\mathcal{B}} - t\mathbf{I}_n\big) = \det_n\left(\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{O} & \mathbf{C} \end{bmatrix} - \begin{bmatrix} t\mathbf{I}_m & \mathbf{O} \\ \mathbf{O} & t\mathbf{I}_{n-m} \end{bmatrix}\right) \\ &= \det_n\left(\begin{bmatrix} \mathbf{A} - t\mathbf{I}_m & \mathbf{B} \\ \mathbf{O} & \mathbf{C} - t\mathbf{I}_{n-m} \end{bmatrix}\right) = \det_m(\mathbf{A} - t\mathbf{I}_m)\det_{n-m}(\mathbf{C} - t\mathbf{I}_{n-m}) \\ &= \det_m\big([L|_W]_{\mathcal{C}} - t\mathbf{I}_m\big)\det_{n-m}(\mathbf{C} - t\mathbf{I}_{n-m}) = P_{L|_W}(t)\det_{n-m}(\mathbf{C} - t\mathbf{I}_{n-m}), \end{aligned}$$

and since $\det_{n-m}(\mathbf{C} - t\mathbf{I}_{n-m})$ is a polynomial we conclude that $P_{L|_W}(t)$ divides $P_L(t)$. ■

**Definition 6.51.** *Suppose $V$ is a vector space, and $\mathbf{v} \in V$ such that $\mathbf{v} \neq \mathbf{0}$. The **$L$-cyclic subspace of $V$ generated by** $L$ is the subspace*

$$\text{Span}\{L^k(\mathbf{v}) : k \ge 0\}.$$

As usual we take it as understood that $L^0 = I_V$, the identity operator on $V$, so that $L^0(\mathbf{v}) = I_V(\mathbf{v}) = \mathbf{v}$.

**Proposition 6.52.** *Suppose $V$ is a finite-dimensional vector space, $\mathbf{v} \in V$ is a nonzero vector, $L \in \mathcal{L}(V)$, and $W$ is the $L$-cyclic subspace of $V$ generated by $\mathbf{v}$. If $\dim(W) = m$, then the following hold.*

1. *The set $\{\mathbf{v}, L(\mathbf{v}), \dots, L^{m-1}(\mathbf{v})\}$ is a basis for $W$.*
2. *If $a_0, \dots, a_{m-1} \in \mathbb{F}$ are such that*

$$\sum_{k=0}^{m-1} a_k L^k(\mathbf{v}) + L^m(\mathbf{v}) = \mathbf{0},$$

*then*

$$P_{L|_W}(t) = (-1)^m \left( \sum_{k=0}^{m-1} a_k t^k + t^m \right).$$

**Proof.**

*Proof of Part (1).* Since $\mathbf{v} \neq \mathbf{0}$ the set $S_0 = \{\mathbf{v}\}$ is linearly independent. For each $k \geq 0$ let

$$S_k = \{\mathbf{v}, L(\mathbf{v}), \dots, L^k(\mathbf{v})\},$$

and define

$$n = \max\{k : S_k \text{ is a linearly independent set}\}.$$

Then $S_n$ is a linearly independent set and $S_{n+1} = S_n \cup \{L^{n+1}(\mathbf{v})\}$ is linearly dependent, and by Proposition 3.39 it follows that $L^{n+1}(\mathbf{v}) \in \mathrm{Span}(S_n)$.

Fix $j \geq 1$ and suppose $L^{n+j}(\mathbf{v}) \in \mathrm{Span}(S_n)$, so that there exist $a_0, \dots, a_n \in \mathbb{F}$ such that

$$L^{n+j}(\mathbf{v}) = \sum_{k=0}^{n} a_k L^k(\mathbf{v}).$$

Now,

$$\begin{aligned} L^{n+j+1}(\mathbf{v}) = L(L^{n+j}(\mathbf{v})) = L\left( \sum_{k=0}^{n} a_k L^k(\mathbf{v}) \right) &= \sum_{k=0}^{n} a_k L^{k+1}(\mathbf{v}) \\ &= a_0 L(\mathbf{v}) + a_1 L^2(\mathbf{v}) + \cdots + a_{n-1} L^n(\mathbf{v}) + a_n L^{n+1}(\mathbf{v}), \end{aligned}$$

and since $a_{k-1} L^k(\mathbf{v}) \in \mathrm{Span}(S_n)$ for all $1 \leq k \leq n+1$, we conclude that $L^{n+j+1}(\mathbf{v}) \in \mathrm{Span}(S)$ as well. Therefore $L^k(\mathbf{v}) \in \mathrm{Span}(S_n)$ for all $k \geq 0$ by the principle of induction.

It is clear that

$$\mathrm{Span}(S_n) \subseteq W = \mathrm{Span}\{L^k(\mathbf{v}) : k \geq 0\}.$$

Fix $\mathbf{w} \in W$. Then there exist

$$a_0, \dots, a_r \in \mathbb{F} \quad \text{and} \quad 0 \leq k_0 < k_1 < \cdots < k_r$$

such that

$$\mathbf{w} = \sum_{j=0}^{r} a_j L^{k_j}(\mathbf{v})$$

for some $r \in \mathbb{W}$, and since $a_j L^{k_j}(\mathbf{v}) \in \mathrm{Span}(S_n)$ for each $j$, we have $\mathbf{w} \in \mathrm{Span}(S_n)$ also, and thus $W \subseteq \mathrm{Span}(S_n)$. It is now established that $\mathrm{Span}(S_n) = W$, and since $S_n$ is a linearly independent set, it follows that $S_n$ is a basis for $W$ and hence $|S_n| = \dim(W) = m$. Therefore

$$S_n = \{\mathbf{v}, L(\mathbf{v}), \ldots, L^n(\mathbf{v})\} = \{\mathbf{v}, L(\mathbf{v}), \ldots, L^{m-1}(\mathbf{v})\},$$

as was to be shown.

*Proof of Part (2)* Suppose $a_0, \ldots, a_{m-1} \in \mathbb{F}$ are such that

$$L^m(\mathbf{v}) = -a_0\mathbf{v} - a_1 L(\mathbf{v}) - \cdots - a_{m-1}L^{m-1}(\mathbf{v}).$$

By Part (1) the ordered set $\mathcal{C} = \{\mathbf{v}, L(\mathbf{v}), \ldots, L^{m-1}(\mathbf{v})\}$ is a basis for $W$, and so

$$\begin{aligned}
[L|_W]_{\mathcal{C}} &= \Big[\big[L|_W(\mathbf{v})\big]_{\mathcal{C}} \ \big[L|_W(L(\mathbf{v}))\big]_{\mathcal{C}} \ \cdots \ \big[L|_W(L^{m-1}(\mathbf{v}))\big]_{\mathcal{C}}\Big] \\
&= \Big[\big[L(\mathbf{v})\big]_{\mathcal{C}} \ \big[L^2(\mathbf{v})\big]_{\mathcal{C}} \ \cdots \ \big[L^{m-1}(\mathbf{v})\big]_{\mathcal{C}} \ \big[L^m(\mathbf{v})\big]_{\mathcal{C}}\Big] \\
&= \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{m-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{m-1} \end{bmatrix}.
\end{aligned}$$

It follows by Example 6.22 that the characteristic polynomial of $[L|_W]_{\mathcal{C}}$ is

$$(-1)^m(a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} + t^m),$$

and therefore

$$P_{L|_W}(t) = (-1)^m\left(\sum_{k=0}^{m-1} a_k t^k + t^m\right)$$

by Definition 6.16. ■

**Definition 6.53.** *Let $f \in \mathcal{P}_n(\mathbb{F})$ be a polynomial function $\mathbb{F} \to \mathbb{F}$ given by*

$$f(t) = \sum_{k=0}^{n} a_k t^k.$$

*If $V$ is a vector space over $\mathbb{F}$, $L \in \mathcal{L}(V)$, and $\mathbf{A} \in \mathbb{F}^{n\times n}$, we define the mapping $f(L)$ and matrix $f(\mathbf{A})$ by*

$$f(L) = \sum_{k=0}^{n} a_k L^k \quad \text{and} \quad f(\mathbf{A}) = \sum_{k=0}^{n} a_k \mathbf{A}^k.$$

Some needed basic properties of mappings of the form $f(L)$ and matrices of the form $f(\mathbf{A})$ which are routine to verify are the following.

**Proposition 6.54.** *Suppose that $V$ is a vector space over $\mathbb{F}$, $L \in \mathcal{L}(V)$, $\mathbf{A} \in \mathbb{F}^{n\times n}$, and $f, g, h \in \mathcal{P}(\mathbb{F})$. Then*

1. $f(L) \in \mathcal{L}(V)$ *and* $f(\mathbf{A}) \in \mathbb{F}^{n\times n}$.
2. $f(L) \circ g(L) = g(L) \circ f(L)$ *and* $f(\mathbf{A})g(\mathbf{A}) = g(\mathbf{A})f(\mathbf{A})$.
3. *If* $h(t) = f(t)g(t)$*, then* $h(L) = f(L) \circ g(L)$ *and* $h(\mathbf{A}) = f(\mathbf{A})g(\mathbf{A})$.

**Theorem 6.55 (Cayley-Hamilton Theorem).** *Let $V$ be a finite-dimensional vector space. If $L \in \mathcal{L}(V)$, then $P_L(L) = O_V$.*

**Proof.** Suppose $L \in \mathcal{L}(V)$, and fix $\mathbf{v} \in V$ such that $\mathbf{v} \neq \mathbf{0}$. Let $W$ be the $L$-cyclic subspace of $V$ generated by $\mathbf{v}$, with $m = \dim(W)$. By Proposition 6.52(1) the set

$$\mathcal{B} = \{\mathbf{v}, L(\mathbf{v}), \ldots, L^{m-1}(\mathbf{v})\}$$

is a basis for $W$, so that $L^m(\mathbf{v}) \in \text{Span}(\mathcal{B})$ and there exist scalars $a_0, \ldots, a_{m-1} \in \mathbb{F}$ such that

$$L^m(\mathbf{v}) = -a_0\mathbf{v} - a_1L(\mathbf{v}) - \cdots - a_{m-1}L^{m-1}(\mathbf{v}).$$

By Proposition 6.52(2) it follows that

$$P_{L|_W}(t) = (-1)^m(a_0I_V + a_1t + a_2t^2 + \cdots + a_{m-1}t^{m-1} + t^m).$$

Now, by Proposition 6.50, the polynomial $P_{L|_W}$ divides $P_L$, which is to say there exists some $f \in \mathcal{P}(\mathbb{F})$ such that

$$P_L(t) = f(t)P_{L|_W}(t),$$

and hence by Proposition 6.54(3)

$$P_L(L) = f(L) \circ P_{L|_W}(L).$$

However,

$$\begin{aligned} P_{L|_W}(L)(\mathbf{v}) &= \big((-1)^m(a_0I_V + a_1L + \cdots + a_{m-1}L^{m-1} + L^m)\big)(\mathbf{v}) \\ &= (-1)^m(a_0\mathbf{v} + a_1L(\mathbf{v}) + \cdots + a_{m-1}L^{m-1}(\mathbf{v}) + L^m(\mathbf{v})) \\ &= (-1)^m(-L^m(\mathbf{v}) + L^m(\mathbf{v})) = (-1)^m\mathbf{0} = \mathbf{0}, \end{aligned}$$

and so

$$P_L(L)(\mathbf{v}) = \big(f(L) \circ P_{L|_W}(L)\big)(\mathbf{v}) = f(L)\big(P_{L|_W}(L)(\mathbf{v})\big) = f(L)(\mathbf{0}) = \mathbf{0},$$

where the last equality follows from the observation that $f(L)$ is a linear operator by Proposition 6.54(1). Therefore $P_L(L)(\mathbf{v}) = \mathbf{0}$ for all nonzero $\mathbf{v} \in V$, and since $P_L(L)(\mathbf{0}) = \mathbf{0}$ also, we conclude that $P_L(L) = O_V$. ■

**Corollary 6.56.** *If $\mathbf{A} \in \mathbb{F}^{n\times n}$, then $P_{\mathbf{A}}(\mathbf{A}) = \mathbf{O}_n$.*

**Proof.** Suppose $\mathbf{A} \in \mathbb{F}^{n\times n}$. Let $L \in \mathcal{L}(\mathbb{F}^n)$ be such that $[L]_{\mathcal{E}} = \mathbf{A}$, so $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$ for all $\mathbf{x} \in \mathbb{F}^n$. By Definition 6.16 we have $P_L = P_{\mathbf{A}}$, where $\deg(P_{\mathbf{A}}) = n$ by Proposition 6.27 and so

$$P_{\mathbf{A}}(t) = P_L(t) = a_0 + a_1t + \cdots + a_nt^n$$

for some $a_0, \ldots, a_n \in \mathbb{F}$. By the Cayley-Hamilton Theorem $P_L(L) = O$, the zero operator on $\mathbb{F}^n$, which is to say

$$P_L(L)(\mathbf{x}) = (a_0I + a_1L + \cdots + a_nL^n)(\mathbf{x}) = O(\mathbf{x}) = \mathbf{0}$$

for all $\mathbf{x} \in \mathbb{F}^n$, where $I$ is the identity operator on $\mathbb{F}^n$. Now, $P_{\mathbf{A}}(\mathbf{A}) \in \mathbb{F}^{n\times n}$ is given by

$$P_{\mathbf{A}}(\mathbf{A}) = a_0\mathbf{I}_n + a_1\mathbf{A} + \cdots + a_n\mathbf{A}^n,$$

so that

$$\begin{aligned} P_{\mathbf{A}}(\mathbf{A})(\mathbf{x}) &= (a_0\mathbf{I}_n + a_1\mathbf{A} + \cdots + a_n\mathbf{A}^n)(\mathbf{x}) = a_0\mathbf{x} + a_1\mathbf{A}\mathbf{x} + \cdots + a_n\mathbf{A}^n\mathbf{x} \\ &= a_0 I(\mathbf{x}) + a_1 L(\mathbf{x}) + \cdots + a_n L^n(\mathbf{x}) = (a_0 I + a_1 L + \cdots + a_n L^n)(\mathbf{x}) \\ &= P_L(L)(\mathbf{x}) = O(\mathbf{x}) = \mathbf{0} \end{aligned}$$

for all $\mathbf{x} \in \mathbb{F}^n$, and therefore $P_{\mathbf{A}}(\mathbf{A}) = \mathbf{O}_n$ by Proposition 2.12(2). ∎

# 7

# Inner Product Spaces

## 7.1 – Inner Products

Recall that if $z$ is a complex number, then $\bar{z}$ denotes the conjugate of $z$, $\mathrm{Re}(z)$ denotes the real part of $z$, and $\mathrm{Im}(z)$ denotes the imaginary part of $z$. By definition,

$$\overline{a+bi} = a - bi, \quad \mathrm{Re}(a+bi) = a, \quad \mathrm{Im}(a+bi) = b$$

for any $a, b \in \mathbb{R}$. Throughout this chapter we take $\mathbb{F}$ to represent any field that is a subfield of the complex numbers $\mathbb{C}$, which is to say $\mathbb{F}$ is a field consisting of objects on which the operation of conjugation may be done. This of course includes $\mathbb{C}$ itself, as well as the field of real numbers $\mathbb{R}$, rational numbers $\mathbb{Q}$, and others.

**Definition 7.1.** *An* ***inner product*** *on a vector space $V$ over $\mathbb{F}$ is a function $\langle\ \rangle : V \times V \to \mathbb{F}$ that associates each pair of vectors $(\mathbf{u}, \mathbf{v}) \in V \times V$ with a scalar $\langle \mathbf{u}, \mathbf{v} \rangle \in \mathbb{F}$ in accordance with the following axioms:*

IP1. $\langle \mathbf{u}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{u} \rangle}$ *for all* $\mathbf{u}, \mathbf{v} \in V$
IP2. $\langle \mathbf{u} + \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle$ *for all* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$
IP3. $\langle a\mathbf{u}, \mathbf{v} \rangle = a\langle \mathbf{u}, \mathbf{v} \rangle$ *for all* $\mathbf{u}, \mathbf{v} \in V$ *and* $a \in \mathbb{F}$.
IP4. $\langle \mathbf{u}, \mathbf{u} \rangle > 0$ *for all* $\mathbf{u} \neq \mathbf{0}$.

*A vector space $V$ together with an associated inner product $\langle\ \rangle$ is called an* ***inner product space*** *and denoted by $(V, \langle\ \rangle)$.*

**Remark.** Care must be taken to not confuse the symbol for the inner product of two vectors $\langle \mathbf{u}, \mathbf{v} \rangle$ with, say, the symbol for a Euclidean vector $\langle x, y \rangle \in \mathbb{R}^2$ that is used in some textbooks (particularly calculus books). One features a pair of *vectors* between angle brackets, while the other features a pair of *scalars*.

An inner product $\langle\ \rangle$ associated with a vector space $V$ over $\mathbb{C}$ is generally complex-valued and called a **hermitian inner product** or simply a **hermitian product**, in which case the pair $(V, \langle\ \rangle)$ is called a **hermitian inner product space**.

Axiom IP1 is the **conjugate symmetry** property. If $V$ is a vector space over $\mathbb{R}$ (or some subfield of $\mathbb{R}$), then this axiom becomes

$$\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle \text{ for all } \mathbf{u}, \mathbf{v} \in V$$

and is called the **symmetry** property.

Axioms IP2 and IP3 taken together are the **linearity** properties, and using them we easily obtain

$$\langle \mathbf{u} - \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u} + (-\mathbf{v}), \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle -\mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle - \langle \mathbf{v}, \mathbf{w} \rangle.$$

Axiom IP4 is the **positive-definiteness** property. Products which satisfy all axioms save IP4 (or which satisfy a modified version of IP4) are also of theoretical interest, but will not be entertained in this chapter.

**Theorem 7.2.** *Let $(V, \langle\ \rangle)$ be an inner product space over $\mathbb{F}$. For $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and $a \in \mathbb{F}$, the following properties hold:*
1. $\langle \mathbf{0}, \mathbf{u} \rangle = \langle \mathbf{u}, \mathbf{0} \rangle = 0$.
2. $\langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle$.
3. $\langle \mathbf{u}, a\mathbf{v} \rangle = \bar{a}\langle \mathbf{u}, \mathbf{v} \rangle$.
4. $\langle \mathbf{u}, \mathbf{u} \rangle = 0$ *if and only if* $\mathbf{u} = \mathbf{0}$.
5. *If* $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle$ *for all* $\mathbf{u} \in V$, *then* $\mathbf{v} = \mathbf{w}$.

**Proof.**
*Proof of Part (1):* Let $\mathbf{u} \in V$. By Axiom IP2 we have

$$\langle \mathbf{0}, \mathbf{u} \rangle = \langle \mathbf{0} + \mathbf{0}, \mathbf{u} \rangle = \langle \mathbf{0}, \mathbf{u} \rangle + \langle \mathbf{0}, \mathbf{u} \rangle.$$

Subtracting $\langle \mathbf{0}, \mathbf{u} \rangle$ from the leftmost and rightmost expressions yields $\langle \mathbf{0}, \mathbf{u} \rangle = 0$ as desired. Then

$$\langle \mathbf{u}, \mathbf{0} \rangle = \overline{\langle \mathbf{0}, \mathbf{u} \rangle} = \bar{0} = 0$$

completes the proof.

*Proof of Part (2):* For any $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ we have

$$\begin{aligned}
\langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle &= \overline{\langle \mathbf{v} + \mathbf{w}, \mathbf{u} \rangle} && \text{Axiom IP1} \\
&= \overline{\langle \mathbf{v}, \mathbf{u} \rangle + \langle \mathbf{w}, \mathbf{u} \rangle} && \text{Axiom IP2} \\
&= \overline{\langle \mathbf{v}, \mathbf{u} \rangle} + \overline{\langle \mathbf{w}, \mathbf{u} \rangle} && \text{Property of complex conjugates} \\
&= \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle && \text{Axiom IP1}
\end{aligned}$$

*Proof of Part (3):* For any $\mathbf{u}, \mathbf{v} \in V$ and $a \in \mathbb{F}$ we have

$$\begin{aligned}
\langle \mathbf{u}, a\mathbf{v} \rangle &= \overline{\langle a\mathbf{v}, \mathbf{u} \rangle} && \text{Axiom IP1} \\
&= \overline{a\langle \mathbf{v}, \mathbf{u} \rangle} && \text{Axiom IP3} \\
&= \bar{a}\overline{\langle \mathbf{v}, \mathbf{u} \rangle} && \text{Property of complex conjugates}
\end{aligned}$$

$$= \bar{a}\langle \mathbf{u}, \mathbf{v}\rangle \qquad \text{Axiom IP1}$$

*Proof of Part (4):* The contrapositive of Axiom IP4 states that if $\langle \mathbf{u}, \mathbf{u}\rangle \leq 0$, then $\mathbf{u} = \mathbf{0}$. Thus, in particular, $\langle \mathbf{u}, \mathbf{u}\rangle = 0$ implies that $\mathbf{u} = \mathbf{0}$.

For the converse, suppose that $\mathbf{u} = \mathbf{0}$. Then, applying Axiom IP2,

$$\langle \mathbf{u}, \mathbf{u}\rangle = \langle \mathbf{0}, \mathbf{0}\rangle = \langle \mathbf{0} + \mathbf{0}, \mathbf{0}\rangle = \langle \mathbf{0}, \mathbf{0}\rangle + \langle \mathbf{0}, \mathbf{0}\rangle;$$

that is,

$$\langle \mathbf{0}, \mathbf{0}\rangle + \langle \mathbf{0}, \mathbf{0}\rangle = \langle \mathbf{0}, \mathbf{0}\rangle,$$

from which we obtain $\langle \mathbf{0}, \mathbf{0}\rangle = 0$. We conclude that $\mathbf{u} = \mathbf{0}$ implies that $\langle \mathbf{u}, \mathbf{u}\rangle = 0$.

*Proof of Part (5):* Suppose that $\langle \mathbf{u}, \mathbf{v}\rangle = \langle \mathbf{u}, \mathbf{w}\rangle$ for all $\mathbf{u} \in V$. Then

$$\begin{aligned}\langle \mathbf{u}, \mathbf{v} - \mathbf{w}\rangle &= \langle \mathbf{u}, \mathbf{v} + (-1)\mathbf{w}\rangle = \langle \mathbf{u}, \mathbf{v}\rangle + \langle \mathbf{u}, (-1)\mathbf{w}\rangle \\ &= \langle \mathbf{u}, \mathbf{v}\rangle + (-1)\langle \mathbf{u}, \mathbf{w}\rangle = \langle \mathbf{u}, \mathbf{v}\rangle - \langle \mathbf{u}, \mathbf{w}\rangle \\ &= \langle \mathbf{u}, \mathbf{v}\rangle - \langle \mathbf{u}, \mathbf{v}\rangle = 0\end{aligned}$$

for all $\mathbf{u} \in V$, making use of Proposition 3.3, parts (2) and (3), and the property

$$x + (-1)y = x - y$$

for $x, y \in \mathbb{F}$. Letting $\mathbf{u} = \mathbf{v} - \mathbf{w}$ subsequently yields

$$\langle \mathbf{v} - \mathbf{w}, \mathbf{v} - \mathbf{w}\rangle = 0,$$

so that $\mathbf{v} - \mathbf{w} = \mathbf{0}$ by part (4), and therefore $\mathbf{v} = \mathbf{w}$. ■

One sure result that obtains from Axiom IP4 and Theorem 7.2(4) is that $\langle \mathbf{u}, \mathbf{u}\rangle \geq 0$ for all $\mathbf{u} \in V$. This will be important when the discussion turns to norms in the next section.

Recall the Euclidean dot product as defined for vectors

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \quad \text{and} \quad \mathbf{y} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$$

in $\mathbb{R}^n$:

$$\mathbf{x} \cdot \mathbf{y} = \mathbf{y}^\top \mathbf{x} = \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \sum_{k=1}^{n} x_k y_k.$$

It is easily verified that the Euclidean dot product applied to $\mathbb{R}^n$ satisfies the four axioms of an inner product, and so $(\mathbb{R}^n, \cdot)$ is an inner product space.

It might be assumed that $(\mathbb{C}^n, \cdot)$ is also an inner product space (where as usual $\mathbb{C}^n$ is taken to have underlying field $\mathbb{C}$), but this is not the case. Consider for instance the vector $\mathbf{z} = [\,1 \;\; i\,]^\top$ in $\mathbb{C}^2$. We have

$$\mathbf{z} \cdot \mathbf{z} = \mathbf{z}^\top \mathbf{z} = \begin{bmatrix} 1 & i \end{bmatrix} \begin{bmatrix} 1 \\ i \end{bmatrix} = 1^2 + i^2 = 1 + (-1) = 0;$$

that is, $\mathbf{z} \cdot \mathbf{z} = 0$ even though $\mathbf{z} \neq \mathbf{0}$, and so Axiom IP4 fails! Or consider $\mathbf{z} = [\,i\;\;0\;\;0\,]^\top$ in $\mathbb{C}^3$, for which we find that

$$\mathbf{z} \cdot \mathbf{z} = \mathbf{z}^\top \mathbf{z} = \begin{bmatrix} i & 0 & 0 \end{bmatrix} \begin{bmatrix} i \\ 0 \\ 0 \end{bmatrix} = i^2 = -1 < 0$$

and again Axiom IP4 fails. To remedy the situation only requires a modest modification of the dot product definition. For the definition we need the **conjugate transpose** matrix operation: If $\mathbf{A} = [a_{ij}] \in \mathbb{C}^{m \times n}$, then set

$$\mathbf{A}^* = \overline{\mathbf{A}}^\top = [\overline{a}_{ij}]^\top.$$

Thus, in particular, if

$$\mathbf{z} = \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \in \mathbb{C}^n,$$

then

$$\mathbf{z}^* = \begin{bmatrix} \overline{z}_1 & \cdots & \overline{z}_n \end{bmatrix}.$$

**Definition 7.3.** *If $\mathbf{w}, \mathbf{z} \in \mathbb{C}^n$, then the* ***hermitian dot product*** *of $\mathbf{w}$ and $\mathbf{z}$ is*

$$\mathbf{w} \cdot \mathbf{z} = \mathbf{z}^* \mathbf{w} = \begin{bmatrix} \overline{z}_1 & \cdots & \overline{z}_n \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} = \sum_{k=1}^n w_k \overline{z}_k. \tag{7.1}$$

The natural isomorphism $[a]_{1\times 1} \mapsto a$ is an implicit part of the definition, so that the hermitian dot product produces a scalar value as expected.

Letting $\cdot$ denote the hermitian dot product, we return to the vector $[\,1\;\;i\,]^\top \in \mathbb{C}^2$ and find that

$$\begin{bmatrix} 1 \\ i \end{bmatrix} \cdot \begin{bmatrix} 1 \\ i \end{bmatrix} = \begin{bmatrix} \overline{1} & \overline{i} \end{bmatrix} \begin{bmatrix} 1 \\ i \end{bmatrix} = \begin{bmatrix} 1 & -i \end{bmatrix} \begin{bmatrix} 1 \\ i \end{bmatrix} = 1 \cdot 1 + i(-i) = 1 - i^2 = 1 - (-1) = 2,$$

which is an outcome that does not run afoul of Axiom IP4 and so corrects the problem $[\,1\;\;i\,]^\top$ presented for the Euclidean dot product above.

The hermitian dot product becomes the Euclidean dot product when applied to vectors in $\mathbb{R}^n$: letting $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ we have

$$\mathbf{x} \cdot \mathbf{y} = \mathbf{y}^* \mathbf{x} = \overline{\mathbf{y}}^\top \mathbf{x} = \begin{bmatrix} \overline{y}_1 & \cdots & \overline{y}_n \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} y_1 & \cdots & y_n \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \mathbf{y}^\top \mathbf{x},$$

since $y_k \in \mathbb{R}$ implies that $\overline{y}_k = y_k$ for each $1 \leq k \leq n$. For this reason we will henceforth always assume (unless stated otherwise) that $\cdot$ denotes the hermitian dot product, and call it simply the **dot product**.

**Example 7.4.** Let $a, b \in \mathbb{R}$ such that $a < b$, and let $V$ be the vector space over $\mathbb{R}$ consisting of all continuous functions $f : [a, b] \to \mathbb{R}$. Given $f, g \in V$, define

$$\langle f, g \rangle = \int_a^b fg. \tag{7.2}$$

We verify that $(V, \langle\ \rangle)$ is an inner product space. Since $\langle f, g\rangle$ is real-valued for any $f, g \in V$, we have

$$\langle f, g\rangle = \int_a^b fg = \int_a^b gf = \langle g, f\rangle = \overline{\langle g, f\rangle}$$

and thus Axiom IP1 is confirmed.

Next, for any $f, g, h \in V$ we have

$$\langle f + g, h\rangle = \int_a^b (f+g)h = \int_a^b (fh + fg) = \int_a^b fh + \int_a^b fg = \langle f, h\rangle + \langle f, g\rangle,$$

confirming Axiom IP2.

Axiom IP3 obtains readily:

$$\langle af, g\rangle = \int_a^b (af)g = \int_a^b a(fg) = a\int_a^b fg = a\langle f, g\rangle.$$

Next, for any $f \in V$ we have $f^2(x) \geq 0$ for all $x \in [a, b]$, and so

$$\langle f, f\rangle = \int_a^b f^2 \geq 0$$

follows from an established property of the definite integral. Finally, if

$$\int_a^b f^2 = 0$$

it follows from another property of definite integrals that $f(x) = 0$ for all $x \in [a, b]$, which is to say $f = 0$ and therefore Axiom IP4 holds. ■

**Example 7.5.** Recall the notion of the trace of a square matrix, which is a linear mapping $\text{tr} : \mathbb{F}^{n\times n} \to \mathbb{F}$ given by

$$\text{tr}(\mathbf{A}) = \sum_{i=1}^{n} a_{ii}$$

for each $\mathbf{A} = [a_{ij}] \in \mathbb{F}^{n\times n}$. Letting $\mathbb{F} = \mathbb{R}$, define $\langle\ \rangle : \text{Sym}_n(\mathbb{R}) \times \text{Sym}_n(\mathbb{R}) \to \mathbb{R}$ by

$$\langle \mathbf{A}, \mathbf{B}\rangle = \text{tr}(\mathbf{AB}).$$

The claim is that $(\text{Sym}_n(\mathbb{R}), \langle\ \rangle)$ is an inner product space. To substantiate the claim we must verify that the four axioms of an inner product are satisfied.

Let $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$ be elements of $\text{Sym}_n(\mathbb{R})$. The $ii$-entry of $\mathbf{AB}$ is $\sum_{j=1}^{n} a_{ij}b_{ji}$, and so

$$\text{tr}(\mathbf{AB}) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}b_{ji}. \tag{7.3}$$

The $ii$-entry of $\mathbf{BA}$ is $\sum_{j=1}^{n} b_{ij}a_{ji}$, from which we obtain

$$\begin{aligned}\text{tr}(\mathbf{BA}) &= \sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}a_{ji} \\ &= \sum_{j=1}^{n}\sum_{i=1}^{n} b_{ji}a_{ij} \qquad \text{(Interchange } i \text{ and } j\text{)}\end{aligned}$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}b_{ji} \qquad \text{(Interchange summations)}$$

$$= \mathrm{tr}(\mathbf{AB}). \qquad \text{(Equation (7.3))}$$

Hence

$$\langle \mathbf{A}, \mathbf{B} \rangle = \mathrm{tr}(\mathbf{AB}) = \mathrm{tr}(\mathbf{BA}) = \langle \mathbf{B}, \mathbf{A} \rangle$$

and Axiom IP1 is confirmed to hold.

In Chapter 4 it was found that the trace operation is a linear mapping, and so for any $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathrm{Sym}_n(\mathbb{R})$ and $x \in \mathbb{R}$ we have

$$\langle \mathbf{A}+\mathbf{B}, \mathbf{C} \rangle = \mathrm{tr}((\mathbf{A}+\mathbf{B})\mathbf{C}) = \mathrm{tr}(\mathbf{AC}+\mathbf{BC}) = \mathrm{tr}(\mathbf{AC}) + \mathrm{tr}(\mathbf{BC}) = \langle \mathbf{A}, \mathbf{C} \rangle + \langle \mathbf{B}, \mathbf{C} \rangle$$

and

$$\langle x\mathbf{A}, \mathbf{B} \rangle = \mathrm{tr}((x\mathbf{A})\mathbf{B}) = \mathrm{tr}(x(\mathbf{AB})) = x\,\mathrm{tr}(\mathbf{AB}) = x\langle \mathbf{A}, \mathbf{B} \rangle,$$

which confirms Axioms IP2 and IP3.

Next, observing that $\mathbf{A} = [a_{ij}] \in \mathrm{Sym}_n(\mathbb{R})$ if and only if $a_{ij} = a_{ji}$ for all $1 \leq i, j \leq n$, we have

$$\langle \mathbf{A}, \mathbf{A} \rangle = \mathrm{tr}(\mathbf{A}^2) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}a_{ji} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}a_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^2 \geq 0.$$

It is easy to see that if $\mathrm{tr}(\mathbf{A}^2) = 0$, then we must have $a_{ij} = 0$ for all $1 \leq i, j \leq n$, and thus $\mathbf{A} = \mathbf{O}_n$. Axiom IP4 is confirmed. ∎

## 7.2 – Norms

Given an inner product space $(V, \langle\ \rangle)$ and a vector $\mathbf{u} \in V$, we define the **norm** of $\mathbf{u}$ to be the scalar

$$\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}.$$

If $\|\mathbf{u}\| = 1$ we say that $\mathbf{u}$ is a **unit vector**. Notice that, by Axiom IP4, $\|\mathbf{u}\|$ is always a nonnegative real number. The **distance** $d(\mathbf{u}, \mathbf{v})$ between two vectors $\mathbf{u}, \mathbf{v} \in V$ is given by

$$d(\mathbf{u}, \mathbf{v}) = \|\mathbf{u} - \mathbf{v}\|,$$

also always a nonnegative real number. If

$$\langle \mathbf{u}, \mathbf{v} \rangle = 0$$

we say that $\mathbf{u}$ and $\mathbf{v}$ are **orthogonal** and write $\mathbf{u} \perp \mathbf{v}$.

**Proposition 7.6.** *Let $(V, \langle\ \rangle)$ be an inner product space. If $W \subseteq V$ is a subspace of $V$, then*

$$W^\perp = \{\mathbf{v} \in V : \langle \mathbf{v}, \mathbf{w} \rangle = 0 \text{ for all } \mathbf{w} \in W\} \tag{7.4}$$

*is also a subspace of $V$.*

**Proof.** Suppose $\mathbf{u}, \mathbf{v} \in W^\perp$. Then for any $\mathbf{w} \in W$ we have

$$\langle \mathbf{u} + \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle = 0 + 0 = 0,$$

which shows that $\mathbf{u} + \mathbf{v} \in W^\perp$. Moreover, for any $a \in \mathbb{F}$ we have

$$\langle a\mathbf{u}, \mathbf{w} \rangle = a\langle \mathbf{u}, \mathbf{w} \rangle = a(0) = 0$$

for any $\mathbf{w} \in W$, which shows that $a\mathbf{u} \in W^\perp$. Since $W^\perp \subseteq V$ is closed under scalar multiplication and vector addition, we conclude that it is a subspace of $V$. ■

The subspace $W^\perp$ defined by (7.4) is called the **orthogonal complement** of $W$.[6] If $\mathbf{v} \in W^\perp$, then we say $\mathbf{v}$ is **orthogonal** to $W$ and write $\mathbf{v} \perp W$.

**Proposition 7.7.** *Let $(V, \langle\ \rangle)$ be an inner product space. Let $\mathbf{w}_1, \dots, \mathbf{w}_m \in V$, and define the subspace*

$$U = \{\mathbf{v} \in V : \mathbf{v} \perp \mathbf{w}_i \text{ for all } 1 \le i \le m\}.$$

*If $W = \text{Span}\{\mathbf{w}_1, \dots, \mathbf{w}_m\}$, then $U = W^\perp$.*

**Proof.** It is a routine matter to verify that $U$ is indeed a subspace of $V$. Let $\mathbf{v} \in U$. For any $\mathbf{w} \in W$ we have

$$\mathbf{w} = c_1\mathbf{w}_1 + \cdots + c_m\mathbf{w}_m$$

for some $c_1, \dots, c_m \in \mathbb{F}$, and then since $\mathbf{v} \perp \mathbf{w}_i$ implies $\langle \mathbf{w}_i, \mathbf{v} \rangle = 0$ we obtain

$$\langle \mathbf{w}, \mathbf{v} \rangle = \left\langle \sum_{i=1}^m c_i\mathbf{w}_i, \mathbf{v} \right\rangle = \sum_{i=1}^m c_i\langle \mathbf{w}_i, \mathbf{v} \rangle = \sum_{i=1}^m c_i(0) = 0$$

[6]The symbol $W^\perp$ is often read as "$W$ perp."

by Axioms IP2 and IP3. Hence $\mathbf{v} \perp \mathbf{w}$ for all $\mathbf{w} \in W$, so that $\mathbf{v} \in W^\perp$ and therefore $U \subseteq W^\perp$.

Next, let $\mathbf{v} \in W^\perp$. Then $\langle \mathbf{w}, \mathbf{v} \rangle = 0$ for all $\mathbf{w} \in W$, or equivalently

$$\left\langle \sum_{i=1}^m c_i \mathbf{w}_i, \mathbf{v} \right\rangle = 0 \tag{7.5}$$

for any $c_1, \ldots, c_m \in \mathbb{F}$. If for any $1 \leq i \leq m$ we choose $c_i = 1$ and $c_j = 0$ for $j \neq i$, then (7.5) gives $\langle \mathbf{w}_i, \mathbf{v} \rangle = 0$. Thus $\mathbf{v} \perp \mathbf{w}_i$ for all $1 \leq i \leq m$, implying that $\mathbf{v} \in U$ and so $W^\perp \subseteq U$.

Therefore $U = W^\perp$. ∎

Let $\mathbf{v} \in (V, \langle\, \rangle)$ such that $\|\mathbf{v}\| \neq 0$. Given any $\mathbf{u} \in (V, \langle\, \rangle)$ there can be found some $c \in \mathbb{F}$ such that

$$\langle \mathbf{v}, \mathbf{u} - c\mathbf{v} \rangle = 0.$$

Indeed

$$\begin{aligned} \langle \mathbf{v}, \mathbf{u} - c\mathbf{v} \rangle = 0 \quad &\Leftrightarrow \quad \langle \mathbf{v}, \mathbf{u} \rangle - \langle \mathbf{v}, c\mathbf{v} \rangle = 0 \quad \Leftrightarrow \quad \langle \mathbf{v}, \mathbf{u} \rangle - \bar{c}\langle \mathbf{v}, \mathbf{v} \rangle = 0 \\ &\Leftrightarrow \quad \bar{c}\langle \mathbf{v}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle \quad \Leftrightarrow \quad \overline{\bar{c}\langle \mathbf{v}, \mathbf{v} \rangle} = \overline{\langle \mathbf{v}, \mathbf{u} \rangle} \\ &\Leftrightarrow \quad c\langle \mathbf{v}, \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle \quad \Leftrightarrow \quad c = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle}, \end{aligned} \tag{7.6}$$

where $\langle \mathbf{v}, \mathbf{v} \rangle \neq 0$ since $\|\mathbf{v}\| \neq 0$.

**Definition 7.8.** *Let $\|\mathbf{v}\| \neq 0$. The **orthogonal projection of $\mathbf{u}$ onto $\mathbf{v}$** is given by*

$$\operatorname{proj}_{\mathbf{v}} \mathbf{u} = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle} \mathbf{v}.$$

**Theorem 7.9.** *Let $\mathbf{u}, \mathbf{v} \in (V, \langle\, \rangle)$.*

1. *Pythagorean Theorem: If $\mathbf{u} \perp \mathbf{v}$, then*
$$\|\mathbf{u} + \mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2.$$
2. *Parallelogram Law:*
$$\|\mathbf{u} + \mathbf{v}\|^2 + \|\mathbf{u} - \mathbf{v}\|^2 = 2\|\mathbf{u}\|^2 + 2\|\mathbf{v}\|^2.$$
3. *Schwarz Inequality:*
$$|\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\|\|\mathbf{v}\|.$$
4. *Triangle Inequality:*
$$\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|.$$
5. *Cauchy Inequality:*
$$\|\mathbf{u}\|\|\mathbf{v}\| \leq \frac{1}{2}\|\mathbf{u}\|^2 + \frac{1}{2}\|\mathbf{v}\|^2.$$

**Proof.**

*Pythagorean Theorem:* Suppose $\mathbf{u} \perp \mathbf{v}$, so that $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle = 0$. By direct calculation we have

$$\begin{aligned} \|\mathbf{u} + \mathbf{v}\|^2 &= \langle \mathbf{u} + \mathbf{v}, \mathbf{u} + \mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} + \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{u} + \mathbf{v} \rangle && \text{Axiom IP2} \\ &= \langle \mathbf{u}, \mathbf{u} \rangle + \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{u} \rangle + \langle \mathbf{v}, \mathbf{v} \rangle && \text{Theorem 7.2(2)} \end{aligned}$$

$$= \langle \mathbf{u}, \mathbf{u} \rangle + \langle \mathbf{v}, \mathbf{v} \rangle = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2$$

*Parallelogram Law:* We have

$$\|\mathbf{u}+\mathbf{v}\|^2 = \langle \mathbf{u}, \mathbf{u} \rangle + \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{u} \rangle + \langle \mathbf{v}, \mathbf{v} \rangle = \|\mathbf{u}\|^2 + \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{u} \rangle + \|\mathbf{v}\|^2 \tag{7.7}$$

from the proof of the Pythagorean Theorem, and

$$\|\mathbf{u}-\mathbf{v}\|^2 = \langle \mathbf{u}-\mathbf{v}, \mathbf{u}-\mathbf{v} \rangle = \|\mathbf{u}\|^2 - \langle \mathbf{u}, \mathbf{v} \rangle - \langle \mathbf{v}, \mathbf{u} \rangle + \|\mathbf{v}\|^2. \tag{7.8}$$

Adding equations (7.7) and (7.8) completes the proof.

*Schwarz Inequality:* If $\mathbf{u} = \mathbf{0}$ or $\mathbf{v} = \mathbf{0}$, then by Theorem 7.2(1) we obtain

$$\|\langle \mathbf{u}, \mathbf{v} \rangle\| = |0| = 0 = \|\mathbf{u}\|\|\mathbf{v}\|,$$

which affirms the theorem's conclusion.

Suppose $\mathbf{u}, \mathbf{v} \neq \mathbf{0}$, and let

$$c = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle} = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{v}\|^2}.$$

Now, by (7.6),

$$\langle \mathbf{u} - c\mathbf{v}, c\mathbf{v} \rangle = c\langle \mathbf{u} - c\mathbf{v}, \mathbf{v} \rangle = c\overline{\langle \mathbf{v}, \mathbf{u} - c\mathbf{v} \rangle} = c(\bar{0}) = c(0) = 0.$$

Thus $\mathbf{u} - c\mathbf{v}$ and $c\mathbf{v}$ are orthogonal, and by the Pythagorean Theorem

$$\|\mathbf{u}\|^2 = \|(\mathbf{u} - c\mathbf{v}) + c\mathbf{v}\|^2 = \|\mathbf{u} - c\mathbf{v}\|^2 + \|c\mathbf{v}\|^2.$$

Hence $\|c\mathbf{v}\|^2 \leq \|\mathbf{u}\|^2$ since $\|\mathbf{u} - c\mathbf{v}\|^2 \geq 0$. However, recalling that $z\bar{z} = |z|^2$ for any $z \in \mathbb{F}$, we obtain

$$\|c\mathbf{v}\|^2 = \langle c\mathbf{v}, c\mathbf{v} \rangle = c\bar{c}\langle \mathbf{v}, \mathbf{v} \rangle = |c|^2\|\mathbf{v}\|^2 = \frac{|\langle \mathbf{u}, \mathbf{v} \rangle|^2}{\|\mathbf{v}\|^4}\|\mathbf{v}\|^2 = \frac{|\langle \mathbf{u}, \mathbf{v} \rangle|^2}{\|\mathbf{v}\|^2},$$

and so $\|c\mathbf{v}\|^2 \leq \|\mathbf{u}\|^2$ implies that

$$\frac{|\langle \mathbf{u}, \mathbf{v} \rangle|^2}{\|\mathbf{v}\|^2} \leq \|\mathbf{u}\|^2.$$

Therefore we have

$$|\langle \mathbf{u}, \mathbf{v} \rangle|^2 \leq \|\mathbf{u}\|^2\|\mathbf{v}\|^2,$$

and taking the square root of both sides completes the proof.

*Triangle Inequality:* For any $\mathbf{u}, \mathbf{v} \in V$ we have $\langle \mathbf{u}, \mathbf{v} \rangle = a + bi$ for some $a, b \in \mathbb{R}$, so that the real part of $\langle \mathbf{u}, \mathbf{v} \rangle$ is $\text{Re}(\langle \mathbf{u}, \mathbf{v} \rangle) = a$. (If $V$ is a vector field over $\mathbb{R}$ then $b = 0$, but this will not affect our analysis.) By the Schwarz Inequality we have

$$\sqrt{a^2 + b^2} = |a + bi| = |\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\|\|\mathbf{v}\|,$$

and since

$$\text{Re}\big(\langle \mathbf{u}, \mathbf{v} \rangle\big) = a \leq |a| = \sqrt{a^2} \leq \sqrt{a^2 + b^2},$$

it follows that

$$\text{Re}\big(\langle \mathbf{u}, \mathbf{v} \rangle\big) \leq \|\mathbf{u}\|\|\mathbf{v}\|. \tag{7.9}$$

Recalling the property of complex numbers $z + \bar{z} = 2\,\mathrm{Re}(z)$, we have

$$\langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{u} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \overline{\langle \mathbf{u}, \mathbf{v} \rangle} = 2\,\mathrm{Re}\big(\langle \mathbf{u}, \mathbf{v} \rangle\big). \tag{7.10}$$

Now,

$$\begin{aligned}
\|\mathbf{u}+\mathbf{v}\|^2 &= \|\mathbf{u}\|^2 + \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{u} \rangle + \|\mathbf{v}\|^2 && \text{Equation (7.7)}\\
&= \|\mathbf{u}\|^2 + 2\,\mathrm{Re}\big(\langle \mathbf{u}, \mathbf{v} \rangle\big) + \|\mathbf{v}\|^2 && \text{Equation (7.10)}\\
&\leq \|\mathbf{u}\|^2 + 2\|\mathbf{u}\|\|\mathbf{v}\| + \|\mathbf{v}\|^2, && \text{Inequality (7.9)}
\end{aligned}$$

and so

$$\|\mathbf{u}+\mathbf{v}\|^2 \leq \big(\|\mathbf{u}\| + \|\mathbf{v}\|\big)^2.$$

Taking the square root of both sides completes the proof.

*Cauchy Inequality:* This inequality in fact holds for all real numbers: if $a, b \in \mathbb{R}$, then

$$0 \leq (a-b)^2 = a^2 - 2ab + b^2 \;\;\Rightarrow\;\; 2ab \leq a^2 + b^2 \;\;\Rightarrow\;\; ab \leq \frac{1}{2}a^2 + \frac{1}{2}b^2,$$

and we're done. ■

**Proposition 7.10.** *Let $(V, \langle\ \rangle)$ be an inner product space, and let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ be such that $\mathbf{v}_i \neq \mathbf{0}$ for each $1 \leq i \leq n$ and $\mathbf{v}_i \perp \mathbf{v}_j$ whenever $i \neq j$. If $\mathbf{v} \in V$ and*

$$c_i = \frac{\langle \mathbf{v}, \mathbf{v}_i \rangle}{\langle \mathbf{v}_i, \mathbf{v}_i \rangle}$$

*for each $1 \leq i \leq n$, then*

$$\mathbf{v} - \sum_{i=1}^{n} c_i \mathbf{v}_i$$

*is orthogonal to $\mathbf{v}_1, \ldots, \mathbf{v}_n$.*

**Proof.** Fix $1 \leq k \leq n$. Since $\mathbf{v}_k \neq 0$ we have $\langle \mathbf{v}_k, \mathbf{v}_k \rangle \neq 0$. Also $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0$ whenever $i \neq j$. Now,

$$\begin{aligned}
\left\langle \mathbf{v} - \sum_{i=1}^{n} c_i \mathbf{v}_i, \mathbf{v}_k \right\rangle &= \langle \mathbf{v}, \mathbf{v}_k \rangle - \left\langle \sum_{i=1}^{n} c_i \mathbf{v}_i, \mathbf{v}_k \right\rangle = \langle \mathbf{v}, \mathbf{v}_k \rangle - \sum_{i=1}^{n} c_i \langle \mathbf{v}_i, \mathbf{v}_k \rangle\\
&= \langle \mathbf{v}, \mathbf{v}_k \rangle - c_k \langle \mathbf{v}_k, \mathbf{v}_k \rangle = \langle \mathbf{v}, \mathbf{v}_k \rangle - \frac{\langle \mathbf{v}, \mathbf{v}_k \rangle}{\langle \mathbf{v}_k, \mathbf{v}_k \rangle} \langle \mathbf{v}_k, \mathbf{v}_k \rangle\\
&= \langle \mathbf{v}, \mathbf{v}_k \rangle - \langle \mathbf{v}, \mathbf{v}_k \rangle = 0,
\end{aligned}$$

and therefore $\mathbf{v} - \sum_{k=1}^{n} c_k \mathbf{v}_k \perp \mathbf{v}_k$ for any $1 \leq k \leq n$. ■

**Proposition 7.11.** *Let $(V, \langle\ \rangle)$ be an inner product space, and let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ be such that $\mathbf{v}_i \neq \mathbf{0}$ for each $1 \leq i \leq n$ and $\mathbf{v}_i \perp \mathbf{v}_j$ whenever $i \neq j$. If $\mathbf{v} \in V$ and $c_i = \langle \mathbf{v}, \mathbf{v}_i \rangle / \langle \mathbf{v}_i, \mathbf{v}_i \rangle$ for each $1 \leq i \leq n$, then*

$$\left\| \mathbf{v} - \sum\nolimits_{i=1}^{n} c_i \mathbf{v}_i \right\| \leq \left\| \mathbf{v} - \sum\nolimits_{i=1}^{n} a_i \mathbf{v}_i \right\|$$

*for any $a_1, \ldots, a_n \in \mathbb{F}$.*

**Proof.** Fix $\mathbf{v} \in V$ and $a_1, \ldots, a_n \in \mathbb{F}$, and let $c_i = \langle \mathbf{v}, \mathbf{v}_i \rangle / \langle \mathbf{v}_i, \mathbf{v}_i \rangle$ for each $1 \leq i \leq n$. First we observe that for any scalars $x_1, \ldots, x_n$ we have

$$\begin{aligned}
\left\langle \mathbf{v} - \sum\nolimits_{k=1}^{n} c_k \mathbf{v}_k, \sum\nolimits_{i=1}^{n} x_i \mathbf{v}_i \right\rangle &= \sum\nolimits_{i=1}^{n} \left\langle \mathbf{v} - \sum\nolimits_{k=1}^{n} c_k \mathbf{v}_k, x_i \mathbf{v}_i \right\rangle && \text{Theorem 7.2(2)} \\
&= \sum\nolimits_{i=1}^{n} \bar{x}_i \left\langle \mathbf{v} - \sum\nolimits_{k=1}^{n} c_k \mathbf{v}_k, \mathbf{v}_i \right\rangle && \text{Theorem 7.2(3)} \\
&= \sum\nolimits_{i=1}^{n} \bar{x}_i (0) = 0, && \text{Proposition 7.10}
\end{aligned}$$

which is to say that $\mathbf{v} - \sum_{k=1}^{n} c_k \mathbf{v}_k$ is orthogonal to any linear combination of the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$. In particular

$$\mathbf{v} - \sum_{i=1}^{n} c_i \mathbf{v}_i \ \perp \ \sum_{i=1}^{n} (c_i - a_i) \mathbf{v}_i,$$

and so by the Pythagorean Theorem

$$\begin{aligned}
\left\| \mathbf{v} - \sum\nolimits_{i=1}^{n} a_i \mathbf{v}_i \right\|^2 &= \left\| \mathbf{v} - \sum\nolimits_{i=1}^{n} c_i \mathbf{v}_i + \sum\nolimits_{i=1}^{n} (c_i - a_i) \mathbf{v}_i \right\|^2 \\
&= \left\| \mathbf{v} - \sum\nolimits_{i=1}^{n} c_i \mathbf{v}_i \right\|^2 + \left\| \sum\nolimits_{i=1}^{n} (c_i - a_i) \mathbf{v}_i \right\|^2 \\
&\geq \left\| \mathbf{v} - \sum\nolimits_{i=1}^{n} c_i \mathbf{v}_i \right\|^2.
\end{aligned}$$

Taking square roots completes the proof. ∎

## Problems

1. Let $(V, \langle\ \rangle)$ be an inner product space, and let $S \subseteq V$ with $S \neq \varnothing$. Show that
$$S^{\perp} = \{\mathbf{v} \in V : \langle \mathbf{v}, \mathbf{s} \rangle = 0 \text{ for all } \mathbf{s} \in S\}$$
is a subspace of $V$ even if $S$ is not a subspace.

## 7.3 – Orthogonal Bases

If $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis for a vector space $V$ and $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$ is an inner product, then we refer to $\mathcal{B}$ as a basis for the inner product space $(V, \langle\,\rangle)$.

**Definition 7.12.** *Let $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis for an inner product space $(V, \langle\,\rangle)$. If $\mathbf{v}_i \perp \mathbf{v}_j$ whenever $i \neq j$, then $\mathcal{B}$ is an **orthogonal basis**. If $\mathcal{B}$ is an orthogonal basis such that $\|\mathbf{v}_i\| = 1$ for all $i$, then $\mathcal{B}$ is called an **orthonormal basis**.*

**Lemma 7.13.** *Let $\mathbf{v}_1, \dots, \mathbf{v}_n \in (V, \langle\,\rangle)$ be nonzero vectors. If $\mathbf{v}_i \perp \mathbf{v}_j$ whenever $i \neq j$, then $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent.*

**Proof.** Suppose that $\mathbf{v}_i \perp \mathbf{v}_j$ whenever $i \neq j$. Let $x_1, \dots, x_n \in \mathbb{F}$ and set

$$x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n = \mathbf{0}. \tag{7.11}$$

Now, for each $1 \leq i \leq n$,

$$\left\langle \sum_{k=1}^{n} x_k\mathbf{v}_k, \mathbf{v}_i \right\rangle = \langle \mathbf{0}, \mathbf{v}_i \rangle = 0.$$

On the other hand,

$$\left\langle \sum_{k=1}^{n} x_k\mathbf{v}_k, \mathbf{v}_i \right\rangle = \sum_{k=1}^{n} x_k\langle \mathbf{v}_k, \mathbf{v}_i \rangle = x_i\langle \mathbf{v}_i, \mathbf{v}_i \rangle.$$

Hence

$$x_i\langle \mathbf{v}_i, \mathbf{v}_i \rangle = 0,$$

and since $\mathbf{v}_i \neq \mathbf{0}$ implies $\langle \mathbf{v}_i, \mathbf{v}_i \rangle \neq 0$, it follows that $x_i = 0$. Therefore (7.11) leads to the conclusion that $x_1 = \cdots = x_n = 0$, and so $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent. ■

**Theorem 7.14 (Gram-Schmidt Orthogonalization Process).** *Let $m \in \mathbb{N}$. For any $n \in \mathbb{N}$, if $(V, \langle\,\rangle)$ is an inner product space over $\mathbb{F}$ with $\dim(V) = m + n$, $W$ is a subspace of $V$ with orthogonal basis $(\mathbf{w}_i)_{i=1}^{m}$, and*

$$(\mathbf{w}_1, \dots, \mathbf{w}_m, \mathbf{u}_{m+1}, \dots, \mathbf{u}_{m+n}) \tag{7.12}$$

*is a basis for $V$, then an orthogonal basis for $V$ is $(\mathbf{w}_i)_{i=1}^{m+n}$, where*

$$\mathbf{w}_i = \mathbf{u}_i - \sum_{k=1}^{i-1} \frac{\langle \mathbf{u}_i, \mathbf{w}_k \rangle}{\langle \mathbf{w}_k, \mathbf{w}_k \rangle}\mathbf{w}_k \tag{7.13}$$

*for each $m + 1 \leq i \leq m + n$. Moreover,*

$$\operatorname{Span}(\mathbf{w}_i)_{i=1}^{m+k} = \operatorname{Span}(\mathbf{w}_1, \dots, \mathbf{w}_m, \mathbf{u}_{m+1}, \dots, \mathbf{u}_{m+k}) \tag{7.14}$$

*for all $1 \leq k \leq n$.*

Note that the existence of vectors $\mathbf{u}_{m+1}, \dots, \mathbf{u}_{m+n} \in V$ such that (7.12) is a basis for $V$ is assured by Theorem 3.55. Also observe that, since $m, n \in \mathbb{N}$ implies $m + n \geq 2$, the theorem does not address one-dimensional vector spaces. This is because one-dimensional vector spaces are not of much interest: any nonzero vector serves as an orthogonal basis!

**Proof.** We carry out an argument by induction on $n$ by first considering the case when $n = 1$. That is, we let $m \in \mathbb{N}$ be arbitrary, and suppose $(V, \langle\ \rangle)$ is an inner product space with $\dim(V) = m+1$, $W$ is a subspace of $V$ with orthogonal basis $(\mathbf{w}_i)_{i=1}^m$, and $\mathcal{B} = (\mathbf{w}_1, \dots, \mathbf{w}_m, \mathbf{u}_{m+1})$ is a basis for $V$. Let

$$\mathbf{w}_{m+1} = \mathbf{u}_{m+1} - \sum_{k=1}^{m} \frac{\langle \mathbf{u}_{m+1}, \mathbf{w}_k \rangle}{\langle \mathbf{w}_k, \mathbf{w}_k \rangle} \mathbf{w}_k.$$

If $\mathbf{w}_{m+1} = \mathbf{0}$, then

$$\mathbf{u}_{m+1} = \sum_{k=1}^{m} \frac{\langle \mathbf{u}_{m+1}, \mathbf{w}_k \rangle}{\langle \mathbf{w}_k, \mathbf{w}_k \rangle} \mathbf{w}_k$$

obtains, so that $\mathbf{u}_{m+1} \in \mathrm{Span}(\mathbf{w}_i)_{i=1}^m$ and by Proposition 3.39 it follows that $\mathcal{B}$ is a linearly dependent set—a contradiction. Hence $\mathbf{w}_{m+1} \neq \mathbf{0}$ is assured. Moreover $\mathbf{w}_{m+1}$ is orthogonal to $\mathbf{w}_1, \dots, \mathbf{w}_m$ by Proposition 7.10, implying that $\mathbf{w}_i \perp \mathbf{w}_j$ for all $1 \le i, j \le m+1$ such that $i \neq j$. Since $\{\mathbf{w}_1, \dots, \mathbf{w}_{m+1}\}$ is an orthogonal set of nonzero vectors, by Lemma 7.13 it is also a linearly independent set. Therefore, by Theorem 3.54, $(\mathbf{w}_i)_{i=1}^{m+1}$ is a basis for $V$ that is also an orthogonal basis. We have proven that the theorem is true in the base case when $n = 1$.

Next, suppose the theorem is true for some particular $n \in \mathbb{N}$. Fix $m \in \mathbb{N}$, suppose $(V, \langle\ \rangle)$ is an inner product space with $\dim(V) = m + n + 1$, $W$ is a subspace of $V$ with orthogonal basis $(\mathbf{w}_i)_{i=1}^m$, and

$$\mathcal{B} = (\mathbf{w}_1, \dots, \mathbf{w}_m, \mathbf{u}_{m+1}, \dots, \mathbf{u}_{m+n+1})$$

is a basis for $V$. Let $V' = \mathrm{Span}(\mathcal{B} \setminus \{\mathbf{u}_{m+n+1}\})$, which is to say $(V', \langle\ \rangle)$ is an inner product space with basis

$$\mathcal{B}' = (\mathbf{w}_1, \dots, \mathbf{w}_m, \mathbf{u}_{m+1}, \dots, \mathbf{u}_{m+n}),$$

and $W$ is a subspace of $V'$. Since $\dim(V') = m + n$, by our inductive hypothesis we conclude that $(\mathbf{w}_i)_{i=1}^{m+n}$, where

$$\mathbf{w}_i = \mathbf{u}_i - \sum_{k=1}^{i-1} \frac{\langle \mathbf{u}_i, \mathbf{w}_k \rangle}{\langle \mathbf{w}_k, \mathbf{w}_k \rangle} \mathbf{w}_k$$

for each $m + 1 \le i \le m + n$, is an orthogonal basis for $V'$.

Now, $V'$ is a subspace of $V$ with orthogonal basis $(\mathbf{w}_i)_{i=1}^{m+n}$, and

$$\mathcal{C} = (\mathbf{w}_1, \dots, \mathbf{w}_{m+n}, \mathbf{u}_{m+n+1})$$

is a basis for $V$. (To substantiate the latter claim use Proposition 3.39 twice: first to find that

$$\mathbf{u}_{m+n+1} \notin \mathrm{Span}(\mathcal{B}') = V' = \mathrm{Span}(\mathbf{w}_i)_{i=1}^{m+n},$$

and then to find that $\mathcal{C}$ is a linearly independent set. Now invoke Theorem 3.54.) Applying the base case proven above, only with $m$ replaced by $m + n$, we conclude that $(\mathbf{w}_i)_{i=1}^{m+n+1}$ is an orthogonal basis for $V$, where

$$\mathbf{w}_{m+n+1} = \mathbf{u}_{m+n+1} - \sum_{k=1}^{m+n} \frac{\langle \mathbf{u}_{m+n+1}, \mathbf{w}_k \rangle}{\langle \mathbf{w}_k, \mathbf{w}_k \rangle} \mathbf{w}_k.$$

We have now shown that if the theorem holds when $m \in \mathbb{N}$ is arbitrary and $\dim(V) = m+n$, then it holds when $m \in \mathbb{N}$ is arbitrary and $\dim(V) = m + n + 1$. All but the last statement of the theorem is now proven by the Principle of Induction.

Finally, to see that (7.14) holds for each $1 \le k \le n$, simply note from (7.13) that each vector in $(\mathbf{w}_i)_{i=1}^{m+k}$ lies in

$$\operatorname{Span}(\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_{m+1}, \ldots, \mathbf{u}_{m+k}),$$

and also each vector in

$$(\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{u}_{m+1}, \ldots, \mathbf{u}_{m+k})$$

lies in $\operatorname{Span}(\mathbf{w}_i)_{i=1}^{m+k}$. ■

**Corollary 7.15.** *If $(V, \langle\,\rangle)$ is an inner product space over $\mathbb{F}$ of dimension $n \in \mathbb{N}$, then it has an orthonormal basis.*

**Example 7.16.** Give the vector space $\mathbb{R}^3$ the customary dot product, thereby producing the inner product space $(\mathbb{R}^3, \cdot)$. Let

$$\mathbf{u}_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \quad \mathbf{u}_2 = \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{u}_3 = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}.$$

Then $\mathcal{B} = \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ is a basis for $(\mathbb{R}^3, \cdot)$. Use the Gram-Schmidt Process to transform $\mathcal{B}$ into an orthogonal basis for $(\mathbb{R}^3, \cdot)$, and then find an orthonormal basis for $(\mathbb{R}^3, \cdot)$.

**Solution.** Let $\mathbf{w}_1 = \mathbf{u}_1$. Then $\{\mathbf{w}_1\}$ is an orthogonal basis for the subspace $W = \operatorname{Span}\{\mathbf{w}_1\}$. Certainly $W \neq \mathbb{R}^3$, and we already know that $\{\mathbf{w}_1, \mathbf{u}_2, \mathbf{u}_3\}$ is a basis for $\mathbb{R}^3$. Hence we have the essential ingredients to commence the Gram-Schmidt Process and find vectors $\mathbf{w}_2$ and $\mathbf{w}_3$ so that $\{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3\}$ constitutes an orthogonal basis for $(\mathbb{R}^3, \cdot)$. The formula for finding $\mathbf{w}_i$ (where $i = 2, 3$) is

$$\mathbf{w}_i = \mathbf{u}_i - \sum_{k=1}^{i-1} \frac{\mathbf{u}_i \cdot \mathbf{w}_k}{\mathbf{w}_k \cdot \mathbf{w}_k} \mathbf{w}_k.$$

Hence

$$\mathbf{w}_2 = \mathbf{u}_2 - \frac{\mathbf{u}_2 \cdot \mathbf{w}_1}{\mathbf{w}_1 \cdot \mathbf{w}_1} \mathbf{w}_1 = \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix} - \frac{[-1,1,0]^\top \cdot [1,1,1]^\top}{[1,1,1]^\top \cdot [1,1,1]^\top} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix},$$

and

$$\begin{aligned} \mathbf{w}_3 = \mathbf{u}_3 - \sum_{k=1}^{2} \frac{\mathbf{u}_3 \cdot \mathbf{w}_k}{\mathbf{w}_k \cdot \mathbf{w}_k} \mathbf{w}_k &= \mathbf{u}_3 - \frac{\mathbf{u}_3 \cdot \mathbf{w}_1}{\mathbf{w}_1 \cdot \mathbf{w}_1} \mathbf{w}_1 - \frac{\mathbf{u}_3 \cdot \mathbf{w}_2}{\mathbf{w}_2 \cdot \mathbf{w}_2} \mathbf{w}_2 \\ &= \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} - \frac{4}{3} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/6 \\ 1/6 \\ -1/3 \end{bmatrix}. \end{aligned}$$

(Note: it should not be surprising that $\mathbf{w}_2 = \mathbf{u}_2$ since $\mathbf{u}_2$ is in fact already orthogonal to $\mathbf{w}_1$.) We have obtained

$$\{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3\} = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1/6 \\ 1/6 \\ -1/3 \end{bmatrix} \right\}$$

as an orthogonal basis for $(\mathbb{R}^3, \cdot)$.

To find an orthonormal basis all we need do is normalize the vectors $\mathbf{w}_1$, $\mathbf{w}_2$ and $\mathbf{w}_3$. We have

$$\hat{\mathbf{w}}_1 = \frac{\mathbf{w}_1}{\|\mathbf{w}_1\|} = \left[\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right]^\top, \quad \hat{\mathbf{w}}_2 = \frac{\mathbf{w}_2}{\|\mathbf{w}_2\|} = \left[-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right]^\top,$$

and

$$\hat{\mathbf{w}}_3 = \frac{\mathbf{w}_3}{\|\mathbf{w}_3\|} = \left[\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, -\frac{2}{\sqrt{6}}\right]^\top.$$

The set $\{\hat{\mathbf{w}}_1, \hat{\mathbf{w}}_2, \hat{\mathbf{w}}_3\}$ is an orthonormal basis for $(\mathbb{R}^3, \cdot)$. ■

**Example 7.17.** Recall the vector space $\mathcal{P}_2(\mathbb{R})$ of polynomial functions of degree at most 2 with coefficients in $\mathbb{R}$, which here we shall denote simply by $\mathcal{P}_2$. Define

$$\langle p, q \rangle = \int_{-1}^{1} pq$$

for all $p, q \in \mathcal{P}_2$. The verification that $(\mathcal{P}_2, \langle\,\rangle)$ is an inner product space proceeds in much the same way as Example 7.4. Apply the Gram-Schmidt Process to transform the standard basis $\mathcal{E} = \{1, x, x^2\}$ into an orthonormal basis for $(\mathcal{P}_2, \langle\,\rangle)$.

**Solution.** Let $\mathbf{w}_1 = 1$, the polynomial function with constant value 1. If $W = \operatorname{Span}\{\mathbf{w}_1\}$, then $W$ is a subspace of $\mathcal{P}_2$ such that $W \neq \mathcal{P}_2$, and $\{\mathbf{w}_1\}$ is an orthogonal basis for $W$. Starting with $\mathbf{w}_1$, we employ the Gram-Schmidt Process to obtain $\mathbf{w}_2$ and $\mathbf{w}_3$ from $\mathbf{u}_2 = x$ and $\mathbf{u}_3 = x^2$, respectively. We have

$$\mathbf{w}_2 = \mathbf{u}_2 - \frac{\langle \mathbf{u}_2, \mathbf{w}_1 \rangle}{\langle \mathbf{w}_1, \mathbf{w}_1 \rangle}\mathbf{w}_1 = x - \frac{\langle x, 1 \rangle}{\langle 1, 1 \rangle} = x - \frac{\int_{-1}^{1} x\,dx}{\int_{-1}^{1} 1\,dx} = x - \frac{0}{2} = x,$$

and

$$\begin{aligned}\mathbf{w}_3 = \mathbf{u}_3 - \frac{\langle \mathbf{u}_3, \mathbf{w}_1 \rangle}{\langle \mathbf{w}_1, \mathbf{w}_1 \rangle}\mathbf{w}_1 - \frac{\langle \mathbf{u}_3, \mathbf{w}_2 \rangle}{\langle \mathbf{w}_2, \mathbf{w}_2 \rangle}\mathbf{w}_2 &= x^2 - \frac{\langle x^2, 1 \rangle}{\langle 1, 1 \rangle} - \frac{\langle x^2, x \rangle}{\langle x, x \rangle}x \\ &= x^2 - \frac{\int_{-1}^{1} x^2\,dx}{\int_{-1}^{1} 1\,dx} - \frac{\int_{-1}^{1} x^3\,dx}{\int_{-1}^{1} x^2\,dx}x = x^2 - \tfrac{1}{3},\end{aligned}$$

and so

$$\{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3\} = \left\{1, x, x^2 - \tfrac{1}{3}\right\}$$

is an orthogonal basis for $\mathcal{P}_2$.

To find an orthonormal basis we need only normalize the vectors $\mathbf{w}_1$, $\mathbf{w}_2$ and $\mathbf{w}_3$. From

$$\|\mathbf{w}_1\| = \sqrt{\langle \mathbf{w}_1, \mathbf{w}_1 \rangle} = \sqrt{\langle 1, 1 \rangle} = \sqrt{\int_{-1}^{1} 1\,dx} = \sqrt{2},$$

$$\|\mathbf{w}_2\| = \sqrt{\langle \mathbf{w}_2, \mathbf{w}_2 \rangle} = \sqrt{\langle x, x \rangle} = \sqrt{\int_{-1}^{1} x^2\,dx} = \sqrt{\tfrac{2}{3}},$$

and

$$\|\mathbf{w}_3\| = \sqrt{\langle \mathbf{w}_3, \mathbf{w}_3 \rangle} = \sqrt{\left\langle x^2 - \tfrac{1}{3}, x^2 - \tfrac{1}{3} \right\rangle} = \sqrt{\int_{-1}^{1} \left(x^2 - \tfrac{1}{3}\right)^2 dx} = \sqrt{\tfrac{8}{45}},$$

we obtain

$$\hat{\mathbf{w}}_1 = \frac{\mathbf{w}_1}{\|\mathbf{w}_1\|} = \frac{1}{\sqrt{2}}, \quad \hat{\mathbf{w}}_2 = \frac{\mathbf{w}_2}{\|\mathbf{w}_2\|} = \frac{\sqrt{6}}{2}x, \quad \hat{\mathbf{w}}_3 = \frac{\mathbf{w}_3}{\|\mathbf{w}_3\|} = \frac{\sqrt{10}}{4}(3x^2 - 1).$$

The set $\{\hat{\mathbf{w}}_1, \hat{\mathbf{w}}_2, \hat{\mathbf{w}}_3\}$, which consists of the first three of what are known as normalized Legendre polynomials, is an orthonormal basis for $(\mathcal{P}_2, \langle\ \rangle)$. ■

**Proposition 7.18.** *Let $(V, \langle\ \rangle)$ be an inner product space over $\mathbb{F}$ of dimension $n \in \mathbb{N}$, let*

$$\mathcal{B} = \{\mathbf{w}_1, \dots, \mathbf{w}_r, \mathbf{u}_1, \dots, \mathbf{u}_s\}$$

*be an orthogonal basis for $V$, and let*

$$W = \operatorname{Span}\{\mathbf{w}_1, \dots, \mathbf{w}_r\} \quad \text{and} \quad U = \operatorname{Span}\{\mathbf{u}_1, \dots, \mathbf{u}_s\}.$$

*Then $U = W^\perp$, $W = U^\perp$, and*

$$\dim(W) + \dim(W^\perp) = \dim(V).$$

**Proof.** Let $\mathbf{u} \in U$. Then there exist scalars $x_1, \dots, x_s \in \mathbb{F}$ such that

$$\mathbf{u} = \sum_{i=1}^{s} x_i \mathbf{u}_i.$$

Let $\mathbf{w} \in W$ be arbitrary, so that

$$\mathbf{w} = \sum_{j=1}^{r} y_j \mathbf{w}_j$$

for scalars $y_1, \dots, y_r \in \mathbb{F}$. Now,

$$\begin{aligned}
\langle \mathbf{u}, \mathbf{w} \rangle &= \left\langle \sum\nolimits_{i=1}^{s} x_i \mathbf{u}_i, \mathbf{w} \right\rangle = \sum\nolimits_{i=1}^{s} x_i \langle \mathbf{u}_i, \mathbf{w} \rangle && \text{(Axiom IP2)} \\
&= \sum\nolimits_{i=1}^{s} \left( x_i \left\langle \mathbf{u}_i, \sum\nolimits_{j=1}^{r} y_j \mathbf{w}_j \right\rangle \right) \\
&= \sum\nolimits_{i=1}^{s} \left( x_i \sum\nolimits_{j=1}^{r} \langle \mathbf{u}_i, y_j \mathbf{w}_j \rangle \right) && \text{(Theorem 7.2(2))} \\
&= \sum\nolimits_{i=1}^{s} \left( x_i \sum\nolimits_{j=1}^{r} \bar{y}_j \langle \mathbf{u}_i, \mathbf{w}_j \rangle \right) && \text{(Theorem 7.2(3))}
\end{aligned}$$

Since $\mathcal{B}$ is an orthogonal basis we have $\langle \mathbf{u}_i, \mathbf{w}_j \rangle = 0$ for all $1 \le i \le s$ and $1 \le j \le r$, so that

$$\langle \mathbf{u}, \mathbf{w} \rangle = \sum_{i=1}^{s} \sum_{j=1}^{r} x_i \bar{y}_j \langle \mathbf{u}_i, \mathbf{w}_j \rangle = 0$$

and therefore $\mathbf{u} \perp \mathbf{w}$. Since $\mathbf{w} \in W$ is arbitrary, we conclude that $\mathbf{u} \in W^\perp$ and hence $U \subseteq W^\perp$.

Next, let $\mathbf{v} \in W^\perp$. Since $\mathcal{B}$ is a basis for $V$, there exist scalars $x_1, \dots, x_s, y_1, \dots, y_r \in \mathbb{F}$ such that

$$\mathbf{v} = \sum_{i=1}^{s} x_i \mathbf{u}_i + \sum_{j=1}^{r} y_j \mathbf{w}_j.$$

Fix $1 \le k \le r$. Since $y_k \mathbf{w}_k \in W$ we have

$$\langle \mathbf{v}, y_k \mathbf{w}_k \rangle = 0. \tag{7.15}$$

On the other hand, since $\langle \mathbf{u}_i, \mathbf{w}_k \rangle = 0$ for all $1 \le i \le s$, and $\langle \mathbf{w}_j, \mathbf{w}_k \rangle = 0$ for all $j \ne k$, we have

$$\langle \mathbf{v}, y_k \mathbf{w}_k \rangle = \sum_{i=1}^{s} x_i \bar{y}_k \langle \mathbf{u}_i, \mathbf{w}_k \rangle + \sum_{j=1}^{r} y_j \bar{y}_k \langle \mathbf{w}_j, \mathbf{w}_k \rangle = y_k \bar{y}_k \langle \mathbf{w}_k, \mathbf{w}_k \rangle = |y_k|^2 \langle \mathbf{w}_k, \mathbf{w}_k \rangle. \tag{7.16}$$

Combining (7.15) and (7.16) yields

$$|y_k|^2 \langle \mathbf{w}_k, \mathbf{w}_k \rangle = 0,$$

and since $\mathbf{w}_k \ne \mathbf{0}$ implies that $\langle \mathbf{w}_k, \mathbf{w}_k \rangle \ne 0$ by Axiom IP4, it follows that $y_k = 0$. We conclude, then, that

$$\mathbf{v} = \sum_{i=1}^{s} x_i \mathbf{u}_i \in U,$$

and so $W^\perp \subseteq U$. Therefore $U = W^\perp$, and by symmetry $W = U^\perp$.

Finally, since $\{\mathbf{u}_1, \dots, \mathbf{u}_s\}$ is a basis for $U$ and $\{\mathbf{w}_1, \dots, \mathbf{w}_r\}$ is a basis for $W$, we obtain

$$\dim(V) = n = r + s = \dim(W) + \dim(U) = \dim(W) + \dim(W^\perp),$$

which completes the proof. ∎

The conclusions of Proposition 7.18 in fact apply to any arbitrary subspace of an inner product space, as the next theorem establishes.

**Theorem 7.19.** *Let $W$ be a subspace of an inner product space $(V, \langle\ \rangle)$ over $\mathbb{F}$ with $\dim(V) \in \mathbb{N}$. Then*

$$(W^\perp)^\perp = W$$

*and*

$$\dim(W) + \dim(W^\perp) = \dim(V).$$

**Proof.** The proof is trivial in the case when $\dim(V) = 0$, since the only possible subspace is then $\{\mathbf{0}\}$. So suppose henceforth that $n = \dim(V) > 0$.

If $W = \{\mathbf{0}\}$, then $W^\perp = V$. Now,

$$(W^\perp)^\perp = V^\perp = \{\mathbf{0}\} = W,$$

and since $\dim(\{\mathbf{0}\}) = 0$ we have

$$\dim(V) = \dim(\{\mathbf{0}\}) + \dim(V) = \dim(W) + \dim(W^\perp)$$

If $W = V$, then $W^\perp = \{\mathbf{0}\}$ and a symmetrical argument to the one above leads to the same conclusions.

Set $m = \dim(W)$, and suppose $W \ne \{\mathbf{0}\}$ and $W \ne V$. Then $m \le n$ by Theorem 3.56(2), and $m \ne n$ by Theorem 3.56(3), so that $0 < m < n$. Since $W$ is a nontrivial vector space in its own right, by Corollary 7.15 it has an orthogonal basis $\{\mathbf{w}_1, \dots, \mathbf{w}_m\}$. Since $W \ne V$ it follows by Theorem 7.14 that there exist $\mathbf{w}_{m+1}, \dots, \mathbf{w}_n \in V$ such that $\mathcal{B} = \{\mathbf{w}_1, \dots, \mathbf{w}_n\}$ is an orthogonal basis for $V$. Observing that $W = \mathrm{Span}\{\mathbf{w}_1, \dots, \mathbf{w}_m\}$ and defining

$$U = \mathrm{Span}\{\mathbf{w}_{m+1}, \dots, \mathbf{w}_n\},$$

by Proposition 7.18 we have $U = W^\perp$, $W = U^\perp$, and

$$\dim(W) + \dim(W^\perp) = \dim(V).$$

Finally, observe that

$$(W^\perp)^\perp = U^\perp = W,$$

which finishes the proof. ■

The dimension equation in Theorem 7.19 amounts to a generalization of Proposition 4.46 from the setting of real Euclidean vector spaces (equipped specifically with the Euclidean dot product) to that of abstract inner product spaces over an arbitrary field $\mathbb{F}$.

**Example 7.20.** As a compelling application of some of the developments thus far, we give a proof that the row rank of a matrix equals its column rank that is quite different (and shorter) than the proof given in §3.6. Let $\mathbf{A} = [a_{ij}] \in \mathbb{R}^{m\times n}$.

Define the linear mapping $L : \mathbb{R}^n \to \mathbb{R}^m$ by $L(\mathbf{x}) = \mathbf{A}\mathbf{x}$, and let $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{R}^n$ be such that $\mathbf{a}_1^\top, \ldots, \mathbf{a}_m^\top$ are the row vectors of $\mathbf{A}$. Then $\text{Nul}(L)$ is a subspace of the inner product space $(\mathbb{R}^n, \cdot)$ by Proposition 4.14, and so too is $\text{Row}(\mathbf{A}) = \text{Span}\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$. Now,

$$\mathbf{x} \in \text{Nul}(L) \quad\Leftrightarrow\quad \mathbf{A}\mathbf{x} = \mathbf{0} \quad\Leftrightarrow\quad \begin{bmatrix} \mathbf{a}_1^\top\mathbf{x} \\ \vdots \\ \mathbf{a}_m^\top\mathbf{x} \end{bmatrix} = \begin{bmatrix} \mathbf{x}\cdot\mathbf{a}_1 \\ \vdots \\ \mathbf{x}\cdot\mathbf{a}_m \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \quad\Leftrightarrow\quad \mathbf{x} \perp \mathbf{a}_1, \ldots, \mathbf{x} \perp \mathbf{a}_m,$$

so that

$$\text{Nul}(L) = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \perp \mathbf{a}_i \text{ for all } 1 \le i \le m\}$$

and by Proposition 7.7 we have $\text{Nul}(L) = \text{Row}(\mathbf{A})^\perp$. By Theorem 7.19

$$\dim(\text{Row}(\mathbf{A})) + \dim(\text{Row}(\mathbf{A})^\perp) = \dim(\mathbb{R}^n),$$

whence

$$\text{row-rank}(\mathbf{A}) + \dim(\text{Nul}(L)) = n$$

and finally

$$\text{row-rank}(\mathbf{A}) = n - \dim(\text{Nul}(L)).$$

Next, by Theorem 4.37,

$$\dim(\text{Nul}(L)) + \dim(\text{Img}(L)) = \dim(\mathbb{R}^n),$$

and since $\text{Img}(L) = \text{Col}(\mathbf{A})$ by Proposition 4.35, it follows that

$$n = \dim(\mathbb{R}^n) = \dim(\text{Nul}(L)) + \dim(\text{Col}(\mathbf{A})) = \dim(\text{Nul}(L)) + \text{col-rank}(\mathbf{A})$$

and finally

$$\text{col-rank}(\mathbf{A}) = n - \dim(\text{Nul}(L)).$$

Therefore

$$\text{row-rank}(\mathbf{A}) = \text{col-rank}(\mathbf{A}) = n - \dim(\text{Nul}(L)),$$

and we're done. ■

**Proposition 7.21.** *If $W$ is a subspace of an inner product space $(V, \langle\ \rangle)$ over $\mathbb{F}$, then $V = W \oplus W^\perp$.*

**Proof.** The situation is trivial in the cases when $W = \{\mathbf{0}\}$ or $W = V$, so suppose $W$ is a subspace such that $W \neq \{\mathbf{0}\}, V$. Let $\dim(W) = m$ and $\dim(V) = n$, and note that $0 < m < n$. Since $(W, \langle\ \rangle)$ is a nontrivial inner product space, by Corollary 7.15 is has an orthogonal basis $\{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$. By Theorem 7.14 there exist $\mathbf{w}_{m+1}, \ldots, \mathbf{w}_n \in V$ such that $\mathcal{B} = \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ is an orthogonal basis for $V$, and $W^\perp = \mathrm{Span}\{\mathbf{w}_{m+1}, \ldots, \mathbf{w}_n\}$ by Proposition 7.18.

Let $\mathbf{v} \in V$. Since $\mathrm{Span}(\mathcal{B}) = V$, there exist scalars $c_1, \ldots, c_n \in \mathbb{F}$ such that

$$\mathbf{v} = \sum_{k=1}^{n} c_k \mathbf{w}_k = \sum_{k=1}^{m} c_k \mathbf{w}_k + \sum_{k=m+1}^{n} c_k \mathbf{w}_k,$$

and so $\mathbf{v} \in W + W^\perp$. Hence $V \subseteq W + W^\perp$, and since the reverse containment is obvious we have $V = W + W^\perp$.

Suppose that $\mathbf{v} \in W \cap W^\perp$. From $\mathbf{v} \in W^\perp$ we have $\mathbf{v} \perp \mathbf{w}$ for all $\mathbf{w} \in W$, and since $\mathbf{v} \in W$ it follows that $\mathbf{v} \perp \mathbf{v}$. Thus $\langle \mathbf{v}, \mathbf{v} \rangle = 0$, and so $\mathbf{v} = \mathbf{0}$ by Theorem 7.2(4). Hence $W \cap W^\perp \subseteq \{\mathbf{0}\}$, and since the reverse containment is obvious we have $W \cap W^\perp = \{\mathbf{0}\}$.

Since $V = W + W^\perp$ and $W \cap W^\perp = \{\mathbf{0}\}$, we conclude that $V = W \oplus W^\perp$. ■

**Corollary 7.22.** *If $W$ is a subspace of an inner product space $(V, \langle\ \rangle)$ over $\mathbb{F}$, then*

$$\dim(W \oplus W^\perp) = \dim(W) + \dim(W^\perp).$$

**Proof.** By Proposition 7.21 we have $V = W \oplus W^\perp$, and thus $\dim(V) = \dim(W \oplus W^\perp)$. The conclusion then follows from Theorem 7.19. ■

The corollary could also be proved quite easily by utilizing Proposition 4.36, which applies to abstract vector spaces over $\mathbb{F}$.

For the following theorem we take all vectors in $\mathbb{F}^n$ to be, as ever, $n \times 1$ column matrices (i.e. column vectors).

**Theorem 7.23.** *Let $(V, \langle\ \rangle)$ be a finite-dimensional inner product space over $\mathbb{F}$. If $\mathcal{O}$ is an ordered orthonormal basis for $V$, then*

$$\langle \mathbf{u}, \mathbf{v} \rangle = [\mathbf{v}]_{\mathcal{O}}^{*} [\mathbf{u}]_{\mathcal{O}} \tag{7.17}$$

*for all $\mathbf{u}, \mathbf{v} \in V$.*

**Proof.** The statement of the theorem is clearly true if $V = \{\mathbf{0}\}$, so assume $\dim(V) = n \in \mathbb{N}$ and set $\mathcal{O} = (\mathbf{w}_1, \ldots, \mathbf{w}_n)$. Let $\mathbf{u}, \mathbf{v} \in V$, so there exist $u_1, \ldots, u_n, v_1, \ldots, v_n \in \mathbb{F}$ such that

$$\mathbf{u} = u_1 \mathbf{w}_1 + \cdots + u_n \mathbf{w}_n \quad \text{and} \quad \mathbf{v} = v_1 \mathbf{w}_1 + \cdots + v_n \mathbf{w}_n,$$

and hence

$$[\mathbf{u}]_{\mathcal{O}} = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \quad \text{and} \quad [\mathbf{v}]_{\mathcal{O}} = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}.$$

Now, because $\mathcal{O}$ is orthonormal, $\langle \mathbf{w}_i, \mathbf{w}_j \rangle = 0$ whenever $i \neq j$, and $\langle \mathbf{w}_i, \mathbf{w}_i \rangle = \|\mathbf{w}_i\|^2 = 1$ for all $i = 1, \ldots, n$. By Definition 7.1 and Theorem 7.2 we obtain

$$\langle \mathbf{u}, \mathbf{v} \rangle = \left\langle \sum_{i=1}^{n} u_i \mathbf{w}_i, \sum_{j=1}^{n} v_j \mathbf{w}_j \right\rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} u_i \bar{v}_j \langle \mathbf{w}_i, \mathbf{w}_j \rangle$$

$$= \sum_{i=1}^{n} u_i \bar{v}_i \langle \mathbf{w}_i, \mathbf{w}_i \rangle = \sum_{i=1}^{n} u_i \bar{v}_i = [\mathbf{v}]_{\mathcal{O}}^* [\mathbf{u}]_{\mathcal{O}},$$

as desired. ∎

In the case when $\mathbb{F} = \mathbb{R}$ we find that $[\mathbf{v}]_{\mathcal{O}}^* = [\mathbf{v}]_{\mathcal{O}}^\top$, since the components of $[\mathbf{v}]_{\mathcal{O}}$ are all real numbers, and thus we readily obtain the following.

**Corollary 7.24.** *If $(V, \langle\ \rangle)$ is an inner product space over $\mathbb{R}$, and $\mathcal{O} = (\mathbf{w}_1, \ldots, \mathbf{w}_n)$ is an ordered orthonormal basis for $V$, then*

$$\langle \mathbf{u}, \mathbf{v} \rangle = [\mathbf{v}]_{\mathcal{O}}^\top [\mathbf{u}]_{\mathcal{O}}$$

*for all $\mathbf{u}, \mathbf{v} \in V$.*

In Theorem 7.23, let $\varphi_{\mathcal{O}} : V \to \mathbb{F}^n$ denote the $\mathcal{O}$-coordinate map, so that

$$\varphi_{\mathcal{O}}(\mathbf{v}) = [\mathbf{v}]_{\mathcal{O}}$$

for all $\mathbf{v} \in V$, and then (7.17) may be written as

$$\langle \mathbf{u}, \mathbf{v} \rangle = \varphi_{\mathcal{O}}(\mathbf{u}) \cdot \varphi_{\mathcal{O}}(\mathbf{v}),$$

recalling Definition 7.3. Now, if $\|\cdot\|_V$ denotes the norm in $V$ and $\|\cdot\|_{\mathbb{F}^n}$ the norm in $\mathbb{F}^n$, then

$$\|\mathbf{v}\|_V = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle} = \sqrt{\varphi_{\mathcal{O}}(\mathbf{v}) \cdot \varphi_{\mathcal{O}}(\mathbf{v})} = \|\varphi_{\mathcal{O}}(\mathbf{v})\|_{\mathbb{F}^n} \tag{7.18}$$

for all $\mathbf{v} \in V$. In fact, if $d_V$ and $d_{\mathbb{F}^n}$ are the distance functions on $V$ and $\mathbb{F}^n$, respectively, so that for any $\mathbf{u}, \mathbf{v} \in V$ and $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ we have

$$d_V(\mathbf{u}, \mathbf{v}) = \|\mathbf{u} - \mathbf{v}\|_V \quad \text{and} \quad d_{\mathbb{F}^n}(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_{\mathbb{F}^n},$$

then it follows from (7.18) that

$$d_V(\mathbf{u}, \mathbf{v}) = \|\mathbf{u} - \mathbf{v}\|_V = \|\varphi_{\mathcal{O}}(\mathbf{u} - \mathbf{v})\|_{\mathbb{F}^n} = \|\varphi_{\mathcal{O}}(\mathbf{u}) - \varphi_{\mathcal{O}}(\mathbf{v})\|_{\mathbb{F}^n} = d_{\mathbb{F}^n}(\varphi_{\mathcal{O}}(\mathbf{u}), \varphi_{\mathcal{O}}(\mathbf{v})), \tag{7.19}$$

recalling that $\varphi_{\mathcal{O}}$ is an isomorphism.

Equation (7.18) exhibits a property of the mapping $\varphi_{\mathcal{O}}$ that is called **norm-preserving**, and equation (7.19) exhibits the **distance-preserving** property of $\varphi_{\mathcal{O}}$.

**Definition 7.25.** *Let $(U, \langle\ \rangle_U)$ and $(V, \langle\ \rangle_V)$ be inner product spaces, and let $\|\cdot\|_U$ and $\|\cdot\|_V$ denote the norms on $U$ and $V$ induced by the inner products $\langle\ \rangle_U$ and $\langle\ \rangle_V$, respectively. A linear mapping $L : U \to V$ is an **isometry** if it is norm-preserving; that is,*

$$\|\mathbf{u}\|_U = \|L(\mathbf{u})\|_V$$

*for all $\mathbf{u} \in U$. If $L$ is also an isomorphism, then $(U, \langle\ \rangle_U)$ and $(V, \langle\ \rangle_V)$ are said to be **isometrically isomorphic**.*

Thus we see that the mapping $\varphi_{\mathcal{O}}$ is an isometry as well as an isomorphism, where it must not be forgotten that $\mathcal{O}$ represents an orthonormal basis for an inner product space $(V, \langle\ \rangle)$ over $\mathbb{F}$ of dimension $n \geq 1$. By Corollary 7.15 every such inner product space admits an orthonormal basis, and so must be isometrically isomorphic to $(\mathbb{F}^n, \cdot)$.

## Problems

1. Let $\mathbb{R}^2$ have the Euclidean inner product. Use the Gram-Schmidt Process to transform the basis $\{\mathbf{u}_1, \mathbf{u}_2\}$ into an orthonormal basis.
   (a) $\mathbf{u}_1 = [1, -3]^\top$, $\mathbf{u}_2 = [2, 2]^\top$.
   (b) $\mathbf{u}_1 = [1, 0]^\top$, $\mathbf{u}_2 = [3, -5]^\top$.

2. Let $\mathbb{R}^3$ have the Euclidean inner product. Use the Gram-Schmidt Process to transform the basis $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ into an orthonormal basis.
   (a) $\mathbf{u}_1 = [1, 1, 1]^\top$, $\mathbf{u}_2 = [-1, 1, 0]^\top$, $\mathbf{u}_3 = [1, 2, 1]^\top$.
   (b) $\mathbf{u}_1 = [1, 0, 0]^\top$, $\mathbf{u}_2 = [3, 7, -2]^\top$, $\mathbf{u}_3 = [0, 4, 1]^\top$.

3. Let $\mathbb{R}^4$ have the Euclidean inner product. Use the Gram-Schmidt Process to transform the basis $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4\}$ into an orthonormal basis:

$$\mathbf{u}_1 = \begin{bmatrix} 0 \\ 2 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{u}_2 = \begin{bmatrix} 1 \\ -1 \\ 0 \\ 0 \end{bmatrix}, \quad \mathbf{u}_3 = \begin{bmatrix} 1 \\ 2 \\ 0 \\ -1 \end{bmatrix}, \quad \mathbf{u}_4 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

4. Let $W$ be the subspace of $\mathbb{R}^4$ spanned by the vectors

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 3 \\ 0 \\ 2 \\ 0 \end{bmatrix}, \quad \mathbf{v}_3 = \begin{bmatrix} 2 \\ 1 \\ -1 \\ 3 \end{bmatrix}.$$

   (a) Beginning with the vector $\mathbf{v}_1$, use the Gram-Schmidt Orthogonalization Process to obtain an orthogonal basis for $W$.
   (b) Find an orthonormal basis for $W$.

5. Consider the matrix

$$\mathbf{A} = \begin{bmatrix} 1 & 2 & 5 \\ -1 & 1 & -4 \\ -1 & 4 & -3 \\ 1 & -4 & 7 \\ 1 & 2 & 1 \end{bmatrix}.$$

   Let $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$ denote the column vectors of $\mathbf{A}$.
   (a) Show that $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ is a basis for $\mathrm{Col}(\mathbf{A})$.
   (b) Find an orthogonal basis for $\mathrm{Col}(\mathbf{A})$.
   (c) Find an orthonormal basis for $\mathrm{Col}(\mathbf{A})$.

(d) Letting $\mathbf{r}_1, \ldots, \mathbf{r}_5 \in \mathbb{R}^3$ denote the row vectors of $\mathbf{A}$, find a basis for $\text{Row}(\mathbf{A})$ of the form $\mathcal{R} = \{\mathbf{r}_1^\top, \mathbf{r}_i^\top, \mathbf{r}_j^\top\}$, where $1 < i < j \leq 5$ are such that $i$ and $j$ are as small as possible.[7]

(e) Use the basis $\mathcal{R}$ found in part (d) to obtain an orthogonal basis for $\text{Row}(\mathbf{A})$.

(f) Find an orthonormal basis for $\text{Row}(\mathbf{A})$.

[7] This ensures that there is only one possible answer.

## 7.4 – Quadratic Forms

Recall from §7.1 that the vector space $\mathbb{C}^n$ together with the operation given by

$$\mathbf{w} \cdot \mathbf{z} = \mathbf{z}^* \mathbf{w}$$

for $\mathbf{w}, \mathbf{z} \in \mathbb{C}^n$ is an inner product space over $\mathbb{C}$ (and the product itself is called the hermitian inner product). For the conjugate transpose operation $\mathbf{z}^* = \overline{\mathbf{z}}^\top$ we find that if $\mathbf{z}$ has only real-valued entries (so that $\mathbf{z} \in \mathbb{R}^n$) then $\mathbf{z}^* = \mathbf{z}^\top$. The norm of $\mathbf{z}$ is

$$\|\mathbf{z}\| = \sqrt{\mathbf{z} \cdot \mathbf{z}} = \sqrt{\mathbf{z}^* \mathbf{z}}. \tag{7.20}$$

For the statement and proof of the next theorem recall that the standard form for elements of $\mathbb{C}^n$ is $\mathbf{x} + i\mathbf{y}$, where $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. In particular if $z = x + iy \in \mathbb{C}$ for $x, y \in \mathbb{R}$, then $\overline{z} = z$ implies $z$ is real:

$$\overline{z} = z \quad \Rightarrow \quad x - iy = x + iy \quad \Rightarrow \quad 2iy = 0 \quad \Rightarrow \quad y = 0 \quad \Rightarrow \quad z = x.$$

**Theorem 7.26.** *All eigenvalues of a real symmetric matrix* $\mathbf{A}$ *are real, and if* $\mathbf{x} + i\mathbf{y} \in \mathbb{C}^n$ *is a complex eigenvector corresponding to* $\lambda$*, then either* $\mathbf{x}$ *or* $\mathbf{y}$ *is a real eigenvector corresponding to* $\lambda$*.*

**Proof.** Suppose $\mathbf{A} \in \mathrm{Sym}_n(\mathbb{R})$, so $\overline{\mathbf{A}} = \mathbf{A}$ since $\mathbf{A}$ is real and $\mathbf{A}^\top = \mathbf{A}$ since $\mathbf{A}$ is symmetric, and thus $\mathbf{A}^* = \mathbf{A}$. Let $\lambda$ be an eigenvalue of $\mathbf{A}$ with corresponding eigenvector $\mathbf{z} \in \mathbb{C}^n$, so $\mathbf{z} \neq \mathbf{0}$ is such that $\mathbf{A}\mathbf{z} = \lambda\mathbf{z}$. Now,

$$\mathbf{z}^* \mathbf{A} \mathbf{z} = \mathbf{z}^* \lambda \mathbf{z} = \lambda(\mathbf{z}^* \mathbf{z}) = \lambda \|\mathbf{z}\|^2,$$

and since $\|\mathbf{z}\| > 0$ by Axiom IP4, we may write

$$\lambda = \frac{\mathbf{z}^* \mathbf{A} \mathbf{z}}{\|\mathbf{z}\|^2}.$$

As a $1 \times 1$ matrix $\overline{\lambda}$ is symmetric, so that

$$\overline{\lambda} = (\overline{\lambda})^\top = \lambda^* = \left( \frac{\mathbf{z}^* \mathbf{A} \mathbf{z}}{\|\mathbf{z}\|^2} \right)^* = \frac{\mathbf{z}^* \mathbf{A}^* (\mathbf{z}^*)^*}{\|\mathbf{z}\|^2} = \frac{\mathbf{z}^* \mathbf{A} \mathbf{z}}{\|\mathbf{z}\|^2} = \lambda,$$

and hence $\lambda$ is real.

Next, $\mathbf{z} \in \mathbb{C}^n$ implies $\mathbf{z} = \mathbf{x} + i\mathbf{y}$ for $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, and then from $\mathbf{A}\mathbf{z} = \lambda\mathbf{z}$ we obtain

$$\mathbf{A}\mathbf{x} + i\mathbf{A}\mathbf{y} = \lambda\mathbf{x} + i\lambda\mathbf{y}.$$

Since the entries of $\mathbf{A}$ are real and $\lambda$ is real, it follows that

$$\mathbf{A}\mathbf{x} = \lambda\mathbf{x} \quad \text{and} \quad \mathbf{A}\mathbf{y} = \lambda\mathbf{y}.$$

Now, because $\mathbf{z} \neq \mathbf{0}$, either $\mathbf{x} \neq \mathbf{0}$ or $\mathbf{y} \neq \mathbf{0}$. Therefore either $\mathbf{x}$ or $\mathbf{y}$ is a real eigenvector of $\mathbf{A}$ corresponding to $\lambda$. ∎

Let $a_{ij} \in \mathbb{R}$ for all $1 \leq i, j \leq n$. A function $f : \mathbb{R}^n \to \mathbb{R}$ given by

$$f(\mathbf{x}) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j. \tag{7.21}$$

for each $\mathbf{x} = [x_1, \ldots, x_n]^\top$ is called a **quadratic form** on $\mathbb{R}^n$. An example of a quadratic form on $\mathbb{R}^2$ is

$$f(x, y) = 2x^2 + 10xy - 2y^2.$$

Letting

$$\mathbf{x} = \begin{bmatrix} x \\ y \end{bmatrix} \quad \text{and} \quad \mathbf{A} = \begin{bmatrix} 2 & 5 \\ 5 & -2 \end{bmatrix},$$

it is easy to check that $f(\mathbf{x}) = \mathbf{x}^\top \mathbf{A}\mathbf{x}$ if we identify the $1 \times 1$ matrix $\mathbf{x}^\top \mathbf{A}\mathbf{x}$ with its scalar entry. The fact that $\mathbf{A}$ is a symmetric real matrix here is not an accident: any quadratic form on $\mathbb{R}^n$ may be written in the form $\mathbf{x}^\top \mathbf{A}\mathbf{x}$ for some $\mathbf{A} \in \mathrm{Sym}_n(\mathbb{R})$.

**Definition 7.27.** *If $\mathbf{A} \in \mathrm{Sym}_n(\mathbb{R})$, then the **quadratic form associated with** $\mathbf{A}$ is the function $Q_{\mathbf{A}} : \mathbb{R}^n \to \mathbb{R}$ given by*

$$Q_{\mathbf{A}}(\mathbf{x}) = \mathbf{x}^\top \mathbf{A}\mathbf{x}$$

*for all $\mathbf{x} \in \mathbb{R}^n$.*

Again we note that, formally, $\mathbf{x}^\top \mathbf{A}\mathbf{x}$ is a $1 \times 1$ matrix, but the natural isomorphism $[c] \mapsto c$ is implicitly in play in Definition 7.27 so that $Q_{\mathbf{A}}(\mathbf{x})$ is a real number.

**Example 7.28.** Any quadratic form in $\mathbb{R}^2$ may be written as

$$f(x, y) = ax^2 + 2bxy + cy^2$$

for $a, b, c \in \mathbb{R}$. We wish to find a real symmetric $2 \times 2$ matrix $\mathbf{A}$ such that $Q_{\mathbf{A}} = f$ on $\mathbb{R}^2$. We have

$$\begin{aligned} f(x, y) &= (ax^2 + bxy) + (bxy + cy^2) = (ax + by)x + (bx + cy)y \\ &= \begin{bmatrix} ax + by & bx + cy \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b \\ b & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}, \end{aligned}$$

which shows that $f$ is the quadratic form associated with

$$\mathbf{A} = \begin{bmatrix} a & b \\ b & c \end{bmatrix}.$$

■

**Example 7.29.** Let

$$\mathbf{A} = \begin{bmatrix} 3 & -1 & 2 \\ -1 & 1 & 4 \\ 2 & 4 & -2 \end{bmatrix} \quad \text{and} \quad \mathbf{x} = \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

Then

$$Q_{\mathbf{A}}(\mathbf{x}) = \begin{bmatrix} x & y & z \end{bmatrix} \begin{bmatrix} 3 & -1 & 2 \\ -1 & 1 & 4 \\ 2 & 4 & -2 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x & y & z \end{bmatrix} \begin{bmatrix} 3x - y + 2z \\ -x + y + 4z \\ 2x + 4y - 2z \end{bmatrix}$$

$$= x(3x - y + 2z) + y(-x + y + 4z) + z(2x + 4y - 2z)$$
$$= 3x^2 - 2xy + 4xz + y^2 + 8yz - 2z^2$$

is the quadratic form associated with $\mathbf{A}$.

More generally, if

$$\mathbf{A} = \begin{bmatrix} a & b & c \\ b & d & e \\ c & e & f \end{bmatrix}$$

then

$$Q_{\mathbf{A}}(\mathbf{x}) = ax^2 + 2bxy + 2cxz + dy^2 + 2eyz + fz^2 \tag{7.22}$$

is the associated quadratic form. ■

For $n \in \mathbb{N}$ define $\mathbb{S}^n$ to be the set of all unit vectors in the vector space $\mathbb{R}^{n+1}$ with respect to the Euclidean dot product:

$$\mathbb{S}^n = \{\mathbf{x} \in \mathbb{R}^{n+1} : \|\mathbf{x}\| = 1\} = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_{n+1} \end{bmatrix} \in \mathbb{R}^{n+1} : \sum_{k=1}^{n+1} x_k^2 = 1 \right\}.$$

The set $\mathbb{S}^n$ may be referred to as the ***n*-sphere** or the ($n$-dimensional) **unit sphere**.[8] If $n = 1$ we obtain a circle centered at $\langle 0, 0 \rangle$,

$$\mathbb{S}^1 = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2 : x^2 + y^2 = 1 \right\},$$

and if $n = 2$ we obtain a sphere with center $\langle 0, 0, 0 \rangle$,

$$\mathbb{S}^2 = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^2 : x^2 + y^2 + z^2 = 1 \right\}.$$

The next proposition establishes an important property of the quadratic forms of symmetric matrices that have, in particular, *real-valued* entries. It depends on a fact from analysis, not proven here, that if $f : S \subseteq \mathbb{R}^n \to \mathbb{R}$ is a continuous function and $S$ is a closed and bounded set, then $f$ attains a maximum value on $S$. That is, there exists some $\mathbf{x}_0 \in S$ such that

$$f(\mathbf{x}_0) = \max\{f(\mathbf{x}) : \mathbf{x} \in S\}.$$

Certainly $\mathbb{S}^{n-1}$, as a subset of $\mathbb{R}^n$, is closed and bounded with respect to the Euclidean dot product. Also a cursory examination of (7.21) should make it clear that, for any $\mathbf{A} \in \mathbb{R}^{n \times n}$, the function $Q_{\mathbf{A}}$ is a polynomial function. Hence $Q_{\mathbf{A}}$ is continuous on $\mathbb{R}^n$ with respect to the Euclidean dot product, which easily implies that $Q_{\mathbf{A}}$ is continuous on $\mathbb{S}^{n-1} \subseteq \mathbb{R}^n$.

[8] It makes no difference whether we regard the elements of $\mathbb{S}^n$ as vectors or points. For consistency's sake we keep on with the "vector interpretation" here, but later will make occasional use of the "point interpretation" to aid intuitive understanding.

**Definition 7.30.** *Let $U \subseteq \mathbb{R}$ be an open set, and let $\mathbf{f} : U \to \mathbb{R}^n$ be given by*

$$\mathbf{f}(t) = \begin{bmatrix} f_1(t) \\ \vdots \\ f_n(t) \end{bmatrix},$$

*where $f_k : U \to \mathbb{R}$ for each $1 \le k \le n$. If the derivatives $f_1'(t_0), \dots, f_n'(t_0)$ are defined at $t_0 \in U$, then the **derivative** of the vector-valued function $\mathbf{f}$ at $t_0$ is*

$$\mathbf{f}'(t_0) = \begin{bmatrix} f_1'(t_0) \\ \vdots \\ f_n'(t_0) \end{bmatrix}.$$

Since all the eigenvalues of a symmetric real matrix $\mathbf{A}$ are real by Theorem 7.26, it makes sense to speak of the "smallest" and "largest" eigenvalue of $\mathbf{A}$, as in the next theorem.

**Theorem 7.31.** *Suppose $\mathbf{A} \in \mathrm{Sym}_n(\mathbb{R})$, and let $\lambda_{\min}$ and $\lambda_{\max}$ be the smallest and largest eigenvalues of $\mathbf{A}$, respectively.*

1. *If*
$$Q_{\mathbf{A}}(\mathbf{v}_1) = \max\{Q_{\mathbf{A}}(\mathbf{x}) : \mathbf{x} \in \mathbb{S}^{n-1}\} \quad \text{and} \quad Q_{\mathbf{A}}(\mathbf{v}_2) = \min\{Q_{\mathbf{A}}(\mathbf{x}) : \mathbf{x} \in \mathbb{S}^{n-1}\},$$
*then $\mathbf{v}_1$ and $\mathbf{v}_2$ are eigenvectors of $\mathbf{A}$.*
2. *For all $\mathbf{x} \in \mathbb{S}^{n-1}$,*
$$\lambda_{\min} \le \mathbf{x}^\top \mathbf{A}\mathbf{x} \le \lambda_{\max}.$$
3. *For $\mathbf{x} \in \mathbb{R}^n$ such that $\|\mathbf{x}\| = 1$, $\mathbf{x}^\top \mathbf{A}\mathbf{x} = \lambda_{\max}$ (resp. $\lambda_{\min}$) iff $\mathbf{x}$ is an eigenvector of $\mathbf{A}$ corresponding to $\lambda_{\max}$ (resp. $\lambda_{\min}$).*

**Proof.**
*Proof of (1).* Define $U \subseteq \mathbb{R}^n$ to be the set

$$U = \{\mathbf{u} \in \mathbb{R}^n : \mathbf{u} \cdot \mathbf{v}_1 = 0\}.$$

Since $\|\mathbf{v}_1\| = 1$ implies that $\mathbf{v}_1 \ne \mathbf{0}$, by Example 4.39 we find that $U$ is a subspace of $\mathbb{R}^n$ and $\dim(U) = n - 1$. By Proposition 4.46

$$\dim(U^\perp) = \dim(\mathbb{R}^n) - \dim(U) = n - (n-1) = 1,$$

and since clearly $\mathbf{v}_1 \in U^\perp$ and $\{\mathbf{v}_1\}$ is a linearly independent set, it follows by Theorem 3.54(1) that $\{\mathbf{v}_1\}$ is a basis for $U^\perp$. Hence

$$U^\perp = \mathrm{Span}(\mathbf{v}_1) = \{c\mathbf{v}_1 : c \in \mathbb{R}\}.$$

Fix $\mathbf{u} \in U$ such that $\|\mathbf{u}\| = 1$, and define the vector-valued function $\mathbf{f} : \mathbb{R} \to \mathbb{R}^n$ by

$$\mathbf{f}(t) = \sin(t)\mathbf{u} + \cos(t)\mathbf{v}_1.$$

Since $\mathbf{v}_1 \cdot \mathbf{v}_1 = \|\mathbf{v}_1\|^2 = 1$, $\mathbf{u} \cdot \mathbf{u} = \|\mathbf{u}\|^2 = 1$, and $\mathbf{u} \cdot \mathbf{v}_1 = 0$, we find that

$$\begin{aligned} \|\mathbf{f}(t)\|^2 = \mathbf{f}(t) \cdot \mathbf{f}(t) &= \big(\sin(t)\mathbf{u} + \cos(t)\mathbf{v}_1\big) \cdot \big(\sin(t)\mathbf{u} + \cos(t)\mathbf{v}_1\big) \\ &= \sin^2(t)\mathbf{u} \cdot \mathbf{u} + 2\cos(t)\sin(t)\mathbf{u} \cdot \mathbf{v}_1 + \cos^2(t)\mathbf{v}_1 \cdot \mathbf{v}_1 \end{aligned}$$

$$= \sin^2(t) + \cos^2(t) = 1,$$

and so $\mathbf{f}(t) \in \mathbb{S}^{n-1}$ for all $t \in \mathbb{R}$. That is, the function $\mathbf{f}$ can be regarded as defining a curve on the unit sphere $\mathbb{S}^{n-1}$, and $\mathbf{f}(0) = \mathbf{v}_1$ shows that the curve passes through the point $\mathbf{v}_1$. Letting

$$\mathbf{u} = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \quad \text{and} \quad \mathbf{v}_1 = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$$

we have

$$\mathbf{f}(t) = \begin{bmatrix} u_1 \sin(t) + v_1 \cos(t) \\ \vdots \\ u_n \sin(t) + v_n \cos(t) \end{bmatrix},$$

and so by definition

$$\mathbf{f}'(t) = \begin{bmatrix} u_1 \cos(t) - v_1 \sin(t) \\ \vdots \\ u_n \cos(t) - v_n \sin(t) \end{bmatrix} = \cos(t)\mathbf{u} - \sin(t)\mathbf{v}_1.$$

Now, letting $g = Q_{\mathbf{A}} \circ \mathbf{f}$ and defining the function $\mathbf{Af}$ by $(\mathbf{Af})(t) = \mathbf{Af}(t)$ for $t \in \mathbb{R}$, we have

$$g(t) = Q_{\mathbf{A}}(\mathbf{f}(t)) = \mathbf{f}(t)^\top \mathbf{Af}(t) = \mathbf{f}(t) \cdot \mathbf{Af}(t) = \mathbf{f}(t) \cdot (\mathbf{Af})(t).$$

By the Product Rule of dot product differentiation,

$$\begin{aligned} g'(t) &= \mathbf{f}'(t) \cdot (\mathbf{Af})(t) + \mathbf{f}(t) \cdot (\mathbf{Af})'(t) = \mathbf{f}'(t) \cdot \mathbf{Af}(t) + \mathbf{f}(t) \cdot \mathbf{Af}'(t) \\ &= \mathbf{f}'(t)^\top \mathbf{Af}(t) + \mathbf{f}(t)^\top \mathbf{Af}'(t). \end{aligned} \tag{7.23}$$

Since $\mathbf{f}(t)^\top \mathbf{Af}'(t)$ is a scalar it equals its own transpose, and so by Proposition 2.13 and the fact that $\mathbf{A}^\top = \mathbf{A}$ we obtain

$$\mathbf{f}(t)^\top \mathbf{Af}'(t) = \big(\mathbf{f}(t)^\top \mathbf{Af}'(t)\big)^\top = \mathbf{f}'(t)^\top \mathbf{A}^\top \mathbf{f}(t) = \mathbf{f}'(t)^\top \mathbf{Af}(t).$$

Combining this result with (7.23) yields

$$g'(t) = 2\mathbf{f}'(t)^\top \mathbf{Af}(t). \tag{7.24}$$

Because the function $\mathbf{f}$ maps from $\mathbb{R}$ to $\mathbb{S}^{n-1}$, the function $Q_{\mathbf{A}} : \mathbb{S}^{n-1} \to \mathbb{R}$ has a maximum at $\mathbf{v}_1 \in \mathbb{S}^{n-1}$, and

$$g(0) = Q_{\mathbf{A}}(\mathbf{f}(0)) = Q_{\mathbf{A}}(\mathbf{v}_1),$$

it follows that the function $g : \mathbb{R} \to \mathbb{R}$ has a local maximum at $t = 0$. Thus, since $g'(0)$ exists, it further follows by Fermat's Theorem in §4.1 of the *Calculus Notes* that $g'(0) = 0$. From (7.24) we have

$$\mathbf{u} \cdot \mathbf{Av}_1 = \mathbf{u}^\top \mathbf{Av}_1 = \mathbf{f}'(0)^\top \mathbf{Af}(0) = 0,$$

and since $\mathbf{u} \in U$ is arbitrary we conclude that $\mathbf{Av}_1 \perp \mathbf{u}$ for all $\mathbf{u} \in U$. Therefore

$$\mathbf{Av}_1 \in U^\perp = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \perp \mathbf{u} \text{ for all } \mathbf{u} \in U\} = \mathrm{Span}(\mathbf{v}_1),$$

and so there must exist some $\lambda \in \mathbb{R}$ such that $\mathbf{Av}_1 = \lambda \mathbf{v}_1$. Since $\mathbf{v}_1 \in \mathbb{R}^n$ is nonzero, we conclude that $\mathbf{v}_1$ is an eigenvector of $\mathbf{A}$. The proof that $\mathbf{v}_2 \in \mathbb{S}^{n-1}$ is also an eigenvector of $\mathbf{A}$ is much the same.

*Proof of (2).* By the previous result, letting $\lambda_1$ (resp. $\lambda_2$) be the eigenvalue of $\mathbf{A}$ corresponding to $\mathbf{v}_1$ (resp. $\mathbf{v}_2$), we have

$$\mathbf{x}^\top \mathbf{A}\mathbf{x} = Q_{\mathbf{A}}(\mathbf{x}) \le Q_{\mathbf{A}}(\mathbf{v}_1) = \mathbf{v}_1^\top \mathbf{A}\mathbf{v}_1 = \mathbf{v}_1^\top(\lambda_1 \mathbf{v}_1) = \lambda_1(\mathbf{v}_1^\top \mathbf{v}_1) = \lambda_1 \le \lambda_{\max}$$

and

$$\mathbf{x}^\top \mathbf{A}\mathbf{x} = Q_{\mathbf{A}}(\mathbf{x}) \ge Q_{\mathbf{A}}(\mathbf{v}_2) = \mathbf{v}_2^\top \mathbf{A}\mathbf{v}_2 = \mathbf{v}_2^\top(\lambda_2 \mathbf{v}_2) = \lambda_2(\mathbf{v}_2^\top \mathbf{v}_2) = \lambda_2 \ge \lambda_{\min}$$

for any $\mathbf{x} \in \mathbb{S}^{n-1}$.

*Proof of (3).* We provide only the proof of the statement concerning $\lambda_{\max}$, since the proof of the other statement is similar. Let $\mathbf{x} \in \mathbb{R}^n$ be such that $\|\mathbf{x}\| = 1$.

Suppose $\mathbf{x}^\top \mathbf{A}\mathbf{x} = \lambda_{\max}$. Then

$$Q_{\mathbf{A}}(\mathbf{x}) = \max\{Q_{\mathbf{A}}(\mathbf{u}) : \mathbf{u} \in \mathbb{S}^{n-1}\}$$

by part (2), and it follows by part (1) that $\mathbf{x}$ is an eigenvector of $\mathbf{A}$. Let $\lambda$ be the eigenvalue of $\mathbf{A}$ corresponding to $\mathbf{x}$. We now have

$$\lambda_{\max} = \mathbf{x}^\top \mathbf{A}\mathbf{x} = \mathbf{x}^\top(\lambda \mathbf{x}) = \lambda \mathbf{x}^\top \mathbf{x} = \lambda,$$

and so $\mathbf{x}$ is an eigenvector of $\mathbf{A}$ corresponding to $\lambda_{\max}$.

For the converse, suppose $\mathbf{x}$ is an eigenvector of $\mathbf{A}$ corresponding to $\lambda_{\max}$. Then

$$\mathbf{x}^\top \mathbf{A}\mathbf{x} = \mathbf{x}^\top(\lambda_{\max}\mathbf{x}) = \lambda_{\max}\mathbf{x}^\top \mathbf{x} = \lambda_{\max},$$

and the proof is done. ■

**Example 7.32.** Find the maximum and minimum value of the function $\varphi : \mathbb{R}^3 \to \mathbb{R}$ given by

$$\varphi(x, y, z) = x^2 - 4xy + 4y^2 - 4yz + z^2 \tag{7.25}$$

on the unit sphere $\mathbb{S}^2$.

**Solution.** Comparing (7.25) to equation (7.22) in Example 7.29, we see we have $a = 1$, $b = -2$, $c = 0$, $d = 4$, $e = -2$, and $f = 1$. Thus the function $\varphi$ is the quadratic form associated with the matrix

$$\mathbf{A} = \begin{bmatrix} a & b & c \\ b & d & e \\ c & e & f \end{bmatrix} = \begin{bmatrix} 1 & -2 & 0 \\ -2 & 4 & -2 \\ 0 & -2 & 1 \end{bmatrix}.$$

The characteristic polynomial of $\mathbf{A}$ is

$$\begin{aligned} P_{\mathbf{A}}(t) = \det(\mathbf{A} - t\mathbf{I}_3) &= \begin{vmatrix} 1-t & -2 & 0 \\ -2 & 4-t & -2 \\ 0 & -2 & 1-t \end{vmatrix} \\ &= (-1)^{1+1}(1-t)\begin{vmatrix} 4-t & -2 \\ -2 & 1-t \end{vmatrix} + (-1)^{1+2}(-2)\begin{vmatrix} -2 & -2 \\ 0 & 1-t \end{vmatrix} \\ &= -t^3 + 6t^2 - t - 4, \end{aligned}$$

and so

$$P_{\mathbf{A}}(t) = 0 \quad \Leftrightarrow \quad t^3 - 6t^2 + t + 4 = 0.$$

By the Rational Zeros Theorem of algebra, the only rational numbers that may be zeros of $P_{\mathbf{A}}$ are $\pm 1$, $\pm 2$, and $\pm 4$. It happens that 1 is in fact a zero, and so by the Factor Theorem of algebra $t - 1$ must be a factor of $P_{\mathbf{A}}(t)$. Now,

$$\frac{t^3 - 6t^2 + t + 4}{t - 1} = t^2 - 5t - 4,$$

whence we obtain

$$P_{\mathbf{A}}(t) = 0 \quad \Rightarrow \quad (t-1)(t^2 - 5t - 4) = 0 \quad \Rightarrow \quad t = 1 \quad \text{or} \quad t^2 - 5t - 4 = 0,$$

and so $P_{\mathbf{A}}(t) = 0$ implies that

$$t \in \left\{ \frac{5 + \sqrt{41}}{2}, \frac{5 - \sqrt{41}}{2}, 1 \right\}.$$

By Theorem 6.18 the eigenvalues of $\mathbf{A}$ are

$$\lambda_1 = \frac{5 + \sqrt{41}}{2}, \quad \lambda_2 = \frac{5 - \sqrt{41}}{2}, \quad \lambda_3 = 1,$$

so by Theorem 7.31 the maximum value of $\varphi$ on $\mathbb{S}^2$ is $\lambda_1$ (approximately 5.702) and the minimum value is $\lambda_2$ (approximately $-0.702$). ∎

**Example 7.33.** Find the maximum and minimum value of the function

$$f(x, y) = x^2 + xy + 2y^2$$

on the ellipse $x^2 + 3y^2 = 16$.

**Solution.** We effect a change of variables so that, in terms of the new variables, the ellipse becomes a unit circle. In particular we declare $u$ and $v$ to be such that $4u = x$ and $4v/\sqrt{3} = y$.

# 8

# Operator Theory

## 8.1 – The Adjoint of a Linear Operator

Many of the results developed in this chapter are of a technical nature which will be pressed into service in due course to uncover some of the most wondrous and practical properties of finite-dimensional vector spaces and the linear mappings between them.

**Definition 8.1.** *Let $(V, \langle\,\rangle_V)$ and $(W, \langle\,\rangle_W)$ be inner product spaces over the field $\mathbb{F}$, and let $L \in \mathcal{L}(V, W)$. The* ***adjoint*** *of $L$ is the mapping $L^* \in \mathcal{L}(W, V)$ satisfying*

$$\langle L(\mathbf{v}), \mathbf{w}\rangle_W = \langle \mathbf{v}, L^*(\mathbf{w})\rangle_V$$

*for all $\mathbf{v} \in V$ and $\mathbf{w} \in W$.*

**Theorem 8.2.** *Let $(V, \langle\,\rangle_V)$ and $(W, \langle\,\rangle_W)$ be inner product spaces over $\mathbb{F}$. For every $L \in \mathcal{L}(V, W)$ there exists a unique adjoint $L^* \in \mathcal{L}(W, V)$.*

Given an inner product space $(V, \langle\,\rangle)$ and an operator $L \in \mathcal{L}(V)$, the adjoint of $L$ is the unique operator $L^* \in \mathcal{L}(V)$ satisfying

$$\langle L(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, L^*(\mathbf{v})\rangle \tag{8.1}$$

for all $\mathbf{u}, \mathbf{v} \in V$.

**Proposition 8.3.** *Let $(V, \langle\,\rangle)$ be an inner product space over $\mathbb{F}$. If $L, \hat{L} \in \mathcal{L}(V)$ and $c \in \mathbb{F}$, then*

1. $(cL)^* = \bar{c}L^*$
2. $(L^*)^* = L$
3. $(L + \hat{L})^* = L^* + \hat{L}^*$
4. $(L \circ \hat{L})^* = \hat{L}^* \circ L^*$

**Proof.**
*Proof of Part (2).* Let $\mathbf{u}, \mathbf{v} \in V$ be arbitrary. By definition we have

$$\langle L(\mathbf{v}), \mathbf{u}\rangle = \langle \mathbf{v}, L^*(\mathbf{u})\rangle,$$

and thus

$$\langle L^*(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, L(\mathbf{v})\rangle.$$

This shows that $L$ is the adjoint of $L^*$; that is, $L = (L^*)^*$.

*Proof of Part (4).* Let $\mathbf{u}, \mathbf{v} \in V$. By definition

$$\big\langle (L \circ \hat{L})(\mathbf{u}), \mathbf{v}\big\rangle = \big\langle \mathbf{u}, (L \circ \hat{L})^*(\mathbf{v})\big\rangle \tag{8.2}$$

and

$$\langle \hat{L}(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, \hat{L}^*(\mathbf{v})\rangle. \tag{8.3}$$

Substituting $\hat{L}(\mathbf{u})$ for $\mathbf{u}$ in (8.1), and $L^*(\mathbf{v})$ for $\mathbf{v}$ in (8.3), we obtain

$$\big\langle L(\hat{L}(\mathbf{u})), \mathbf{v}\big\rangle = \langle \hat{L}(\mathbf{u}), L^*(\mathbf{v})\rangle \quad \text{and} \quad \langle \hat{L}(\mathbf{u}), L^*(\mathbf{v})\rangle = \big\langle \mathbf{u}, \hat{L}^*(L^*(\mathbf{v}))\big\rangle,$$

and hence

$$\big\langle (L \circ \hat{L})(\mathbf{u}), \mathbf{v}\big\rangle = \big\langle \mathbf{u}, (\hat{L}^* \circ L^*)(\mathbf{v})\big\rangle.$$

Comparing this equation with (8.2), and recalling that $\mathbf{u}, \mathbf{v} \in V$ are arbitrary, we see that both $(L \circ \hat{L})^*$ and $\hat{L}^* \circ L^*$ are adjoints of $L \circ \hat{L}$. Since the adjoint of a linear operator is unique, we conclude that

$$(L \circ \hat{L})^* = \hat{L}^* \circ L^*$$

as desired.

Proofs of the other parts of the proposition are left as exercises. ■

**Definition 8.4.** *Let* $\mathbf{A} \in \mathbb{F}^{m\times n}$. *The* ***adjoint*** *(or* ***conjugate transpose****) of* $\mathbf{A}$ *is the matrix* $\mathbf{A}^* \in \mathbb{F}^{n\times m}$ *given by* $\mathbf{A}^* = \big(\overline{\mathbf{A}}\big)^\top$.

If $\mathbf{A} = [\mathbf{a}_{ij}]_{m\times n}$, then the $ij$-entry of $\mathbf{A}^*$ is $[\mathbf{A}^*]_{ij} = \overline{\mathbf{a}}_{ji}$. It is an easy matter to verify that

$$\big(\overline{\mathbf{A}}\big)^\top = \overline{(\mathbf{A}^\top)}$$

(that is, the transpose of $\overline{\mathbf{A}}$ is the same as the conjugate of $\mathbf{A}^\top$), so there would be no ambiguity if we were to write simply $\overline{\mathbf{A}}^T$. Hence,

$$\mathbf{A}^* = \overline{\mathbf{A}}^\top = \overline{(\mathbf{A}^\top)} = \big(\overline{\mathbf{A}}\big)^\top. \tag{8.4}$$

Also we define

$$\mathbf{A}^{**} = (\mathbf{A}^*)^*.$$

**Proposition 8.5.** *If* $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{n\times n}$ *and* $c \in \mathbb{F}$, *then*

1. $(c\mathbf{A})^* = \bar{c}\mathbf{A}^*$
2. $\mathbf{A}^{**} = \mathbf{A}$
3. $(\mathbf{A} + \mathbf{B})^* = \mathbf{A}^* + \mathbf{B}^*$
4. $(\mathbf{AB})^* = \mathbf{B}^*\mathbf{A}^*$

**Proof.**
*Proof of Part (2).* Liberal use of equation (8.4) is prescribed here, as well as properties of the transpose and conjugation operations established in chapters 2 and 6, respectively. We have $\mathbf{A}^* = \overline{(\mathbf{A}^\top)}$, and so $\overline{\mathbf{A}^*} = \mathbf{A}^\top$. Now,

$$\mathbf{A}^{**} = (\mathbf{A}^*)^* = \left(\overline{\mathbf{A}^*}\right)^\top = (\mathbf{A}^\top)^\top = \mathbf{A},$$

as desired.

*Proof of Part (4).* For this we must recall Proposition 2.13 as well as equation (8.4):

$$(\mathbf{AB})^* = \left(\overline{\mathbf{AB}}\right)^\top = \overline{(\mathbf{AB})^\top} = \overline{\mathbf{B}^\top\mathbf{A}^\top} = \overline{\mathbf{B}^\top}\,\overline{\mathbf{A}^\top} = \left(\overline{\mathbf{B}}\right)^\top\left(\overline{\mathbf{A}}\right)^\top = \mathbf{B}^*\mathbf{A}^*.$$

Proofs of the other parts of the proposition are left as exercises. ■

**Theorem 8.6.** *Let $(V, \langle\ \rangle)$ be a finite-dimensional inner product space with ordered orthonormal basis $\mathcal{O}$, and let $\Lambda, L \in \mathcal{L}(V)$. Then $\Lambda = L^*$ if and only if $[\Lambda]_\mathcal{O} = [L]^*_\mathcal{O}$.*

**Proof.** Let $[\ ]$ represent $[\ ]_\mathcal{O}$ for simplicity. Suppose that $\Lambda \in \mathcal{L}(V)$ is such that $[\Lambda] = [L]^*$, where

$$[\Lambda] = [L]^* \quad\Leftrightarrow\quad [\Lambda] = \overline{[L]}^\top \quad\Leftrightarrow\quad \overline{[\Lambda]} = [L]^\top.$$

Now, for any $\mathbf{u}, \mathbf{v} \in V$ we have, by Theorem 7.23,

$$\langle L(\mathbf{u}), \mathbf{v}\rangle = [\mathbf{v}]^*[L(\mathbf{u})] = [\mathbf{v}]^*\big([L][\mathbf{u}]\big) = \big([\mathbf{v}]^*[L]\big)[\mathbf{u}]$$

$$= \big([\mathbf{v}]^*[\Lambda^*]\big)[\mathbf{u}] = \big([\Lambda][\mathbf{v}]\big)^*[\mathbf{u}] = [\Lambda(\mathbf{v})]^*[\mathbf{u}] = \langle \mathbf{u}, \Lambda(\mathbf{v})\rangle,$$

and therefore $\Lambda = L^*$. ■

With this theorem we have a way of finding the adjoint of a linear operator: given an operator $L \in \mathcal{L}(V)$, find an orthonormal basis $\mathcal{O}$ for $V$ (perhaps using the Gram-Schmidt Orthogonalization Process), then determine $[L]_\mathcal{O}$ (the matrix corresponding to $L$ with respect to $\mathcal{O}$) using Corollary 4.21, and then obtain $[L]^*_\mathcal{O}$ by taking the conjugate of the transpose of $[L]_\mathcal{O}$. The matrix $[L]^*_\mathcal{O}$ defines a new operator $L^* \in \mathcal{L}(V)$ that will in fact be the adjunct of $L$.

## 8.2 – Self-Adjoint and Unitary Operators

**Definition 8.7.** *Let $(V, \langle\ \rangle)$ be an inner product space over $\mathbb{F}$. A linear operator $L \in \mathcal{L}(V)$ is* ***self-adjoint*** *with respect to the inner product $\langle\ \rangle$ if $L^* = L$. A matrix $\mathbf{A} \in \mathbb{F}^{n\times n}$ is* ***self-adjoint*** *if $\mathbf{A}^* = \mathbf{A}$.*

Observe that if $\mathbf{A} \in \mathbb{R}^{n\times n}$, then $\mathbf{A}$ is self-adjoint if and only if $\mathbf{A} = \mathbf{A}^\top$, since

$$\mathbf{A} = \mathbf{A}^* = \overline{\mathbf{A}}^\top = \mathbf{A}^\top.$$

That is, "self-adjoint" and "symmetric" mean the same thing in the context of matrices with real-valued entries. It is for this reason that a self-adjoint operator on an inner product space over specifically the field $\mathbb{R}$ may also be called a **symmetric** operator. (Meanwhile, physicists especially are fond of calling a self-adjoint operator on an inner product space over $\mathbb{C}$ a **hermitian** operator.)

**Theorem 8.8.** *Let $(V, \langle\ \rangle)$ be an inner product space over $\mathbb{F}$, and let $L \in \mathcal{L}(V)$. Then $L$ is self-adjoint if and only if*

$$\langle L(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, L(\mathbf{v})\rangle$$

*for all $\mathbf{u}, \mathbf{v} \in V$.*

**Proof.** Suppose that $L$ is self-adjoint, so that $L^* = L$. From (8.1) we have

$$\langle L(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, L^*(\mathbf{v})\rangle = \langle \mathbf{u}, L(\mathbf{v})\rangle$$

for all $\mathbf{u}, \mathbf{v} \in V$, as desired.

Now suppose that

$$\langle L(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, L(\mathbf{v})\rangle \tag{8.5}$$

for all $\mathbf{u}, \mathbf{v} \in V$. By Theorem 8.2, $L^*$ is the unique linear operator on $V$ for which

$$\langle L(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, L^*(\mathbf{v})\rangle \tag{8.6}$$

holds for all $\mathbf{u}, \mathbf{v} \in V$. Comparing (8.5) and (8.6), it is clear that $L^* = L$, and therefore $L$ is self-adjoint. ∎

The following proposition more firmly establishes the connection between the concepts of self-adjoint operators and self-adjoint matrices.

**Theorem 8.9.** *Let $(V, \langle\ \rangle)$ be a finite-dimensional inner product space over $\mathbb{F}$ with ordered orthonormal basis $\mathcal{O}$, and let $L \in \mathcal{L}(V)$. Then $L$ is a self-adjoint operator if and only if $[L]_{\mathcal{O}}^* = [L]_{\mathcal{O}}$.*

**Proof.** Let $\mathcal{O} = (\mathbf{w}_1, \ldots, \mathbf{w}_n)$, and let $[\ ]$ represent $[\ ]_{\mathcal{O}}$ for simplicity. Suppose that $L$ is self-adjoint. By definition $[L] \in \mathbb{F}^{n\times n}$, the matrix corresponding to $L$ with respect to $\mathcal{O}$, satisfies

$$[L][\mathbf{v}] = [L(\mathbf{v})] \tag{8.7}$$

for all $\mathbf{v} \in V$. By Corollary 4.21

$$[L] = \begin{bmatrix} [L(\mathbf{w}_1)] & \cdots & [L(\mathbf{w}_n)] \end{bmatrix},$$

and so for any $\mathbf{v} \in V$

$$[L]^\top \overline{[\mathbf{v}]} = \begin{bmatrix} [L(\mathbf{w}_1)]^\top \\ \vdots \\ [L(\mathbf{w}_n)]^\top \end{bmatrix} \overline{[\mathbf{v}]} = \begin{bmatrix} [L(\mathbf{w}_1)]^\top \overline{[\mathbf{v}]} \\ \vdots \\ [L(\mathbf{w}_n)]^\top \overline{[\mathbf{v}]} \end{bmatrix} = \begin{bmatrix} \langle L(\mathbf{w}_1), \mathbf{v} \rangle \\ \vdots \\ \langle L(\mathbf{w}_n), \mathbf{v} \rangle \end{bmatrix}$$

$$= \begin{bmatrix} \langle \mathbf{w}_1, L(\mathbf{v}) \rangle \\ \vdots \\ \langle \mathbf{w}_n, L(\mathbf{v}) \rangle \end{bmatrix} = \begin{bmatrix} [\mathbf{w}_1]^\top \overline{[L(\mathbf{v})]} \\ \vdots \\ [\mathbf{w}_n]^\top \overline{[L(\mathbf{v})]} \end{bmatrix} = \begin{bmatrix} [\mathbf{w}_1]^\top \\ \vdots \\ [\mathbf{w}_n]^\top \end{bmatrix} \overline{[L(\mathbf{v})]},$$

where the third and fifth equalities follow from Theorem 7.23, and the fourth equality is owing to $L$ being self-adjoint. But the $n \times n$ matrix

$$\begin{bmatrix} [\mathbf{w}_1]^\top \\ \vdots \\ [\mathbf{w}_n]^\top \end{bmatrix} \in \mathbb{R}^{n \times n}$$

is the identity matrix $\mathbf{I}_n$, and so we obtain

$$[L]^\top \overline{[\mathbf{v}]} = \overline{[L(\mathbf{v})]}. \tag{8.8}$$

Taking the conjugate of both sides of (8.8) then yields the equation

$$\overline{[L]}^\top [\mathbf{v}] = [L(\mathbf{v})] \tag{8.9}$$

for all $\mathbf{v} \in V$. From (8.7) and (8.9) we conclude that $[L]$ and $\overline{[L]}^\top$ are matrices corresponding to $L$ with respect to $\mathcal{O}$. By Corollary 4.25 the matrix corresponding to $L$ with respect to $\mathcal{O}$ is unique, and therefore it must be that

$$[L] = \overline{[L]}^\top = [L]^*$$

as desired.

For the converse, suppose that $[L] = [L]^*$. We have

$$[L] = [L]^* \quad \Leftrightarrow \quad [L] = \overline{[L]}^\top \quad \Leftrightarrow \quad [L]^\top = \overline{[L]},$$

and so by Theorem 7.23 we find that, for all $\mathbf{u}, \mathbf{v} \in V$,

$$\langle L(\mathbf{u}), \mathbf{v} \rangle = [L(\mathbf{u})]^\top \overline{[\mathbf{v}]} = \big([L][\mathbf{u}]\big)^\top \overline{[\mathbf{v}]} = [\mathbf{u}]^\top [L]^\top \overline{[\mathbf{v}]}$$

$$= [\mathbf{u}]^\top \overline{[L][\mathbf{v}]} = [\mathbf{u}]^\top \overline{[L(\mathbf{v})]} = \langle \mathbf{u}, L(\mathbf{v}) \rangle.$$

Therefore $L$ is a self-adjoint operator. ■

In Theorem 8.9, if we let $\mathbb{F} = \mathbb{R}$ in particular, then the entries of the matrix $[L]_{\mathcal{O}}$ are real valued, in which case

$$\overline{[L]}_{\mathcal{O}}^\top = [L]_{\mathcal{O}}^\top$$

and we obtain the following quite readily.

**Corollary 8.10.** *Let* $(V, \langle\ \rangle)$ *be a finite-dimensional inner product space over* $\mathbb{R}$ *with orthonormal basis* $\mathcal{O}$*. Then* $L \in \mathcal{L}(V)$ *is a self-adjoint operator if and only if* $[L]_{\mathcal{O}} = [L]_{\mathcal{O}}^{\top}$*.*

A self-adjoint operator $L$ on an inner product space over $\mathbb{R}$ is called a symmetric operator precisely because the matrix corresponding to $L$ with respect to an orthonormal basis is a symmetric matrix.

**Corollary 8.11.** *Let* $(V, \langle\ \rangle)$ *be a finite-dimensional inner product space over* $\mathbb{F}$ *with orthonormal basis* $\mathcal{O}$*. If* $L \in \mathcal{L}(V)$ *is a self-adjoint operator, then* $[L^*]_{\mathcal{O}} = [L]_{\mathcal{O}}^*$*.*

**Proof.** Suppose that $L$ is self-adjoint. Then $L = L^*$ and $[L]_{\mathcal{O}} = [L]_{\mathcal{O}}^*$, whereupon it follows trivially that $[L^*]_{\mathcal{O}} = [L]_{\mathcal{O}}^*$. ∎

**Lemma 8.12 (Polarization Identity).** *Let* $(V, \langle\ \rangle)$ *be an inner product space over* $\mathbb{F}$*. If* $L \in \mathcal{L}(V)$*, then*

$$\langle L(\mathbf{u}+\mathbf{v}), \mathbf{u}+\mathbf{v}\rangle - \langle L(\mathbf{u}-\mathbf{v}), \mathbf{u}-\mathbf{v}\rangle = 2\big[\langle L(\mathbf{u}), \mathbf{v}\rangle + \langle L(\mathbf{v}), \mathbf{u}\rangle\big]$$

*for all* $\mathbf{u}, \mathbf{v} \in V$*.*

**Proof.** Suppose that $L \in \mathcal{L}(V)$, and let $\mathbf{u}, \mathbf{v} \in V$. We have

$$\langle L(\mathbf{u}+\mathbf{v}), \mathbf{u}+\mathbf{v}\rangle = \langle L(\mathbf{u}), \mathbf{u}\rangle + \langle L(\mathbf{u}), \mathbf{v}\rangle + \langle L(\mathbf{v}), \mathbf{u}\rangle + \langle L(\mathbf{v}), \mathbf{v}\rangle$$

and

$$\langle L(\mathbf{u}-\mathbf{v}), \mathbf{u}-\mathbf{v}\rangle = \langle L(\mathbf{u}), \mathbf{u}\rangle - \langle L(\mathbf{u}), \mathbf{v}\rangle - \langle L(\mathbf{v}), \mathbf{u}\rangle + \langle L(\mathbf{v}), \mathbf{v}\rangle.$$

Subtraction then yields

$$\langle L(\mathbf{u}+\mathbf{v}), \mathbf{u}+\mathbf{v}\rangle - \langle L(\mathbf{u}-\mathbf{v}), \mathbf{u}-\mathbf{v}\rangle = 2\langle L(\mathbf{u}), \mathbf{v}\rangle + 2\langle L(\mathbf{v}), \mathbf{u}\rangle,$$

the desired outcome. ∎

**Proposition 8.13.** *Let* $(V, \langle\ \rangle)$ *be an inner product space over* $\mathbb{F}$*, and let* $L \in \mathcal{L}(V)$*.*

1. *Suppose* $\mathbb{F} = \mathbb{C}$*. If* $\langle L(\mathbf{v}), \mathbf{v}\rangle = 0$ *for all* $\mathbf{v} \in V$*, then* $L = O_V$*.*
2. *Suppose* $\mathbb{F} = \mathbb{C}$*. Then* $L$ *is self-adjoint if and only if* $\langle L(\mathbf{v}), \mathbf{v}\rangle \in \mathbb{R}$ *for all* $\mathbf{v} \in V$*.*
3. *If* $L$ *is self-adjoint and* $\langle L(\mathbf{v}), \mathbf{v}\rangle = 0$ *for all* $\mathbf{v} \in V$*, then* $L = O_V$*.*

**Proof.**
*Proof of Part (1).* Suppose that $\langle L(\mathbf{v}), \mathbf{v}\rangle = 0$ for all $\mathbf{v} \in V$. From the polarization identity of Lemma 8.12 we obtain

$$\langle L(\mathbf{u}), \mathbf{v}\rangle + \langle L(\mathbf{v}), \mathbf{u}\rangle = 0 \tag{8.10}$$

for all $\mathbf{u}, \mathbf{v} \in V$. Thus we have, for all $\mathbf{u}, \mathbf{v} \in V$,

$$\langle L(\mathbf{u}), i\mathbf{v}\rangle + \langle L(i\mathbf{v}), \mathbf{u}\rangle = -i\langle L(\mathbf{u}), \mathbf{v}\rangle + i\langle L(\mathbf{v}), \mathbf{u}\rangle = 0,$$

whence

$$-\langle L(\mathbf{u}), \mathbf{v}\rangle + \langle L(\mathbf{v}), \mathbf{u}\rangle = 0. \tag{8.11}$$

Adding equations (8.10) and (8.11) then gives

$$\langle L(\mathbf{v}), \mathbf{u} \rangle = 0$$

for all $\mathbf{u}, \mathbf{v} \in V$. Letting $\mathbf{v}$ be arbitrary and choosing $\mathbf{u} = L(\mathbf{v})$, we obtain

$$\langle L(\mathbf{v}), L(\mathbf{v}) \rangle = 0,$$

and thus $L(\mathbf{v}) = \mathbf{0}$. Therefore $L = O_V$.

*Proof of Part (2).* Suppose that $L$ is self-adjoint. Let $\mathbf{v} \in V$ be arbitrary. We have

$$\langle L(\mathbf{v}), \mathbf{v} \rangle = \langle \mathbf{v}, L(\mathbf{v}) \rangle = \overline{\langle L(\mathbf{v}), \mathbf{v} \rangle},$$

which shows that $\langle L(\mathbf{v}), \mathbf{v} \rangle \in \mathbb{R}$.

For the converse, suppose that $\langle L(\mathbf{v}), \mathbf{v} \rangle \in \mathbb{R}$ for all $\mathbf{v} \in V$. Then

$$\langle L(\mathbf{v}), \mathbf{v} \rangle = \langle \mathbf{v}, L(\mathbf{v}) \rangle,$$

whence we obtain

$$\langle L(\mathbf{v}), \mathbf{v} \rangle - \langle \mathbf{v}, L(\mathbf{v}) \rangle = \langle \mathbf{v}, L^*(\mathbf{v}) \rangle - \langle \mathbf{v}, L(\mathbf{v}) \rangle = \big\langle \mathbf{v}, (L^* - L)(\mathbf{v}) \big\rangle = 0.$$

That is,

$$\big\langle (L^* - L)(\mathbf{v}), \mathbf{v} \big\rangle = 0$$

for all $\mathbf{v} \in V$, and so by Part (1) we conclude that $L^* - L = O_V$. Therefore $L^* = L$.

*Proof of Part (3).* Suppose $L$ is self-adjoint and $\langle L(\mathbf{v}), \mathbf{v} \rangle = 0$ for all $\mathbf{v} \in V$. The conclusion follows by Part (1) if $\mathbb{F} = \mathbb{C}$, so we can assume that $\mathbb{F} = \mathbb{R}$. By the polarization identity we obtain

$$\langle L(\mathbf{u}), \mathbf{v} \rangle + \langle L(\mathbf{v}), \mathbf{u} \rangle = 0,$$

whereupon commutativity gives

$$\langle L(\mathbf{u}), \mathbf{v} \rangle + \langle \mathbf{u}, L(\mathbf{v}) \rangle = 0,$$

and finally self-adjointness delivers

$$\langle L(\mathbf{u}), \mathbf{v} \rangle + \langle L(\mathbf{u}), \mathbf{v} \rangle = 0.$$

So $\langle L(\mathbf{u}), \mathbf{v} \rangle = 0$ for all $\mathbf{u}, \mathbf{v} \in V$. Letting $\mathbf{u}$ be arbitrary and setting $\mathbf{v} = L(\mathbf{u})$, we find that $\langle L(\mathbf{u}), L(\mathbf{u}) \rangle = 0$, and thus $L(\mathbf{u}) = \mathbf{0}$. Therefore $L = O_V$. ■

**Definition 8.14.** *Let $(V, \langle\ \rangle)$ be an inner product space over $\mathbb{F}$. An operator $L \in \mathcal{L}(V)$ is* ***unitary*** *with respect to the inner product $\langle\ \rangle$ if $L^* = L^{-1}$. An invertible matrix $\mathbf{A} \in \mathbb{F}^{n \times n}$ is* ***unitary*** *if $\mathbf{A}^* = \mathbf{A}^{-1}$.*

It is common to call a unitary matrix $\mathbf{A}$ with real-valued entries an **orthogonal** matrix, and a unitary operator on an inner product space over $\mathbb{R}$ an **orthogonal** operator. Note that a unitary operator $L$ on $V$ is invertible: if $\mathbf{v} \in V$ is such that $L(\mathbf{v}) = \mathbf{0}$, then

$$\langle \mathbf{v}, \mathbf{v} \rangle = \langle L(\mathbf{v}), L(\mathbf{v}) \rangle = \langle \mathbf{0}, \mathbf{0} \rangle = 0$$

implies $\mathbf{v} = \mathbf{0}$, so that $\text{Nul}(L) = \{\mathbf{0}\}$ and by the Invertible Operator Theorem we conclude that $L$ is invertible.

**Theorem 8.15.** *Let $(V, \langle\ \rangle)$ be a finite-dimensional inner product space over $\mathbb{F}$ with orthonormal basis $\mathcal{O}$, and let $L \in \mathcal{L}(V)$. Then $L$ is a unitary operator if and only if $[L]_{\mathcal{O}}^* = [L]_{\mathcal{O}}^{-1}$.*

The proof of Theorem 8.15 is much the same as the proof of Theorem 8.9, and so it is left as a problem.

**Theorem 8.16.** *Let $(V, \langle\ \rangle)$ be an inner product space over $\mathbb{F}$, and let $L \in \mathcal{L}(V)$. The following statements are equivalent:*

1. *$L$ is a unitary operator.*
2. *If $\|\mathbf{v}\| = 1$, then $\|L(\mathbf{v})\| = 1$.*
3. *$\|L(\mathbf{v})\| = \|\mathbf{v}\|$ for all $\mathbf{v} \in V$.*
4. *$\langle L(\mathbf{u}), L(\mathbf{v})\rangle = \langle \mathbf{u}, \mathbf{v}\rangle$ for all $\mathbf{u}, \mathbf{v} \in V$.*

**Proof.**
*(1) → (2).* Suppose that $L$ is a unitary operator. Fix $\mathbf{v} \in V$ such that $\|\mathbf{v}\| = 1$. Then

$$\|L(\mathbf{v})\|^2 = \langle L(\mathbf{v}), L(\mathbf{v})\rangle = \langle \mathbf{v}, L^*(L(\mathbf{v}))\rangle = \langle \mathbf{v}, L^{-1}(L(\mathbf{v}))\rangle = \langle \mathbf{v}, \mathbf{v}\rangle = \|\mathbf{v}\|^2 = 1,$$

and hence $\|L(\mathbf{v})\| = 1$.

*(2) → (3).* Suppose that $\|L(\mathbf{v})\| = 1$ for all $\mathbf{v} \in V$ such that $\|\mathbf{v}\| = 1$. Fix $\mathbf{v} \in V$. If $\mathbf{v} = \mathbf{0}$, then $\|L(\mathbf{0})\| = \|\mathbf{0}\|$ obtains immediately, so suppose that $\mathbf{v} \neq \mathbf{0}$. Then $\hat{\mathbf{v}} = \mathbf{v}/\|\mathbf{v}\|$ is a vector in $V$ such that $\|\hat{\mathbf{v}}\| = 1$, and so $\|L(\hat{\mathbf{v}})\| = 1$ by hypothesis. Now,

$$\|L(\mathbf{v})\| = \big\|L\big(\|\mathbf{v}\|\hat{\mathbf{v}}\big)\big\| = \|\mathbf{v}\|\|L(\hat{\mathbf{v}})\| = \|\mathbf{v}\|.$$

Therefore $\|L(\mathbf{v})\| = \|\mathbf{v}\|$ for all $\mathbf{v} \in V$.

*(3) → (4).* Suppose that $\|L(\mathbf{v})\| = \|\mathbf{v}\|$, or equivalently $\langle L(\mathbf{v}), L(\mathbf{v})\rangle = \langle \mathbf{v}, \mathbf{v}\rangle$, for all $\mathbf{v} \in V$. Fix $\mathbf{u}, \mathbf{v} \in V$. By the Parallelogram Law given in Theorem 7.9,

$$\|L(\mathbf{u}) + L(\mathbf{v})\|^2 + \|L(\mathbf{u}) - L(\mathbf{v})\|^2 = 2\|L(\mathbf{u})\|^2 + 2\|L(\mathbf{v})\|^2 = 2\|\mathbf{u}\|^2 + 2\|\mathbf{v}\|^2,$$

whence

$$\|L(\mathbf{u}) + L(\mathbf{v})\|^2 + \|L(\mathbf{u} - \mathbf{v})\|^2 = \|L(\mathbf{u}) + L(\mathbf{v})\|^2 + \|\mathbf{u} - \mathbf{v}\|^2 = 2\|\mathbf{u}\|^2 + 2\|\mathbf{v}\|^2,$$

and then

$$\langle L(\mathbf{u}) + L(\mathbf{v}), L(\mathbf{u}) + L(\mathbf{v})\rangle + \langle \mathbf{u} - \mathbf{v}, \mathbf{u} - \mathbf{v}\rangle = 2\langle \mathbf{u}, \mathbf{u}\rangle + 2\langle \mathbf{v}, \mathbf{v}\rangle. \tag{8.12}$$

Since

$$\begin{aligned}\langle L(\mathbf{u}) + L(\mathbf{v}), L(\mathbf{u}) + L(\mathbf{v})\rangle &= \langle L(\mathbf{u}), L(\mathbf{u})\rangle + \langle L(\mathbf{u}), L(\mathbf{v})\rangle + \langle L(\mathbf{v}), L(\mathbf{u})\rangle + \langle L(\mathbf{v}), L(\mathbf{v})\rangle \\ &= \langle \mathbf{u}, \mathbf{u}\rangle + \langle L(\mathbf{u}), L(\mathbf{v})\rangle + \langle L(\mathbf{v}), L(\mathbf{u})\rangle + \langle \mathbf{v}, \mathbf{v}\rangle\end{aligned}$$

and

$$\langle \mathbf{u} - \mathbf{v}, \mathbf{u} - \mathbf{v}\rangle = \langle \mathbf{u}, \mathbf{u}\rangle - \langle \mathbf{u}, \mathbf{v}\rangle - \langle \mathbf{v}, \mathbf{u}\rangle + \langle \mathbf{v}, \mathbf{v}\rangle,$$

from (8.12) we obtain

$$\langle L(\mathbf{u}), L(\mathbf{v})\rangle + \langle L(\mathbf{v}), L(\mathbf{u})\rangle = \langle \mathbf{u}, \mathbf{v}\rangle + \langle \mathbf{v}, \mathbf{u}\rangle. \tag{8.13}$$

If $\mathbb{F} = \mathbb{R}$, then the inner product is commutative and (8.13) gives $\langle L(\mathbf{u}), L(\mathbf{v})\rangle = \langle \mathbf{u}, \mathbf{v}\rangle$ as desired. If $\mathbb{F} = \mathbb{C}$, then substitute $i\mathbf{u}$ for $\mathbf{u}$ in (8.13) to obtain

$$\langle L(i\mathbf{u}), L(\mathbf{v})\rangle + \langle L(\mathbf{v}), L(i\mathbf{u})\rangle = \langle i\mathbf{u}, \mathbf{v}\rangle + \langle \mathbf{v}, i\mathbf{u}\rangle,$$

so by the linearity of $L$, Axiom IP2 in Definition 7.1, and Theorem 7.2(3),

$$i\langle L(\mathbf{u}), L(\mathbf{v})\rangle - i\langle L(\mathbf{v}), L(\mathbf{u})\rangle = i\langle \mathbf{u}, \mathbf{v}\rangle - i\langle \mathbf{v}, \mathbf{u}\rangle,$$

and thus

$$\langle L(\mathbf{u}), L(\mathbf{v})\rangle - \langle L(\mathbf{v}), L(\mathbf{u})\rangle = \langle \mathbf{u}, \mathbf{v}\rangle - \langle \mathbf{v}, \mathbf{u}\rangle. \tag{8.14}$$

Finally, adding (8.13) and (8.14) gives $\langle L(\mathbf{u}), L(\mathbf{v})\rangle = \langle \mathbf{u}, \mathbf{v}\rangle$ once again.

*(4) → (1).* Suppose that $\langle L(\mathbf{u}), L(\mathbf{v})\rangle = \langle \mathbf{u}, \mathbf{v}\rangle$ for all $\mathbf{u}, \mathbf{v} \in V$. Thus, for any $\mathbf{u}, \mathbf{v} \in V$,

$$\langle L(\mathbf{u}), \mathbf{v}\rangle = \langle L(\mathbf{u}), L(L^{-1}(\mathbf{v}))\rangle = \langle \mathbf{u}, L^{-1}(\mathbf{v})\rangle,$$

which shows that $L^{-1} = L^*$ and therefore $L$ is a unitary operator. ∎

**Proposition 8.17.** *If $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{n\times n}$ are unitary and $c \in \mathbb{F}$, then $\mathbf{A}^{-1}$, $c\mathbf{A}$, $\mathbf{A}+\mathbf{B}$, and $\mathbf{AB}$ are unitary.*

**Proof.** Suppose that $\mathbf{A}, \mathbf{B} \in \mathbb{F}^{n\times n}$ are unitary and $c \in \mathbb{F}$. By Proposition 8.5(2) we have

$$(\mathbf{A}^{-1})^* = (\mathbf{A}^*)^* = \mathbf{A}^{**} = \mathbf{A} = (\mathbf{A}^{-1})^{-1};$$

that is, the adjoint of $\mathbf{A}^{-1}$ equals the inverse of $\mathbf{A}^{-1}$, and therefore $\mathbf{A}^{-1}$ is unitary. ∎

**Proposition 8.18.** *If $\mathcal{O}$ and $\mathcal{O}'$ are two ordered orthonormal bases for an inner product space $(V, \langle\,\rangle)$ over $\mathbb{F}$, then the change of basis matrix $\mathbf{I}_{\mathcal{O}\mathcal{O}'}$ is a unitary matrix.*

**Proof.** Suppose that $\mathcal{O} = (\mathbf{w}_1, \ldots, \mathbf{w}_n)$ and $\mathcal{O}' = (\mathbf{w}'_1, \ldots, \mathbf{w}'_n)$ are each orthonormal bases for an inner product space $(V, \langle\,\rangle)$ over $\mathbb{F}$. Then by Theorem 7.23

$$\langle \mathbf{u}, \mathbf{v}\rangle = [\mathbf{u}]_{\mathcal{O}'}^\top \overline{[\mathbf{v}]}_{\mathcal{O}'}$$

for all $\mathbf{u}, \mathbf{v} \in V$, and also

$$\langle \mathbf{w}_i, \mathbf{w}_j\rangle = \delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

By Theorem 4.27

$$\mathbf{I}_{\mathcal{O}\mathcal{O}'} = \Big[ [\mathbf{w}_1]_{\mathcal{O}'} \;\; \cdots \;\; [\mathbf{w}_n]_{\mathcal{O}'} \Big],$$

and so, letting $\mathbf{I} = \mathbf{I}_{\mathcal{O}\mathcal{O}'}$ for brevity,

$$\mathbf{I}^\top \bar{\mathbf{I}} = \begin{bmatrix} [\mathbf{w}_1]_{\mathcal{O}'}^\top \\ \vdots \\ [\mathbf{w}_n]_{\mathcal{O}'}^\top \end{bmatrix} \Big[ \overline{[\mathbf{w}_1]}_{\mathcal{O}'} \;\; \cdots \;\; \overline{[\mathbf{w}_n]}_{\mathcal{O}'} \Big].$$

Thus the $ij$-entry of $\mathbf{I}^\top\overline{\mathbf{I}}$ is

$$\left[\mathbf{I}^\top\overline{\mathbf{I}}\right]_{ij} = [\mathbf{w}_i]_{\mathcal{O}'}^\top\overline{[\mathbf{w}_j]_{\mathcal{O}'}} = \langle \mathbf{w}_i, \mathbf{w}_j\rangle = \delta_{ij} = [\mathbf{I}_n]_{ij}$$

for all $1 \leq i, j \leq n$, and therefore $\mathbf{I}^\top\overline{\mathbf{I}} = \mathbf{I}_n$. Now, since $\mathbf{I}$ is invertible by Proposition 4.31, we have

$$\mathbf{I}^\top\overline{\mathbf{I}} = \mathbf{I}_n \quad \Leftrightarrow \quad \overline{\mathbf{I}}^\top\mathbf{I} = \mathbf{I}_n \quad \Leftrightarrow \quad \left(\overline{\mathbf{I}}^\top\mathbf{I}\right)\mathbf{I}^{-1} = \mathbf{I}_n\mathbf{I}^{-1} \quad \Leftrightarrow \quad \overline{\mathbf{I}}^\top = \mathbf{I}^{-1}$$

and hence $\mathbf{I}^* = \mathbf{I}^{-1}$. Therefore $\mathbf{I}_{\mathcal{O}\mathcal{O}'}$ is a unitary matrix. ■

## 8.3 – Normal Operators

**Definition 8.19.** *Let $(V, \langle\,\rangle)$ be an inner product space over $\mathbb{F}$. An operator $L \in \mathcal{L}(V)$ is **normal** if*

$$L \circ L^* = L^* \circ L.$$

**Proposition 8.20.** *All self-adjoint and unitary operators are normal operators*

**Proof.** Suppose $L$ is a self-adjoint operator on $(V, \langle\,\rangle)$. Then $L^* = L$ by definition, which immediately implies that

$$L \circ L^* = L^* \circ L,$$

and hence $L$ is normal.

Now suppose that $L$ is a unitary operator on $(V, \langle\,\rangle)$. Then $L^* = L^{-1}$ by definition, so that

$$L \circ L^* = L \circ L^{-1} = I_V = L^{-1} \circ L = L^* \circ L$$

and hence $L$ is normal. ■

**Proposition 8.21.** *Let $(V, \langle\,\rangle)$ be an inner product space over $\mathbb{F}$. Then $L \in \mathcal{L}(V)$ is a normal operator if and only if $\|L(\mathbf{v})\| = \|L^*(\mathbf{v})\|$ for all $\mathbf{v} \in V$.*

**Proof.** Suppose that $L \in \mathcal{L}(V)$ is a normal operator. Let $\mathbf{v} \in V$. Then

$$\begin{aligned}\|L(\mathbf{v})\|^2 &= \big\langle L(\mathbf{v}), L(\mathbf{v})\big\rangle = \big\langle \mathbf{v}, L^*(L(\mathbf{v}))\big\rangle = \big\langle \mathbf{v}, (L^* \circ L)(\mathbf{v})\big\rangle = \big\langle \mathbf{v}, (L \circ L^*)(\mathbf{v})\big\rangle \\ &= \big\langle \mathbf{v}, L(L^*(\mathbf{v}))\big\rangle = \big\langle L(L^*(\mathbf{v})), \mathbf{v}\big\rangle = \big\langle L^*(\mathbf{v}), L^*(\mathbf{v})\big\rangle = \|L^*(\mathbf{v})\|^2,\end{aligned}$$

and therefore $\|L(\mathbf{v})\| = \|L^*(\mathbf{v})\|$.

Conversely, suppose that $\|L(\mathbf{v})\| = \|L^*(\mathbf{v})\|$ for all $\mathbf{v} \in V$, or equivalently

$$\langle L(\mathbf{v}), L(\mathbf{v})\rangle = \langle L^*(\mathbf{v}), L^*(\mathbf{v})\rangle$$

for all $\mathbf{v} \in V$. By Proposition 8.3,

$$(L \circ L^* - L^* \circ L)^* = (L \circ L^*)^* - (L^* \circ L)^* = L^{**} \circ L^* - L^* \circ L^{**} = L \circ L^* - L^* \circ L,$$

which shows that $L \circ L^* - L^* \circ L$ is self-adjoint. Now, for any $\mathbf{v} \in V$,

$$\begin{aligned}\big\langle \mathbf{v}, (L^* \circ L)(\mathbf{v})\big\rangle &= \big\langle \mathbf{v}, L^*(L(\mathbf{v}))\big\rangle = \big\langle L(\mathbf{v}), L(\mathbf{v})\big\rangle = \big\langle L^*(\mathbf{v}), L^*(\mathbf{v})\big\rangle \\ &= \big\langle \mathbf{v}, L(L^*(\mathbf{v}))\big\rangle = \big\langle \mathbf{v}, (L \circ L^*)(\mathbf{v})\big\rangle,\end{aligned}$$

and thus

$$\big\langle (L \circ L^* - L^* \circ L)(\mathbf{v}), \mathbf{v}\big\rangle = \big\langle (L \circ L^*)(\mathbf{v}), \mathbf{v}\big\rangle - \big\langle (L^* \circ L)(\mathbf{v}), \mathbf{v}\big\rangle = 0.$$

It follows by Proposition 8.13(3) that

$$L \circ L^* - L^* \circ L = O_V,$$

and therefore $L \circ L^* = L^* \circ L$. ■

**Proposition 8.22.** *Let $(V, \langle\ \rangle)$ be an inner product space over $\mathbb{F}$, and let $L \in \mathcal{L}(V)$ be a normal operator. If $U$ is a subspace of $V$ that is invariant under $L$, then $U^\perp$ is also invariant under $L^*$.*

**Proof.** Suppose that $U$ is a subspace of $V$ that is invariant under $L$. Let $\mathbf{q} \in L^*(U^\perp)$, so there exists some $\mathbf{p} \in U^\perp$ such that $L(\mathbf{p}) = \mathbf{q}$. Now, $\mathbf{p} \in U^\perp$ implies that $\langle \mathbf{u}, \mathbf{p} \rangle = 0$ for all $\mathbf{u} \in U$. On the other hand $L(\mathbf{u}) \in U$ for all $\mathbf{u} \in U$, and so

$$\langle L(\mathbf{u}), \mathbf{p} \rangle = 0$$

for all $\mathbf{u} \in U$. Now,

$$\langle L(\mathbf{u}), \mathbf{p} \rangle = 0 \quad \Leftrightarrow \quad \langle \mathbf{u}, L^*(\mathbf{p}) \rangle = 0 \quad \Leftrightarrow \quad \langle \mathbf{u}, \mathbf{q} \rangle = 0,$$

which demonstrates that $\mathbf{q} \perp \mathbf{u}$ for all $\mathbf{u} \in U$, and hence $\mathbf{q} \in U^\perp$. We conclude that $L^*(U^\perp) \subseteq U^\perp$ and therefore $U^\perp$ is invariant under $L^*$. ■

## 8.4 – The Spectral Theorem

Recall from the previous chapter that if $(V, \langle\ \rangle)$ is an inner product space over $\mathbb{F}$, then a linear operator $L$ on $V$ is called self-adjoint if

$$\langle L(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, L(\mathbf{v})\rangle$$

for all $\mathbf{u}, \mathbf{v} \in V$. As the first part of the next theorem makes clear, any linear operator on a nontrivial inner product space $(V, \langle\ \rangle)$ over the field $\mathbb{C}$, in particular, will always have an eigenvector. If the underlying field of $(V, \langle\ \rangle)$ is $\mathbb{R}$, however, then something more is required for the existence of an eigenvector to be assured: namely, the operator must be self-adjoint.

**Theorem 8.23.** *Let $(V, \langle\ \rangle)$ be a vector space over $\mathbb{F}$ of dimension $n \in \mathbb{N}$, and let $L \in \mathcal{L}(V)$.*

1. *If $\mathbb{F} = \mathbb{C}$, then $L$ has an eigenvector.*
2. *If $\mathbb{F} = \mathbb{R}$ and $L$ is self-adjoint with respect to some inner product on $V$, then $L$ has an eigenvector.*

**Proof.**

*Proof of Part (1).* Suppose $\mathbb{F} = \mathbb{C}$. Let $\mathcal{B}$ be an ordered basis for $V$, and let $[L]_{\mathcal{B}}$ be the matrix corresponding to $L$ with respect to $\mathcal{B}$. Then $[L]_{\mathcal{B}} \in \mathbb{C}^{n\times n}$ since $V$ is a vector space over $\mathbb{C}$, and by Proposition 6.29(1) $[L]_{\mathcal{B}}$ has at least one eigenvalue $\lambda \in \mathbb{C}$. Now Proposition 6.14 implies that $\lambda$ is an eigenvalue of $L$, which is to say there exists some $\mathbf{v} \in V$ such that $\mathbf{v} \neq \mathbf{0}$ and $L(\mathbf{v}) = \lambda\mathbf{v}$. Therefore $L$ has an eigenvector.

*Proof of Part (2).* Suppose $\mathbb{F} = \mathbb{R}$ and $L$ is self-adjoint with respect to some inner product on $V$. By Corollary 7.15 there exists an ordered orthonormal basis $\mathcal{O}$ for $V$, and so $[L]_{\mathcal{O}} \in \mathrm{Sym}_n(\mathbb{R})$ by Corollary 8.10. It then follows by Theorem7.26 that $[L]_{\mathcal{O}}$ has an eigenvalue $\lambda \in \mathbb{R}$ with a corresponding eigenvector in $\mathbb{R}^n$, whereupon Proposition 6.14 implies that $\lambda$ is an eigenvalue of $L$. Therefore $L$ has an eigenvector. ■

**Definition 8.24.** *Let $V$ be a vector space over $\mathbb{F}$, let $U$ be a subspace, and let $L \in \mathcal{L}(V)$ be a linear operator. We say that $U$ is **invariant under** $L$ (or $L$-**invariant**) if $L(U) \subseteq U$.*

Recall that $L(U) = \mathrm{Img}(L)$, and notice that a subspace $U$ of vector space $V$ is invariant under $L \in \mathcal{L}(V)$ if and only if $L|_U \in \mathcal{L}(U)$, where as usual $L|_U$ denotes the restriction of the function $L$ to the set $U$. Many times in proofs, however, we will continue to use the symbol $L$ to denote $L|_U$, after writing either $L \in \mathcal{L}(U)$ or $L : U \to U$, say, to make clear that the domain of $L$ is being restricted to $U$.

**Proposition 8.25.** *Let $(V, \langle\ \rangle)$ be an inner product space over $\mathbb{F}$, and let $L \in \mathcal{L}(V)$ be a normal operator.*

1. *If $\mathbf{v} \in V$ is an eigenvector of $L$ with corresponding eigenvalue $\lambda$, then $\mathbf{v}$ is an eigenvector of $L^*$ with eigenvalue $\overline{\lambda}$.*
2. *If $\mathbf{v}_1, \mathbf{v}_2 \in V$ are eigenvectors of $L$ with corresponding eigenvalues $\lambda_1, \lambda_2 \in \mathbb{F}$ such that $\lambda_1 \neq \lambda_2$, then $\mathbf{v}_1 \perp \mathbf{v}_2$.*

**Proof.**
*Proof of Part (1).* Suppose that $\mathbf{v} \in V$ is an eigenvector of $L$ with corresponding eigenvalue $\lambda$, so that $L(\mathbf{v}) = \lambda\mathbf{v}$. Define $\Lambda = L - \lambda I_V$, and note that $\Lambda \in \mathcal{L}(V)$. In fact $\Lambda$ just so happens to be a normal operator: recalling Proposition 8.3 and noting that $I_V^* = I_V$, for any $\mathbf{u} \in V$ we have

$$\begin{aligned}(\Lambda \circ \Lambda^*)(\mathbf{u}) &= \Lambda((L^* - \overline{\lambda} I_V)(\mathbf{u})) = \Lambda(L^*(\mathbf{u}) - \overline{\lambda}\mathbf{u}) = L(L^*(\mathbf{u}) - \overline{\lambda}\mathbf{u}) - \lambda(L^*(\mathbf{u}) - \overline{\lambda}\mathbf{u}) \\ &= (L \circ L^*)(\mathbf{u}) - \overline{\lambda} L(\mathbf{u}) - \lambda L^*(\mathbf{u}) + \lambda\overline{\lambda}\mathbf{u}\end{aligned}$$

and

$$\begin{aligned}(\Lambda^* \circ \Lambda)(\mathbf{u}) &= \Lambda^*((L - \lambda I_V)(\mathbf{u})) = \Lambda^*(L(\mathbf{u}) - \lambda\mathbf{u}) = L^*(L(\mathbf{u}) - \lambda\mathbf{u}) - \overline{\lambda}(L(\mathbf{u}) - \lambda\mathbf{u}) \\ &= (L^* \circ L)(\mathbf{u}) - \lambda L^*(\mathbf{u}) - \overline{\lambda} L(\mathbf{u}) + \lambda\overline{\lambda}\mathbf{u}.\end{aligned}$$

Now, since $L \circ L^* = L^* \circ L$, we find that

$$\Lambda \circ \Lambda^* = L \circ L^* - \overline{\lambda} L - \lambda L^* + \lambda\overline{\lambda} I_V = \Lambda^* \circ \Lambda$$

and hence $\Lambda$ is normal. Forging on, by Proposition 8.21 we obtain

$$\|(L^* - \overline{\lambda} I_V)(\mathbf{v})\| = \|(L - \lambda I_V)^*(\mathbf{v})\| = \|(L - \lambda I_V)(\mathbf{v})\| = \|L(\mathbf{v}) - \lambda\mathbf{v}\| = \|\mathbf{0}\| = 0,$$

which implies that

$$(L^* - \overline{\lambda} I_V)(\mathbf{v}) = \mathbf{0}.$$

That is, $L^*(\mathbf{v}) = \overline{\lambda}\mathbf{v}$.

*Proof of Part (2).* Suppose that $\mathbf{v}_1, \mathbf{v}_2 \in V$ are eigenvectors of $L$ with corresponding eigenvalues $\lambda_1, \lambda_2 \in \mathbb{F}$ such that $\lambda_1 \neq \lambda_2$. By Part (1), $\mathbf{v}_1, \mathbf{v}_2 \in V$ are eigenvectors of $L^*$ with corresponding eigenvalues $\overline{\lambda}_1$ and $\overline{\lambda}_2$, respectively. Now,

$$\begin{aligned}(\lambda_1 - \lambda_2)\langle \mathbf{v}_1, \mathbf{v}_2 \rangle &= \lambda_1 \langle \mathbf{v}_1, \mathbf{v}_2 \rangle - \lambda_2 \langle \mathbf{v}_1, \mathbf{v}_2 \rangle = \langle \lambda_1 \mathbf{v}_1, \mathbf{v}_2 \rangle - \langle \mathbf{v}_1, \overline{\lambda}_2 \mathbf{v}_2 \rangle \\ &= \langle L(\mathbf{v}_1), \mathbf{v}_2 \rangle - \langle \mathbf{v}_1, L^*(\mathbf{v}_2) \rangle = 0,\end{aligned}$$

and since $\lambda_1 - \lambda_2 \neq 0$ we obtain $\langle \mathbf{v}_1, \mathbf{v}_2 \rangle = 0$. Therefore $\mathbf{v}_1 \perp \mathbf{v}_2$. ■

Whereas the proposition above establishes some eigen theory concerning normal operators, the one below performs a similar favor for self-adjoint operators. The latter will be used to prove the first part of the upcoming Spectral Theorem, the former the second part.

**Proposition 8.26.** *Let $(V, \langle\ \rangle)$ be an inner product space over $\mathbb{F}$, and let $L \in \mathcal{L}(V)$ be a self-adjoint operator.*

1. *All eigenvalues of $L$ are real.*
2. *If $\mathbf{v}$ is an eigenvector of $L$ and $\mathbf{u} \in V$ is such that $\mathbf{u} \perp \mathbf{v}$, then $L(\mathbf{u}) \perp \mathbf{v}$ also.*

**Proof.**
*Proof of Part (1).* Let $\lambda$ be an eigenvalue of $L$. Then there exists some $\mathbf{v} \in V$ such that $\mathbf{v} \neq \mathbf{0}$ and $L(\mathbf{v}) = \lambda\mathbf{v}$. Because $\mathbf{v} \neq \mathbf{0}$ we have $\langle \mathbf{v}, \mathbf{v} \rangle > 0$, and because $L$ is self-adjoint we have

$$\langle L(\mathbf{v}), \mathbf{v} \rangle = \langle \mathbf{v}, L(\mathbf{v}) \rangle.$$

Now,

$$\langle L(\mathbf{v}), \mathbf{v}\rangle = \langle \mathbf{v}, L(\mathbf{v})\rangle \quad\Leftrightarrow\quad \langle \lambda\mathbf{v}, \mathbf{v}\rangle = \langle \mathbf{v}, \lambda\mathbf{v}\rangle \quad\Leftrightarrow\quad \lambda\langle \mathbf{v}, \mathbf{v}\rangle = \overline{\lambda}\langle \mathbf{v}, \mathbf{v}\rangle \quad\Leftrightarrow\quad \lambda = \overline{\lambda},$$

where the last equation obtains upon dividing by $\langle \mathbf{v}, \mathbf{v}\rangle$. Since only a real number can equal its own conjugate, we conclude that $\lambda \in \mathbb{R}$.

*Proof of Part (2).* Suppose that $\mathbf{v}$ is an eigenvector of $L$ and $\mathbf{u} \in V$ is such that $\mathbf{u} \perp \mathbf{v}$. Then $L(\mathbf{v}) = \lambda\mathbf{v}$ for some $\lambda \in \mathbb{F}$, and $\langle \mathbf{u}, \mathbf{v}\rangle = 0$. By Theorem 7.2(3),

$$0 = \bar{\lambda}\langle \mathbf{u}, \mathbf{v}\rangle = \langle \mathbf{u}, \lambda\mathbf{v}\rangle = \langle \mathbf{u}, L(\mathbf{v})\rangle = \langle L(\mathbf{u}), \mathbf{v}\rangle,$$

which demonstrates that $L(\mathbf{u}) \perp \mathbf{v}$. ■

It is a trivial matter to verify that if $L$ is a normal (resp. self-adjoint) operator on $V$, and a subspace $U$ of $V$ is invariant under $L$, then $L|_U$ is a normal (resp. self-adjoint) operator on $U$. This simple fact is assumed in the proof of the following momentous theorem.

**Theorem 8.27** (**Spectral Theorem**). *Let $(V, \langle\,\rangle)$ be an inner product space over $\mathbb{F}$ of dimension $n \in \mathbb{N}$.*

1. *Let $\mathbb{F} = \mathbb{R}$. Then $L \in \mathcal{L}(V)$ is a self-adjoint operator if and only if $V$ has an orthonormal basis consisting of the eigenvectors of $L$.*
2. *Let $\mathbb{F} = \mathbb{C}$. Then $L \in \mathcal{L}(V)$ is a normal operator if and only if $V$ has an orthonormal basis consisting of the eigenvectors of $L$.*

**Proof.**
*Proof of Part (1).* We will first apply induction on $\dim(V)$ to prove that $V$ must have an orthogonal basis consisting of eigenvectors if $L \in \mathcal{L}(V)$ is self-adjoint, whereupon it will be easy to see that $V$ has an orthonormal basis consisting of eigenvectors.

Let $\dim(V) = 1$, and suppose $L$ is self-adjoint. Then $L$ has an eigenvector $\mathbf{w}$ by Theorem 8.23(2), and thus $\mathcal{B} = \{\mathbf{w}\}$ is a basis for $V$ by Theorem 3.54(1) that is clearly orthogonal.

Suppose Part (1) of the statement of the theorem is true for some $n \in \mathbb{N}$. Let $(V, \langle\,\rangle)$ be an inner product space over $\mathbb{R}$ of dimension $n+1$, and let $L : V \to V$ be a self-adjoint operator. Again, $L$ has at least one eigenvector $\mathbf{w}_0$, so that $L(\mathbf{w}_0) = \lambda\mathbf{w}_0$ for some $\lambda \in \mathbb{R}$. By the Gram-Schmidt Process there exist vectors $\mathbf{u}_1, \ldots, \mathbf{u}_n \in V$ such that $\mathcal{B} = \{\mathbf{w}_0, \mathbf{u}_1, \ldots, \mathbf{u}_n\}$ is an orthogonal basis for $V$.

Let $W = \mathrm{Span}\{\mathbf{w}_0\}$ and $U = \mathrm{Span}\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$. For any $\mathbf{v} \in W$ there exists some $c \in \mathbb{R}$ such that $\mathbf{v} = c\mathbf{w}_0$, whereupon we obtain

$$L(\mathbf{v}) = L(c\mathbf{w}_0) = cL(\mathbf{w}_0) = c(\lambda\mathbf{w}_0) = (c\lambda)\mathbf{w}_0 \in W \tag{8.15}$$

and we see that $W$ is invariant under $L$. Since $U = W^{\perp}$ by Proposition 7.18, it follows by Propositions 8.20 and 8.22 that $U$ is also invariant under $L$.

Now, $\dim(U) = n$ because $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ is a basis for $U$, and since $(U, \langle\,\rangle)$ is an $n$-dimensional inner product space over $\mathbb{R}$ and $L : U \to U$ is a self-adjoint operator, it follows by the inductive hypothesis that $U$ has an orthogonal basis $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ consisting of eigenvectors of $L \in \mathcal{L}(U)$.

Thus $U = \mathrm{Span}\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$, where the vectors $\mathbf{w}_1, \ldots, \mathbf{w}_n$ are mutually ortho-gonal. Moreover, for each $1 \le k \le n$,

$$\mathbf{w}_k \in U \quad \Rightarrow \quad \mathbf{w}_k \in W^{\perp} \quad \Rightarrow \quad \langle \mathbf{w}_k, \mathbf{w}_0 \rangle = 0,$$

and so $\mathbf{w}_1, \ldots, \mathbf{w}_n$ are all orthogonal to $\mathbf{w}_0$. Hence $\mathcal{O} = \{\mathbf{w}_0, \ldots, \mathbf{w}_n\}$ is a set of mutually orthogonal vectors, and by Lemma 7.13 we conclude that the vectors in $\mathcal{O}$ are linearly independent. Observing that $|\mathcal{O}| = n + 1 = \dim(V)$, Theorem 3.54(1) implies that $\mathcal{O}$ is a basis for $V$. That is, $\mathcal{O}$ is an orthogonal basis for $V$ consisting of eigenvectors of $L \in \mathcal{L}(V)$.

So by induction we find that, for any $n \in \mathbb{N}$, if $V$ is an inner product space over $\mathbb{R}$ of dimension $n$ and $L$ is a self-adjoint operator on $V$, then $V$ has an orthogonal basis $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ consisting of eigenvectors of $L$. Defining

$$\hat{\mathbf{w}}_k = \frac{\mathbf{w}_k}{\|\mathbf{w}_k\|}$$

for $1 \le k \le n$, then $\{\hat{\mathbf{w}}_1, \ldots, \hat{\mathbf{w}}_n\}$ is an orthonormal basis consisting of eigenvectors of $L$.

For the converse, suppose that $V$ has an orthonormal basis $\mathcal{O} = \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ consisting of the eigenvectors of $L \in \mathcal{L}(V)$. Since $V$ is a vector space over $\mathbb{R}$, it follows that there exist $\lambda_k \in \mathbb{R}$ such that $L(\mathbf{w}_k) = \lambda_k \mathbf{w}_k$ for all $1 \le k \le n$. Let $\mathbf{u}, \mathbf{v} \in V$, so that

$$\mathbf{u} = \sum_{k=1}^{n} a_k \mathbf{w}_k \quad \text{and} \quad \mathbf{v} = \sum_{k=1}^{n} b_k \mathbf{w}_k$$

for some $a_k, b_k \in \mathbb{R}$, $1 \le k \le n$. Now, since $\lambda_k = \overline{\lambda}_k$,

$$\begin{aligned}\langle L(\mathbf{u}), \mathbf{v} \rangle &= \left\langle \sum\nolimits_k a_k \lambda_k \mathbf{w}_k, \mathbf{v} \right\rangle = \sum\nolimits_k \lambda_k \langle a_k \mathbf{w}_k, \mathbf{v} \rangle = \sum\nolimits_k \lambda_k \left\langle a_k \mathbf{w}_k, \sum\nolimits_\ell b_\ell \mathbf{w}_\ell \right\rangle \\ &= \sum\nolimits_k \sum\nolimits_\ell \lambda_k \langle a_k \mathbf{w}_k, b_\ell \mathbf{w}_\ell \rangle = \sum\nolimits_k \lambda_k \langle a_k \mathbf{w}_k, b_k \mathbf{w}_k \rangle = \sum\nolimits_k \langle a_k \mathbf{w}_k, \lambda_k b_k \mathbf{w}_k \rangle \\ &= \sum\nolimits_k \sum\nolimits_\ell \langle a_\ell \mathbf{w}_\ell, \lambda_k b_k \mathbf{w}_k \rangle = \left\langle \sum\nolimits_\ell a_\ell \mathbf{w}_\ell, \sum\nolimits_k \lambda_k b_k \mathbf{w}_k \right\rangle = \langle \mathbf{u}, L(\mathbf{v}) \rangle\end{aligned}$$

and therefore $L$ is self-adjoint.

*Proof of Part (2).* Let $\dim(V) = 1$, and suppose $L$ is normal. Then $L$ has an eigenvector $\mathbf{w}$ by Theorem 8.23(1), and thus $\mathcal{B} = \{\hat{\mathbf{w}}\}$ is an orthonormal basis for $V$ by Theorem 3.54(1).

Suppose Part (2) of the statement of the theorem is true for some $n \in \mathbb{N}$. Let $(V, \langle\,\rangle)$ be an inner product space over $\mathbb{C}$ of dimension $n + 1$, and let $L \in \mathcal{L}(V)$ be normal. Again, $L$ has at least one eigenvector $\mathbf{w}_0$ (which we can assume to be a unit vector), so that $L(\mathbf{w}_0) = \lambda \mathbf{w}_0$ for some $\lambda \in \mathbb{C}$. By the Gram-Schmidt Process there exist vectors $\mathbf{u}_1, \ldots, \mathbf{u}_n \in V$ such that $\mathcal{B} = \{\mathbf{w}_0, \mathbf{u}_1, \ldots, \mathbf{u}_n\}$ is an orthogonal basis for $V$.

Let $W = \mathrm{Span}\{\mathbf{w}_0\}$ and $U = \mathrm{Span}\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$. For any $\mathbf{v} \in W$ there exists some $c \in \mathbb{C}$ such that $\mathbf{v} = c\mathbf{w}_0$, whereupon (8.15) shows that $W$ is invariant under $L$. But $W$ is also invariant under $L^*$, since by Proposition 8.25(1) we have

$$L^*(c\mathbf{w}_0) = cL^*(\mathbf{w}_0) = c(\overline{\lambda}\mathbf{w}_0) = (c\overline{\lambda})\mathbf{w}_0 \in W.$$

Now, since $L^* \in \mathcal{L}(V)$ is normal, by Proposition 8.22 we conclude that $W^{\perp}$ is invariant under $L^{**} = L$, where $W^{\perp} = U$ by Proposition 7.18.

Now, $(U, \langle\,\rangle)$ is an $n$-dimensional inner product space over $\mathbb{C}$ and $L \in \mathcal{L}(U)$ is a normal operator, so by the inductive hypothesis $U$ has an orthonormal basis $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ consisting of eigenvectors of $L$. Thus $U = \text{Span}\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$, where the vectors $\mathbf{w}_1, \ldots, \mathbf{w}_n$ are mutually orthogonal, and as with the proof of Part (1) we find that $\mathbf{w}_1, \ldots, \mathbf{w}_n$ are each orthogonal to $\mathbf{w}_0$. Hence $\mathcal{O} = \{\mathbf{w}_0, \ldots, \mathbf{w}_n\}$ is a set of mutually orthogonal vectors which, as before, we find to be a basis for $V$. In particular, $\mathcal{O}$ is an orthonormal basis for $V$ consisting of eigenvectors of $L \in \mathcal{L}(V)$. By induction we conclude that Part (2) of the theorem is true for all $n \in \mathbb{N}$.

Conversely, suppose that $\mathcal{O} = \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ is an orthonormal basis for $V$ consisting of eigenvectors of $L$. Thus there exist $\lambda_k \in \mathbb{C}$ such that $L(\mathbf{w}_k) = \lambda_k \mathbf{w}_k$ for all $1 \leq k \leq n$, and by Proposition 8.25(1) we also have $L^*(\mathbf{w}_k) = \overline{\lambda}_k \mathbf{w}_k$ for all $1 \leq k \leq n$. Let $\mathbf{v} \in V$, so that

$$\mathbf{v} = \sum_{k=1}^{n} a_k \mathbf{w}_k$$

for some $a_1, \ldots, a_n \in \mathbb{C}$. Now,

$$\begin{aligned}
\langle L(\mathbf{v}), L(\mathbf{v}) \rangle &= \left\langle \sum\nolimits_k a_k \lambda_k \mathbf{w}_k, \sum\nolimits_\ell a_\ell \lambda_\ell \mathbf{w}_\ell \right\rangle = \sum\nolimits_k \sum\nolimits_\ell \langle a_k \lambda_k \mathbf{w}_k, a_\ell \lambda_\ell \mathbf{w}_\ell \rangle \\
&= \sum\nolimits_k \sum\nolimits_\ell \lambda_k \overline{\lambda}_\ell \langle a_k \mathbf{w}_k, a_\ell \mathbf{w}_\ell \rangle = \sum\nolimits_k \sum\nolimits_\ell \lambda_k \overline{\lambda}_\ell \langle a_\ell \mathbf{w}_\ell, a_k \mathbf{w}_k \rangle \\
&= \sum\nolimits_k \sum\nolimits_\ell \langle a_\ell \overline{\lambda}_\ell \mathbf{w}_\ell, a_k \overline{\lambda}_k \mathbf{w}_k \rangle = \sum\nolimits_k \sum\nolimits_\ell \langle a_\ell L^*(\mathbf{w}_\ell), a_k L^*(\mathbf{w}_k) \rangle \\
&= \left\langle \sum\nolimits_\ell L^*(a_\ell \mathbf{w}_\ell), \sum\nolimits_k L^*(a_k \mathbf{w}_k) \right\rangle = \langle L^*(\mathbf{v}), L^*(\mathbf{v}) \rangle,
\end{aligned}$$

where the fourth equality is justified since $\langle a_k \mathbf{w}_k, a_\ell \mathbf{w}_\ell \rangle$ is real-valued for all $1 \leq k, \ell \leq n$:

$$\langle a_k \mathbf{w}_k, a_\ell \mathbf{w}_\ell \rangle = \begin{cases} 0, & \text{if } k \neq \ell \\ |a_k|, & \text{if } k = \ell \end{cases}$$

Hence we have

$$\|L(\mathbf{v})\| = \sqrt{\langle L(\mathbf{v}), L(\mathbf{v}) \rangle} = \sqrt{\langle L^*(\mathbf{v}), L^*(\mathbf{v}) \rangle} = \|L^*(\mathbf{v})\|,$$

and so by Proposition 8.21 we conclude that $L$ is a normal operator. ■

**Corollary 8.28.** *Let $(V, \langle\ \rangle)$ be a nontrivial finite-dimensional inner product space over $\mathbb{F}$, and let $\lambda_1, \ldots, \lambda_m$ be the distinct eigenvalues of $L \in \mathcal{L}(V)$. If $L$ is self-adjoint, or if $L$ is normal and $\mathbb{F} = \mathbb{C}$, then*

$$V = E_L(\lambda_1) \oplus \cdots \oplus E_L(\lambda_m). \tag{8.16}$$

*Moreover, $E_L(\lambda_i) \perp E_L(\lambda_j)$ for all $i \neq j$.*

**Proof.** Suppose that $L$ is self-adjoint, or $L$ is normal and $\mathbb{F} = \mathbb{C}$. By the Spectral Theorem there exists an orthonormal basis $\mathcal{O} = \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ consisting of the eigenvectors of $L$, and thus (8.16) follows by Theorem 6.40.

Next, let $\mathbf{u} \in E_L(\lambda_i)$ and $\mathbf{v} \in E_L(\lambda_j)$ for $1 \leq i < j \leq m$. If either $\mathbf{u} = \mathbf{0}$ or $\mathbf{v} = \mathbf{0}$, we obtain $\mathbf{u} \perp \mathbf{v}$. Suppose that $\mathbf{u}, \mathbf{v} \neq \mathbf{0}$. Then $\mathbf{u}$ is an eigenvector of $L$ with corresponding eigenvalue $\lambda_i$, and $\mathbf{v}$ is an eigenvector of $L$ with corresponding eigenvalue $\lambda_j$. Since $\lambda_i \neq \lambda_j$ and $L$ is a normal operator, by Proposition 8.25(2) we conclude that $\mathbf{u} \perp \mathbf{v}$ once again. Therefore $E_L(\lambda_i) \perp E_L(\lambda_j)$. ■

**Example 8.29.** Let $(V, \langle\ \rangle)$ be an $n$-dimensional inner product space over $\mathbb{F}$, and suppose that $L \in \mathcal{L}(V)$ is a self-adjoint operator. By Proposition 8.20 $L$ is also a normal operator, and so by the Spectral Theorem (regardless of whether $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$) there exist eigenvectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ such that $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ is an ordered basis for $V$. By Proposition 8.26(1) the corresponding eigenvalues $\lambda_1, \ldots, \lambda_n$ must be real numbers, and so for each $1 \le k \le n$ we have $\lambda_k \in \mathbb{R}$ such that $L(\mathbf{v}_k) = \lambda_k \mathbf{v}_k$. By Corollary 4.21 the $\mathcal{B}$-matrix of $L$ is

$$[L]_{\mathcal{B}} = \Big[\big[L(\mathbf{v}_1)\big]_{\mathcal{B}} \ \cdots \ \big[L(\mathbf{v}_n)\big]_{\mathcal{B}}\Big] = \Big[\big[\lambda_1\mathbf{v}_1\big]_{\mathcal{B}} \ \cdots \ \big[\lambda_n\mathbf{v}_n\big]_{\mathcal{B}}\Big]$$

$$= \Big[\lambda_1\big[\mathbf{v}_1\big]_{\mathcal{B}} \ \cdots \ \lambda_n\big[\mathbf{v}_n\big]_{\mathcal{B}}\Big] = \left[\lambda_1\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix} \ \cdots \ \lambda_n\begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}\right] = \begin{bmatrix}\lambda_1 & 0 & \cdots & 0\\ 0 & \lambda_2 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \lambda_n\end{bmatrix}.$$

That is, $[L]_{\mathcal{B}}$ is a diagonal matrix with real-valued entries, which makes it especially easy to work with in applications.

We see, then, that the Spectral Theorem provides a means of diagonalizing self-adjoint operators on nontrivial inner product spaces, and even normal operators if the underlying field is $\mathbb{C}$.

**Proposition 8.30.** *If* $\mathbf{A} \in \mathbb{F}^{n\times n}$ *is self-adjoint, then there exists a unitary matrix* $\mathbf{U}$ *such that* $\mathbf{U}^{-1}\mathbf{A}\mathbf{U}$ *is a diagonal matrix.*

**Proof.** Suppose that $\mathbf{A} \in \mathbb{F}^{n\times n}$ is self-adjoint. Let $\mathcal{E}$ be the standard basis for $\mathbb{F}^n$, and let $L \in \mathcal{L}(\mathbb{F}^n)$ be the operator given by $[L(\mathbf{x})]_{\mathcal{E}} = \mathbf{A}[\mathbf{x}]_{\mathcal{E}}$, so that the matrix corresponding to $L$ with respect to $\mathcal{E}$ is $[L]_{\mathcal{E}} = \mathbf{A}$. Since $\mathcal{E}$ is an orthonormal basis and $[L]_{\mathcal{E}}$ is self-adjoint, by Theorem 8.9 the operator $L$ is self-adjoint, and therefore $L$ is normal by Proposition 8.20. By the Spectral Theorem there exists an ordered orthonormal basis $\mathcal{O}$ consisting of the eigenvectors of $L$, and so $[L]_{\mathcal{O}}$ is found to be a diagonal matrix by Corollary 4.21.

Consider $\mathbf{I}_{\mathcal{E}\mathcal{O}}$, the change of basis matrix from $\mathcal{E}$ to $\mathcal{O}$. Both bases are orthonormal, so $\mathbf{I}_{\mathcal{E}\mathcal{O}}$ is a unitary matrix by Proposition 8.18, and

$$[L]_{\mathcal{O}} = \mathbf{I}_{\mathcal{E}\mathcal{O}}[L]_{\mathcal{E}}\mathbf{I}_{\mathcal{E}\mathcal{O}}^{-1} \tag{8.17}$$

by Corollary 4.33. Now, the inverse of a unitary matrix is also unitary by Proposition 8.17, so if we let $\mathbf{U} = \mathbf{I}_{\mathcal{E}\mathcal{O}}^{-1}$, then $\mathbf{U}$ is unitary. Also we have $\mathbf{U}^{-1} = \mathbf{I}_{\mathcal{E}\mathcal{O}}$ is unitary. From (8.17) comes

$$\mathbf{U}^{-1}\mathbf{A}\mathbf{U} = [L]_{\mathcal{O}},$$

and the proof is done since $[L]_{\mathcal{O}}$ is diagonal. ■

# 9

# Canonical Forms

## 9.1 – Generalized Eigenvectors

Recall that a vector $\mathbf{v} \neq \mathbf{0}$ is an eigenvector of a linear operator $L : V \to V$ if $L(\mathbf{v}) = \lambda\mathbf{v}$ for some scalar $\lambda$, where

$$L(\mathbf{v}) = \lambda\mathbf{v} \quad \Leftrightarrow \quad L(\mathbf{v}) - \lambda\mathbf{v} = \mathbf{0} \quad \Leftrightarrow \quad L(\mathbf{v}) - \lambda I_V(\mathbf{v}) = \mathbf{0} \quad \Leftrightarrow \quad (L - \lambda I_V)(\mathbf{v}) = \mathbf{0}. \tag{9.1}$$

We expand on this idea as follows.

**Definition 9.1.** *Let $V$ be a vector space over $\mathbb{F}$, $L \in \mathcal{L}(V)$, and $\lambda \in \mathbb{F}$. If $\mathbf{v} \in V$ is a nonzero vector such that $(L - \lambda I_V)^n(\mathbf{v}) = \mathbf{0}$ for some $n \in \mathbb{N}$, then $\mathbf{v}$ is a **generalized eigenvector** of $L$ corresponding to $\lambda$.*

From (9.1) is it clear that the set of eigenvectors of $L$ is included in the set of generalized eigenvectors of $L$, and any eigenvalue corresponding to an eigenvector necessarily also corresponds to a generalized eigenvector. Suppose that $\mathbf{v} \neq \mathbf{0}$ is a generalized eigenvector of $L$ corresponding to $\lambda$. Let

$$n = \min\{k \in \mathbb{N} : (L - \lambda I_V)^k(\mathbf{v}) = \mathbf{0}\}.$$

If $n \geq 2$, then $\mathbf{w} = (L - \lambda I_V)^{n-1}(\mathbf{v})$ is a nonzero vector in $V$, and

$$\mathbf{0} = (L - \lambda I_V)^n(\mathbf{v}) = (L - \lambda I_V)\big((L - \lambda I_V)^{n-1}(\mathbf{v})\big) = (L - \lambda I_V)(\mathbf{w}) = L(\mathbf{w}) - \lambda\mathbf{w}$$

implies that $L(\mathbf{w}) = \lambda\mathbf{w}$. This result obtains immediately if $n = 1$, and so it follows that $\lambda$ is an eigenvalue of $L$ with $(L - \lambda I_V)^{n-1}(\mathbf{v})$ as a corresponding eigenvector. We see that any eigenvalue corresponding to a generalized eigenvector necessarily also corresponds to an eigenvector. It is because a scalar $\lambda$ corresponds to an eigenvector if and only if it corresponds to a generalized eigenvector that we make no distinction between "eigenvalues" and "generalized eigenvalues."

**Definition 9.2.** *Let $V$ be a vector space over $\mathbb{F}$ and $L \in \mathcal{L}(V)$. Suppose $\lambda \in \mathbb{F}$ is an eigenvalue of $L$. The set*

$$K_L(\lambda) = \{\mathbf{v} \in V : (L - \lambda I_V)^n(\mathbf{v}) = \mathbf{0} \text{ for some } n \in \mathbb{N}\}$$

*is the **generalized eigenspace** of $L$ corresponding to $\lambda$.*

To prove the following proposition, note that if $W$ is an $L$-invariant subspace of a vector space $V$ over $\mathbb{F}$, then so too is $\mathrm{Img}(L)$, for the simple reason that $L(W) \subseteq W$ implies $L(L(W)) \subseteq W$, and hence $L(\mathrm{Img}(L)) \subseteq W$. Also note that, for any $f \in \mathcal{P}(\mathbb{F})$, the $L$-invariance of $W$ implies the $f(L)$-invariance of $W$.

**Lemma 9.3.** *Let $V$ be a vector space over $\mathbb{F}$, $L \in \mathcal{L}(V)$, and $\lambda \in \mathbb{F}$. For any $n \in \mathbb{N}$,*

$$(L - \lambda I_V)^n \circ L = L \circ (L - \lambda I_V)^n.$$

**Proof.** When $n = 1$ we have, by Theorem 4.50

$$L \circ (L - \lambda I_V) = L \circ L - \lambda L \circ I_V = L \circ L - \lambda I_V \circ L = (L - \lambda I_V) \circ L.$$

Suppose the conclusion of the lemma is true for some fixed $n \in \mathbb{N}$. That is, if $M = L - \lambda I_V$, then $L \circ M^n = M^n \circ L$. Now, making use of Theorem 4.49,

$$\begin{aligned} L \circ M^{n+1} &= (L \circ M^n) \circ M = (M^n \circ L) \circ M = M^n \circ (L \circ M) \\ &= M^n \circ (M \circ L) = (M^n \circ M) \circ L = M^{n+1} \circ L, \end{aligned}$$

and therefore $L \circ M^n = M^n \circ L$ for all $n \in \mathbb{N}$ by induction. ∎

**Proposition 9.4.** *Let $V$ be a vector space over $\mathbb{F}$ and $L \in \mathcal{L}(V)$. Suppose that $\lambda \in \mathbb{F}$ is an eigenvalue of $L$. Then*
1. *$K_L(\lambda)$ is an $L$-invariant subspace of $V$ such that $E_L(\lambda) \subseteq K_L(\lambda)$.*
2. *For any $\mu \in \mathbb{F}$ such that $\mu \neq \lambda$, the operator $L - \mu I_V : K_L(\lambda) \to V$ is injective.*
3. *If $\mu$ is an eigenvalue of $L$ such that $\mu \neq \lambda$, then $K_L(\mu) \cap K_L(\lambda) = \{\mathbf{0}\}$.*

**Proof.**
*Proof of Part (1).* We have $K_L(\lambda) \neq \varnothing$ since $\mathbf{0} \in K_L(\lambda)$. Let $\mathbf{u}, \mathbf{v} \in K_L(\lambda)$, so that

$$(L - \lambda I_V)^m(\mathbf{u}) = \mathbf{0} \quad \text{and} \quad (L - \lambda I_V)^n(\mathbf{v}) = \mathbf{0}$$

for some $m, n \in \mathbb{N}$. Then

$$\begin{aligned} (L - \lambda I_V)^{m+n}(\mathbf{u} + \mathbf{v}) &= (L - \lambda I_V)^{m+n}(\mathbf{u}) + (L - \lambda I_V)^{m+n}(\mathbf{v}) \\ &= (L - \lambda I_V)^n\big((L - \lambda I_V)^m(\mathbf{u})\big) + (L - \lambda I_V)^m\big((L - \lambda I_V)^n(\mathbf{v})\big) \\ &= (L - \lambda I_V)^n(\mathbf{0}) + (L - \lambda I_V)^m(\mathbf{0}) = \mathbf{0} + \mathbf{0} = \mathbf{0}, \end{aligned}$$

and we conclude that $\mathbf{u} + \mathbf{v} \in K_L(\lambda)$. If $c \in \mathbb{F}$, then

$$(L - \lambda I_V)^m(c\mathbf{u}) = c(L - \lambda I_V)^m(\mathbf{u}) = c\mathbf{0} = \mathbf{0}$$

shows that $c\mathbf{u} \in K_L(\lambda)$. Since $K_L(\lambda)$ is a nonempty subset of $V$ that is closed under vector addition and scalar multiplication, we conclude that it is a subspace of $V$. That $E_L(\lambda) \subseteq K_L(\lambda)$ is obvious.

Next, let $\mathbf{v} \in L(K_L(\lambda))$, so there is some $\mathbf{u} \in K_L(\lambda)$ such that $L(\mathbf{u}) = \mathbf{v}$. There exists some $n \in \mathbb{N}$ such that $(L - \lambda I_V)^n(\mathbf{u}) = \mathbf{0}$, and hence by Lemma 9.3

$$(L - \lambda I_V)^n(\mathbf{v}) = (L - \lambda I_V)^n(L(\mathbf{u})) = L\big((L - \lambda I_V)^n(\mathbf{u})\big) = L(\mathbf{0}) = \mathbf{0}.$$

Therefore $\mathbf{v} \in K_L(\lambda)$, and we conclude that $L(K_L(\lambda)) \subseteq K_L(\lambda)$.

*Proof of Part (2).* Let $\mathbf{v} \in K_L(\lambda)$ such that $(L - \mu I_V)(\mathbf{v}) = \mathbf{0}$. Let

$$n = \min\{k \in \mathbb{N} : (L - \lambda I_V)^k(\mathbf{v}) = \mathbf{0}\}.$$

We have

$$(L - \lambda I_V)\big((L - \lambda I_V)^{n-1}(\mathbf{v})\big) = (L - \lambda I_V)^n(\mathbf{v}) = \mathbf{0},$$

so that $(L - \lambda I_V)^{n-1}(\mathbf{v}) \in E_L(\lambda)$. By Lemma 9.3,

$$(L - \mu I_V)\big((L - \lambda I_V)^{n-1}(\mathbf{v})\big) = (L - \lambda I_V)^{n-1}\big((L - \mu I_V)(\mathbf{v})\big) = (L - \lambda I_V)^{n-1}(\mathbf{0}) = \mathbf{0},$$

so that $(L - \lambda I_V)^{n-1}(\mathbf{v}) \in E_L(\mu)$. Since $E_L(\lambda) \cap E_L(\mu) = \{\mathbf{0}\}$ by Proposition 6.7(2), it follows that

$$(L - \lambda I_V)^{n-1}(\mathbf{v}) = \mathbf{0}.$$

Since $n$ is the smallest positive integer for which $(L - \lambda I_V)^n(\mathbf{v}) = \mathbf{0}$ holds, we must conclude that $n - 1 = 0$, and so

$$\mathbf{0} = (L - \lambda I_V)^{n-1}(\mathbf{v}) = (L - \lambda I_V)^0(\mathbf{v}) = \mathbf{v}.$$

Therefore the null space of $L - \mu I_V$ restricted to $K_L(\lambda)$ is $\{\mathbf{0}\}$, and so $L - \mu I_V : K_L(\lambda) \to V$ is injective.

*Proof of Part (3).* Suppose that $\mathbf{v} \in K_L(\lambda) \cap K_L(\mu)$, so in particular $(L - \mu I_V)^n(\mathbf{v}) = \mathbf{0}$ for some $n \in \mathbb{N}$. Since $K_L(\lambda)$ is $L$-invariant by Part (1), it readily follows that $K_L(\lambda)$ is invariant under $L - \mu I_V$, and thus $L - \mu I_V$ is an injective operator on $K_L(\lambda)$ by Part (2). An easy induction argument shows that $(L - \mu I_V)^n$ is likewise an injective operator on $K_L(\lambda)$, and since $\mathbf{v} \in K_L(\lambda)$ is such that $(L - \mu I_V)^n(\mathbf{v}) = \mathbf{0}$, it follows that $\mathbf{v} = \mathbf{0}$ and therefore $K_L(\lambda) \cap K_L(\mu) = \varnothing$. ■

**Proposition 9.5.** *Let $V$ be a finite-dimensional vector space over $\mathbb{F}$ and $L \in \mathcal{L}(V)$. Suppose that $P_L$ splits over $\mathbb{F}$ and $\lambda \in \sigma(L)$ has algebraic multiplicity $m$. Then*

1. $\dim(K_L(\lambda)) \leq m$.
2. $K_L(\lambda) = \mathrm{Nul}((L - \lambda I_V)^m)$.

**Proof.**
*Proof of Part (1).* Letting $\dim(V) = n$, and recalling Corollary 6.28 and Definition 6.30, there exist $a_1, \ldots, a_{n-m} \in \mathbb{F}$ such that

$$P_L(t) = (-1)^n(t - \lambda)^m \prod_{k=1}^{n-m}(t - a_k),$$

where $a_k \neq \lambda$ for all $k$. Let $L_K = L|_{K_L(\lambda)}$. By Proposition 9.4(1), $L_K \in \mathcal{L}(K_L(\lambda))$ and $\lambda$ is an eigenvalue of $L_K$. From the latter fact it follows by Theorem 6.18 that $P_{L_K}(\lambda) = 0$, so that $t - \lambda$ is a factor of $P_{L_K}(t)$.

Suppose that $P_{L_K}(t)$ has a factor $t - \mu$ for some $\mu \neq \lambda$, so that $P_{L_K}(\mu) = 0$. Then $\mu$ is an eigenvalue of $L_K$ by Theorem 6.18 again, so there exists some $\mathbf{v} \neq \mathbf{0}$ in $K_L(\lambda)$ such that $L_K(\mathbf{v}) = \mu\mathbf{v}$, whence $(L_K - \mu I)(\mathbf{v}) = \mathbf{0}$. But $L_K - \mu I : K_L(\lambda) \to K_L(\lambda)$ is injective by

Proposition 9.4(2), so that $\text{Nul}(L_K - \mu I) = \{\mathbf{0}\}$ and hence $\mathbf{v} = \mathbf{0}$, which is a contradiction. Thus there exists no $\mu \neq \lambda$ such that $t - \mu$ is a factor of $P_{L_K}(t)$, and so

$$P_{L_K}(t) = (-1)^r (t - \lambda)^r \tag{9.2}$$

for some $1 \le r \le n$. However, $P_{L_K}(t)$ divides $P_L(t)$ by Proposition 4.55, and since $P_L(t)$ has precisely $m$ factors of the form $t - \lambda$, we conclude that $r \le m$. Observing that $\deg(P_{L_K}) = r$, we finally obtain

$$\dim(K_L(\lambda)) = \deg(P_{L_K}) \le m$$

by Corollary 6.28.

*Proof of Part (2).* Since $K_L(\lambda)$ is a finite-dimensional vector space and $L_K \in \mathcal{L}(K_L(\lambda))$, by the Cayley-Hamilton Theorem and (9.2) we have

$$P_{L_K}(L) = (-1)^r (L_K - \lambda I_K)^r = O_K,$$

where $I_K$ and $O_K$ represent the identity and zero operators on $K_L(\lambda)$, and $1 \le r \le m$. Thus $(L_K - \lambda I_K)^r = O_K$, and so for any $\mathbf{v} \in K_L(\lambda)$,

$$(L_K - \lambda I_K)^r(\mathbf{v}) = \mathbf{0}, \tag{9.3}$$

and then

$$(L_K - \lambda I_K)^m(\mathbf{v}) = (L_K - \lambda I_K)^{m-r}\big((L_K - \lambda I_K)^r(\mathbf{v})\big) = (L_K - \lambda I_K)^{m-r}(\mathbf{0}) = \mathbf{0}$$

shows that

$$\mathbf{v} \in \text{Nul}((L_K - \lambda I_K)^m) \subseteq \text{Nul}((L - \lambda I_V)^m).$$

(Observe that if $r = m$, then (9.3) delivers the desired outcome right away.) On the other hand if $\mathbf{v} \in \text{Nul}((L - \lambda I_V)^m)$, then it is immediate that $\mathbf{v} \in K_L(\lambda)$.

Therefore $K_L(\lambda) = \text{Nul}((L - \lambda I_V)^m)$. ■

## 9.2 – Jordan Form

# 10

# The Geometry of Vector Spaces

## 10.1 – Convex Sets

Recall that, if $V$ is a vector space over $\mathbb{R}$ and $\mathbf{u}, \mathbf{v} \in V$, then the line segment joining $\mathbf{u}$ and $\mathbf{v}$ is the set

$$L_{\mathbf{uv}} = \{(1-t)\mathbf{u} + t\mathbf{v} : 0 \leq t \leq 1\}.$$

A set $C \subseteq V$ that always contains the line segment joining two of its elements is of special interest.

**Definition 10.1.** *Let $V$ be a vector space over $\mathbb{R}$. A set $C \subseteq V$ is* ***convex*** *if $L_{\mathbf{uv}} \subseteq C$ for every $\mathbf{u}, \mathbf{v} \in C$.*

Notice that any vector space $V$ is convex: if $\mathbf{u}$ and $\mathbf{v}$ are in $V$, then any linear combination $c_1\mathbf{u} + c_2\mathbf{v}$ is also in $V$, which certainly includes any linear combination of the form $(1-t)\mathbf{u} + t\mathbf{v}$, $0 \leq t \leq 1$, and therefore $L_{\mathbf{uv}} \subseteq V$.

**Theorem 10.2.** *Let $V$ be a vector space over $\mathbb{R}$. For any $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ the set*

$$S = \left\{ \sum_{i=1}^n t_i\mathbf{v}_i \;\middle|\; t_1, \ldots, t_n \geq 0 \text{ and } \sum_{i=1}^n t_i = 1 \right\} \tag{10.1}$$

*is convex.*

**Proof.** Let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$. Fix $\mathbf{u}, \mathbf{w} \in S$, so that

$$\mathbf{u} = u_1\mathbf{v}_1 + \cdots + u_n\mathbf{v}_n \quad \text{and} \quad \mathbf{w} = w_1\mathbf{v}_1 + \cdots + w_n\mathbf{v}_n$$

for some $u_i, w_i \in \mathbb{R}$ such that $u_i, w_i \geq 0$ for all $1 \leq i \leq n$, and

$$\sum_{i=1}^n u_i = \sum_{i=1}^n w_i = 1.$$

Let $\mathbf{x} \in L_{\mathbf{uw}}$ be arbitrary, so $\mathbf{x} = (1-s)\mathbf{u} + s\mathbf{w}$ for some $s \in [0,1]$. It must be shown that $\mathbf{x} \in S$. Now,

$$\mathbf{x} = (1-s)(u_1\mathbf{v}_1 + \cdots + u_n\mathbf{v}_n) + s(w_1\mathbf{v}_1 + \cdots + w_n\mathbf{v}_n)$$

$$= [(1-s)u_1 + sw_1]\mathbf{v}_1 + \cdots + [(1-s)u_n + sw_n]\mathbf{v}_n,$$

where for each $i$ we clearly have $(1-s)u_i + sw_i \geq 0$, and

$$\sum_{i=1}^{n}[(1-s)u_i + sw_i] = (1-s)\sum_{i=1}^{n} u_i + s\sum_{i=1}^{n} w_i = (1-s)(1) + (s)(1) = (1-s) + s = 1.$$

Thus if we let $x_i = (1-s)u_i + sw_i$ for each $1 \leq i \leq n$, then

$$\mathbf{x} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n$$

with $x_i \geq 0$ for all $i$ and $x_1 + \cdots + x_n = 1$. Hence $\mathbf{x} \in S$, and since $\mathbf{x} \in L_{\mathbf{uw}}$ is arbitrary it follows that $L_{\mathbf{uw}} \subseteq S$. Since $\mathbf{u}, \mathbf{w} \in S$ are arbitrary we conclude that $L_{\mathbf{uw}} \subseteq S$ for all $\mathbf{u}, \mathbf{w} \in S$, and therefore $S$ is convex. ■

**Proposition 10.3.** *Let $V$ be a vector space over $\mathbb{R}$ and $C \subseteq V$ a convex set. If $\mathbf{v}_1, \ldots, \mathbf{v}_n \in C$ and $t_1, \ldots, t_n \geq 0$ with $\sum_{i=1}^{n} t_i = 1$, then $\sum_{i=1}^{n} t_i\mathbf{v}_i \in C$.*

The proof of this proposition will be done by induction.

**Proof.** In the case when $n = 1$, the statement of the proposition reads as: "If $\mathbf{v}_1 \in C$ and $t_1 \geq 0$ with $t_1 = 1$, then $t_1\mathbf{v}_1 \in C$". This is obviously true, and so the base case of the inductive argument is established.

Now assume the statement of the proposition is true for some arbitrary integer $n \geq 1$. Suppose that $\mathbf{v}_1, \ldots, \mathbf{v}_{n+1} \in C$ and $t_1, \ldots, t_{n+1} \geq 0$ with $t_1 + \cdots + t_{n+1} = 1$. It must be shown that $t_1\mathbf{v}_1 + \cdots + t_{n+1}\mathbf{v}_{n+1} \in C$.

If $t_{n+1} = 1$ then we must have $t_i = 0$ for all $1 \leq i \leq n$, whence

$$\sum_{i=1}^{n+1} t_i\mathbf{v}_i = \mathbf{v}_{n+1} \in C$$

and we're done.

Assuming that $t_{n+1} \neq 1$, observe that from $\sum_{i=1}^{n+1} t_i = 1$ we have

$$\sum_{i=1}^{n} t_i = 1 - t_{n+1},$$

and so

$$\sum_{i=1}^{n} \frac{t_i}{1 - t_{n+1}} = 1 \tag{10.2}$$

obtains since $1 - t_{n+1} \neq 0$. Now,

$$\sum_{i=1}^{n+1} t_i\mathbf{v}_i = \sum_{i=1}^{n} t_i\mathbf{v}_i + t_{n+1}\mathbf{v}_{n+1} = (1 - t_{n+1})\sum_{i=1}^{n} \frac{t_i}{1 - t_{n+1}}\mathbf{v}_i + t_{n+1}\mathbf{v}_{n+1},$$

where by the inductive hypothesis

$$\mathbf{u} = \sum_{i=1}^{n} \frac{t_i}{1 - t_{n+1}}\mathbf{v}_i$$

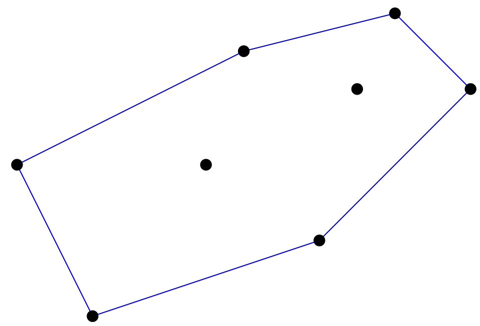


Figure 11. The convex hull of some points in $\mathbb{R}^2$.

is an element of $C$ because of (10.2) and the observation that

$$\frac{t_i}{1-t_{n+1}} \geq 0$$

for all $1 \leq i \leq n$. Thus, since $\mathbf{u}, \mathbf{v}_{n+1} \in C$,

$$\sum_{i=1}^{n+1} t_i \mathbf{v}_i = (1-t_{n+1})\mathbf{u} + t_{n+1}\mathbf{v}_{n+1}$$

for some $0 \leq t_{n+1} < 1$, and $C$ is convex, we conclude that $\sum_{i=1}^{n+1} t_i \mathbf{v}_i \in C$.

Therefore the statement of the proposition is true for $n+1$, and the proof is done. ■

We say that $C'$ is the **smallest** convex set containing $\mathbf{v}_1, \ldots, \mathbf{v}_n$ if, for any convex set $C$ such that $\mathbf{v}_1, \ldots, \mathbf{v}_n \in C$, we have $C' \subseteq C$.

**Corollary 10.4.** *Let $V$ be a vector space and $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$. Then the set $S$ given by* (10.1) *is the smallest convex set that contains $\mathbf{v}_1, \ldots, \mathbf{v}_n$.*

**Proof.** Let $C$ be a convex set containing $\mathbf{v}_1, \ldots, \mathbf{v}_n$. For any $\mathbf{x} \in S$ we have

$$\mathbf{x} = \sum_{i=1}^{n} t_i \mathbf{v}_i$$

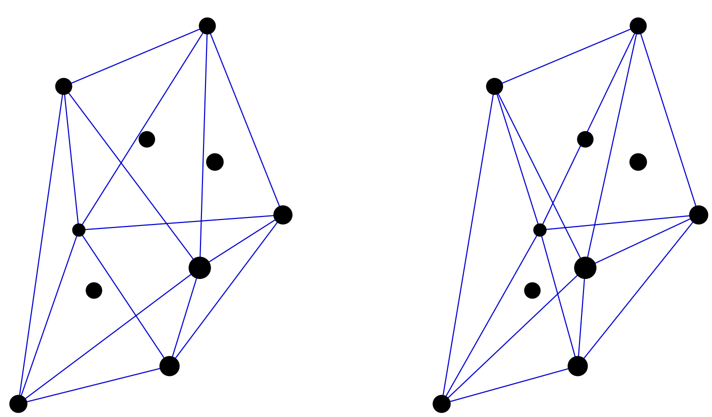


Figure 12. Stereoscopic image of the convex hull of some points in $\mathbb{R}^3$.

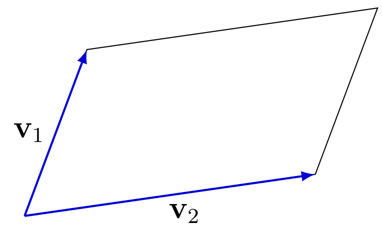



FIGURE 13. The parallelogram spanned by $\mathbf{v}_1$, $\mathbf{v}_2$.

for some $t_1, \ldots, t_n \geq 0$ such that $\sum_{i=1}^{n} t_i = 1$. But by Proposition 10.3 it then follows that $\mathbf{x} \in C$. Therefore $S \subseteq C$. ■

The **convex hull** of a set $A$, denoted here by Conv($A$), is defined to be the smallest convex set that contains $A$. It is easy to show that Conv($A$) is equal to the intersection of all convex sets $C$ that contain $A$:

$$\mathrm{Conv}(A) = \bigcap \{C : A \subseteq C \text{ and } C \text{ is convex}\}$$

Thus Corollary 10.3 states that

$$\mathrm{Conv}(\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}) = \left\{ \sum_{i=1}^{n} t_i \mathbf{v}_i \;\middle|\; t_1, \ldots, t_n \geq 0 \text{ and } \sum_{i=1}^{n} t_i = 1 \right\}.$$

See Figures 11 and 12.

Suppose that $\mathbf{v}_1$ and $\mathbf{v}_2$ are two linearly independent vectors in a vector space $V$. Then the **parallelogram spanned by $\mathbf{v}_1$ and $\mathbf{v}_2$** is the set of vectors (or points, if preferred)

$$\{t_1\mathbf{v}_1 + t_2\mathbf{v}_2 : 0 \leq t_1, t_2 \leq 1\}.$$

Note that $\mathbf{0}$ belongs to this set, as well as $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_1 + \mathbf{v}_2$. To see how the set forms a parallelogram in the geometric sense, we return to the practice introduced in Chapter 1 of representing vectors by arrows, which can still be done even if $V$ is not a Euclidean space (i.e. a vector space consisting of Euclidean vectors). See Figure 13.

**Definition 10.5.** *Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a linearly independent set of vectors in $V$. The **n-dimensional box spanned by** $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is the set*

$$B_n = \left\{ \sum_{i=1}^{n} t_i \mathbf{v}_i \;\middle|\; 0 \leq t_1, \ldots, t_n \leq 1 \right\}.$$

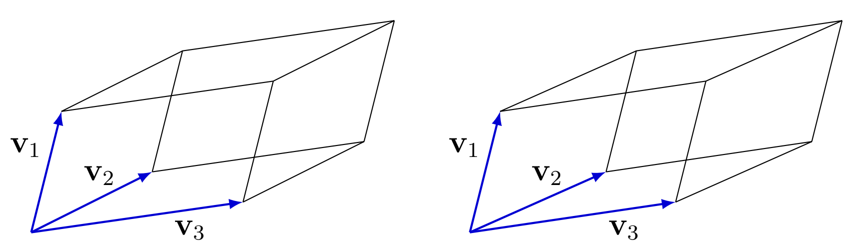



FIGURE 14. The parallelepiped spanned by $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$.

*In particular* $B_1$ *is the* ***line segment spanned by*** $\mathbf{v}_1$*,* $B_2$ *the* ***parallelogram spanned by*** $\mathbf{v}_1$ ***and*** $\mathbf{v}_2$ *and* $B_3$ *the* ***parallelepiped spanned by*** $\mathbf{v}_1$***,*** $\mathbf{v}_2$***, and*** $\mathbf{v}_3$*.*

For a depiction of a parallelepiped (or box) spanned by $\mathbf{v}_1$, $\mathbf{v}_2$, and $\mathbf{v}_3$, see Figure 14. It can be shown that the box $B_n$ is a convex set for any $n \in \mathbb{N}$.

# S

# Symbol Glossary

| | |
|---|---|
| $\mathbf{A}$ | The matrix $\mathbf{A}$. |
| $\mathbf{A}^\top$ | The transpose of $\mathbf{A} = [a_{ij}]$: the $ij$-entry of $\mathbf{A}^\top$ is $a_{ji}$. |
| $\overline{\mathbf{A}}$ | The conjugate of $\mathbf{A} = [a_{ij}]$: the $ij$-entry of $\overline{\mathbf{A}}$ is $\overline{a}_{ij}$. |
| $\mathbf{A}^*$ | The adjoint of $\mathbf{A}$: $\mathbf{A}^* = \left(\overline{\mathbf{A}}\right)^\top$. |
| $\lvert\mathbf{A}\rvert$ | The determinant of the matrix $\mathbf{A}$. |
| $\mathbf{A}_{ij}$ | The submatrix of $\mathbf{A}$ obtained by deleting the $i$th row and $j$th column of $\mathbf{A}$. |
| $\mathbf{A}_{i\star}$ | The submatrix of $\mathbf{A}$ obtained by deleting the $i$th row of $\mathbf{A}$. |
| $\mathbf{A}_{\star j}$ | The submatrix of $\mathbf{A}$ obtained by deleting the $j$th column of $\mathbf{A}$. |
| $(\mathbf{A})_{ij}$ | Same as $\mathbf{A}_{ij}$. Used for such expressions as $(\mathbf{A}^\top)_{ij}$ for clarity. |
| $[\mathbf{A}]_{ij}$ | The $ij$-entry of matrix $\mathbf{A}$. |
| $[a_{ij}]_{m,n}$ | An $m \times n$ matrix with $ij$-entry $a_{ij}$. |
| $[a_{ij}]_n$ | An $n \times n$ square matrix with $ij$-entry $a_{ij}$. |
| $[a_{ij}]$ | A matrix with dimensions either unspecified or understood from context. |
| $\mathbb{C}$ | The set of complex numbers. |
| $\delta_{ij}$ | The Kronecker delta: $\delta_{ij} = 0$ if $i \neq j$, $\delta_{ij} = 1$ if $i = j$. |
| $\mathbf{e}_j$ | The $j$th standard basis element of $\mathbb{R}^n$ or $\mathbb{C}^n$: $\mathbf{e}_j = [\delta_{ij}]_{n\times 1}$. |
| $E_{\mathbf{A}}(\lambda)$ | The eigenspace corresponding to the eigenvalue $\lambda$ of matrix $\mathbf{A}$. |
| $E_L(\lambda)$ | The eigenspace corresponding to the eigenvalue $\lambda$ of operator $L$. |

| | |
|---|---|
| $\mathbb{F}$ | An unspecified field, the elements of which are called scalars. |
| $\mathbb{F}^n$ | $\mathbb{F}^{1\times n}$ in Chapter 1, otherwise $\mathbb{F}^{n\times 1}$. |
| $\mathbb{F}^{m\times n}$ | Set of all $m \times n$ matrices with entries in $\mathbb{F}$. |
| $\varphi_{\mathcal{B}}$ | The coordinate map, where $\varphi_{\mathcal{B}}(\mathbf{v}) = [\mathbf{v}]_{\mathcal{B}}$. |
| $\gamma_{\mathbf{A}}(\lambda)$ | The geometric multiplicity of eigenvalue $\lambda$ of matrix $\mathbf{A}$. |
| $\gamma_L(\lambda)$ | The geometric multiplicity of eigenvalue $\lambda$ of operator $L$. |
| $\mathrm{Img}(L)$ | Image of linear mapping $L : V \to W$. $\mathrm{Img}(L) = \{L(\mathbf{v}) : \mathbf{v} \in V\}$. |
| $\mathbf{I}_{\mathcal{B}\mathcal{B}'}$ | The change of basis matrix from basis $\mathcal{B}$ to basis $\mathcal{B}'$. |
| $\mathbf{I}_n$ | The $n \times n$ identity matrix. |
| $\mathbf{I}$ | An identity matrix, dimensions unspecified or understood from context. |
| $I_V$ | The identity operator on vector space $V$: $I_V(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v} \in V$. |
| $[L]$ | Matrix corresponding to linear mapping $L$ with respect to any basis. |
| $[L]_{\mathcal{B}}$ | Matrix corresponding to linear operator $L$ with respect to the basis $\mathcal{B}$. |
| $[L]_{\mathcal{B}\mathcal{C}}$ | Matrix corresponding to linear mapping $L$ with respect to bases $\mathcal{B}$ and $\mathcal{C}$. |
| $L(V)$ | Image of $V$ under $L : V \to W$. $L(V) = \mathrm{Img}(L)$. |
| $\mathcal{L}(V)$ | Set of all linear operators $L : V \to V$ on some vector space $V$. |
| $\mathcal{L}(V, W)$ | Set of all linear mappings $L : V \to W$ on given vector spaces $V$ and $W$. |
| $\mu_{\mathbf{A}}(\lambda)$ | The algebraic multiplicity of eigenvalue $\lambda$ of matrix $\mathbf{A}$. |
| $\mu_L(\lambda)$ | The algebraic multiplicity of eigenvalue $\lambda$ of operator $L$. |
| $\mathrm{Nul}(L)$ | Null space of linear mapping $L : V \to W$. $\mathrm{Nul}(L) = \{\mathbf{v} \in V : L(\mathbf{v}) = \mathbf{0}\}$. |
| $\mathbb{N}$ | The set of natural numbers (i.e. positive integers): $\mathbb{N} = \{1, 2, 3, \ldots\}$. |
| $O$ | The zero mapping in $\mathcal{L}(V, W)$: $O(\mathbf{v}) = \mathbf{0}$ for all $\mathbf{v} \in V$. |
| $O_V$ | The zero operator on vector space $V$: $O_V(\mathbf{v}) = \mathbf{0}$ for all $\mathbf{v} \in V$. |
| $\mathbf{0}$ | The zero vector. |
| $\mathcal{F}(S, \mathbb{F})$ | The set of all functions $S \to \mathbb{F}$. |
| $\mathbf{0}_V$ | The zero vector of vector space $V$. |

| | |
|---|---|
| $\mathbf{O}_{m,n}$ | The $m \times n$ zero matrix (all entries are 0). |
| $\mathbf{O}_n$ | The $n \times n$ zero matrix (all entries are 0). |
| $\mathbf{O}$ | A zero matrix, dimensions unspecified or understood from context. |
| $\mathcal{O}$ | An orthonormal basis for an inner product space. |
| $\mathcal{P}_n(\mathbb{F})$ | The vector space of all polynomials of degree at most $n$ with coefficients in $\mathbb{F}$. |
| $\mathbb{Q}$ | The set of rational numbers. |
| $\mathbb{R}$ | The set of real numbers. |
| $\lvert S \rvert$ | The number of elements in the set $S$ (i.e. the cardinality of $S$) |
| $\mathrm{Sym}_n(\mathbb{F})$ | Set of all $n \times n$ symmetric matrices with entries in $\mathbb{F}$. |
| $\mathrm{Skw}_n(\mathbb{F})$ | Set of all $n \times n$ skew-symmetric matrices with entries in $\mathbb{F}$. |
| $\stackrel{s}{\sim}$ | The similar matrix relation. |
| $\sigma(\mathbf{A})$ | Set of all eigenvalues in $\mathbb{F}$ of a matrix $\mathbf{A} \in \mathbb{F}^{n \times n}$. |
| $\sigma(L)$ | Set of all eigenvalues in $\mathbb{F}$ of an operator $L \in \mathcal{L}(V)$. |
| $\mathbf{v}$ | The vector $\mathbf{v}$. |
| $\lVert\mathbf{v}\rVert$ | The norm or magnitude of $\mathbf{v}$; that is, $\lVert\mathbf{v}\rVert = \sqrt{\mathbf{v} \cdot \mathbf{v}}$ or $\lVert\mathbf{v}\rVert = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$ |
| $\hat{\mathbf{v}}$ | The normalization of vector $\mathbf{v}$; that is, $\hat{\mathbf{v}} = \mathbf{v}/\lVert\mathbf{v}\rVert$ |
| $[\mathbf{v}]_{\mathcal{B}}$ | The $\mathcal{B}$-coordinates of vector $\mathbf{v}$. |
| $\mathbb{W}$ | The set of whole numbers: $\mathbb{W} = \{0, 1, 2, 3, \ldots\}$. |
| $\mathbb{Z}$ | The set of integers: $\mathbb{Z} = \{1, -1, 2, -2, 3, -3, \ldots\}$. |
| $\langle\ \rangle$ | The inner product function. |
| $\langle\ \rangle_V$ | The inner product function of vector space $V$. |
| $\Rightarrow$ | Symbol for logical implication. Read as "implies" or "implies that." |
| $\Leftrightarrow$ | Symbol for logical equivalence. Read as "is equivalent to" or "if and only if." |