Melvyn B. Nathanson

Linear Algebra: A First Course

February 26, 2019

Springer

Contents

Part I
Solving systems of linear equations

Chapter 1
Linear Equations and Vector Spaces

1.1 One linear equation

Linear algebra begins with the problem of solving linear equations. For example,

$$2x = -10 \tag{1.1}$$

is a linear equation in one variable,

$$4x + 7y = 5 \tag{1.2}$$

is a linear equation in two variables, and

$$3x - 2y - 5z = 17 \tag{1.3}$$

is a linear equation in three variables. A *linear equation* in n variables $x_1, x_2, \ldots, x_n$ is an equation of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \tag{1.4}$$

where $a_1, a_2, \ldots, a_n$, and b are numbers. In linear algebra, a number is also called a *scalar*.

Equation (1.4) is *homogeneous* if $b = 0$ and *inhomogeneous* if $b \neq 0$.

Recall that Σ is the upper case Greek letter sigma. Using "sigma notation," we can write equation (1.4) in the form

$$\sum_{j=1}^{n} a_jx_j = b. \tag{1.5}$$

An equation can contain one variable or any finite number of variables. It is not important what symbols we use for the variables. If there is only one variable, we may write it as x or as x_1. If there are two variables, then we may write them as x, y

or as x_1, x_2. If there are three variables, then we may write them as x, y, z or as x_1, x_2, x_3.

A *solution* of equation (1.4) is a sequence $x_1, \ldots, x_n$ of numbers such that $\sum_{j=1}^{n} a_j x_j = b$. This is traditional notation, which has persisted despite the ambiguity in the use of x_n as both a variable and a scalar. A solution of the linear equation (1.4) is often written as a vertical n-tuple $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. This n-tuple is called an *n-dimensional column vector*, or, simply, a *vector*, and the scalars $x_1, \ldots, x_n$ are the *coordinates* of the vector.

The set of solutions of a linear equation is called the *solution space* of the equation. The solution space of a nonzero linear equation is also called a *hyperplane*,

The linear equation $4x + 7y = 5$ has the solution $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 \\ -1 \end{pmatrix}$. The identity

$$4(3-7t) + 7(-1+4t) = 5$$

is equivalent to the statement that

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3-7t \\ -1+4t \end{pmatrix} \tag{1.6}$$

is a solution of (1.2) for every scalar t, and so the solution space of equation (1.2) is infinite.

The linear equation $3x - 2y - 5z = 17$ has the solution $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \\ -4 \end{pmatrix}$. The identity

$$3(3+5t_1) - 2(6+5t_2) - 5(-4+3t_1-2t_2) = 17$$

is equivalent to the statement that

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3+5t_1 \\ 6+5t_2 \\ -4+3t_1-2t_2 \end{pmatrix} \tag{1.7}$$

is a solution of (1.3) for all scalars t_1 and t_2, and so the solution space of equation (1.3) is "doubly infinite."

Equation (1.4) is a *zero equation* if $a_j = 0$ for all $j = 1, \ldots, n$. Every vector $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ is a solution of the homogeneous zero equation, but an inhomogeneous zero equation has no solution.

Let $\mathbf{R}^n$ be the set of all n-dimensional column vectors with coordinates in the field $\mathbf{R}$. We use boldface letters to denote vectors. Two n-dimensional column vectors are equal if and only if their coordinates are equal. Thus, if $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and $\mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, then $\mathbf{x} = \mathbf{y}$ if and only if $x_j = y_j$ for all $j = 1, \ldots, n$. The n-dimensional *zero vector* is the vector $\mathbf{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ with all coordinates equal to 0.

We define addition of column vectors of the same dimension by adding their coordinates. We subtract column vectors of the same dimension by subtracting their coordinates. Thus, if

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad \text{and} \qquad \mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

then

$$\mathbf{x} + \mathbf{y} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix} \tag{1.8}$$

and

$$\mathbf{x} - \mathbf{y} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} - \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 - y_1 \\ \vdots \\ x_n - y_n \end{pmatrix}. \tag{1.9}$$

We cannot add or subtract column vectors of different dimensions.

We define multiplication of a column vector $\mathbf{x}$ by a scalar c by multiplying each coordinate of the vector by c:

$$c\mathbf{x} = c \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} cx_1 \\ \vdots \\ cx_n \end{pmatrix}. \tag{1.10}$$

Note that

$$\mathbf{x} - \mathbf{y} = \mathbf{x} + (-1)\mathbf{y}.$$

If $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ are vectors and $c_1, c_2, \ldots, c_n$ are scalars, then the vector

$$c_1\mathbf{x}_1 + c_2\mathbf{x}_2 + \cdots + c_n\mathbf{x}_n$$

is called a *linear combination* of $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ For example,

$$5\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} - 3\begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} + 2\begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix} = \begin{pmatrix} 5 \\ 10 \\ 15 \end{pmatrix} - \begin{pmatrix} 12 \\ 15 \\ 18 \end{pmatrix} + \begin{pmatrix} 14 \\ 16 \\ 18 \end{pmatrix} = \begin{pmatrix} 7 \\ 11 \\ 15 \end{pmatrix}.$$

The set $\mathbf{R}^n$ with these operations of *vector addition* and *scalar multiplication* is an example (the most important example) of a vector space.

The general solution (1.6) of equation (1.2) can be written in the form

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3-7t \\ -1+4t \end{pmatrix} = \begin{pmatrix} 3 \\ -1 \end{pmatrix} + \begin{pmatrix} -7t \\ 4t \end{pmatrix} = \begin{pmatrix} 3 \\ -1 \end{pmatrix} + t\begin{pmatrix} -7 \\ 4 \end{pmatrix}.$$

The general solution (1.7) of equation (1.3) can be written in the form

$$\begin{aligned} \begin{pmatrix} x \\ y \\ z \end{pmatrix} &= \begin{pmatrix} 3+5t_1 \\ 6+5t_2 \\ -4+3t_1-2t_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \\ -4 \end{pmatrix} + \begin{pmatrix} 5t_1 \\ 0 \\ 3t_1 \end{pmatrix} + \begin{pmatrix} 0 \\ 5t_2 \\ -2t_2 \end{pmatrix} \\ &= \begin{pmatrix} 3 \\ 6 \\ -4 \end{pmatrix} + t_1\begin{pmatrix} 5 \\ 0 \\ 3 \end{pmatrix} + t_2\begin{pmatrix} 0 \\ 5 \\ -2 \end{pmatrix}. \end{aligned}$$

The homogeneous linear equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$$

always has the *zero solution* $x_j = 0$ for all $j = 1,\dots,n$, that is, $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \mathbf{0}$. This is also called the *trivial solution*. A *nonzero solution* or a *nontrivial solution* of a homogeneous equation is a solution $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ with $x_j \neq 0$ for some j.

Theorem 1.1. *Every nonzero linear equation in n variables has a solution. If $n = 1$, then the solution is unique. If $n \geq 2$, then the equation has infinitely many solutions.*

Proof. Consider the linear equation in n variables

$$a_1x_1 + \cdots + a_nx_n = b.$$

If this equation is nonzero, then $a_{j_0} \neq 0$ for some $j_0 \in \{1,2,\dots,n\}$.

If $n = 1$, the equation is $a_1x_1 = b$ with $a_1 \neq 0$, and the unique solution is $x_1 = b/a_1$.

If $n \geq 2$, then for every sequence of $n-1$ numbers $x_1,\dots,x_{j_0-1},x_{j_0+1},\dots,x_n$, we define

$$x_{j_0} = \frac{1}{a_{j_0}}\left(b - \sum_{\substack{j=1 \\ j\neq j_0}}^{n} a_jx_j\right) \qquad \text{and} \qquad \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_{j_0-1} \\ x_{j_0} \\ x_{j_0+1} \\ \vdots \\ x_n \end{pmatrix}. \tag{1.11}$$

The n-dimensional vector $\mathbf{x}$ is a solution of the equation, and so the equation has infinitely many solutions. Moreover, every solution is of the form (1.11). This completes the proof.

For example, the solutions of the nonzero linear equation

$$3x - 2y + 5z = 7$$

are the column vectors

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ \frac{1}{5}(7 - 3x + 2y) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \frac{7}{5} \end{pmatrix} + x \begin{pmatrix} 1 \\ 0 \\ -\frac{3}{5} \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ \frac{2}{5} \end{pmatrix}$$

for all x and y.

Consider the two-variable linear equation

$$ax + by = c$$

with $(a,b) \neq (0,0)$. If $b \neq 0$, then for every number x we have

$$y = -\frac{a}{b}x + \frac{c}{b}.$$

This is the equation of a line in the plane with slope $-a/b$. We have

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -\frac{a}{b}x + \frac{c}{b} \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{c}{b} \end{pmatrix} + x \begin{pmatrix} 1 \\ -\frac{a}{b} \end{pmatrix}.$$

Because $x \begin{pmatrix} 1 \\ -\frac{a}{b} \end{pmatrix} = \frac{x}{b} \begin{pmatrix} b \\ -a \end{pmatrix}$, the solutions of the equation $ax + by = c$ can also be represented in the form

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{c}{b} \end{pmatrix} + x \begin{pmatrix} b \\ -a \end{pmatrix}.$$

If $b = 0$, then $a \neq 0$ and, for all $y \in \mathbf{R}$, we have

$$x = \frac{c}{a}.$$

This is the equation of a vertical line in the plane. In vector form, the solution is

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c/a \\ y \end{pmatrix} = \begin{pmatrix} c/a \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Exercises

1. Write the solutions of the following linear equations as vectors in $\mathbf{R}^2$:

a.
$$x + y = 0.$$
b.
$$x + y = 3.$$
c.
$$x + 3y = 1$$
d.
$$2x - 7y = -3$$

2. Write the solutions of the following linear equations as vectors in $\mathbf{R}^3$:

a.
$$x + y + z = 0.$$
b.
$$x + y + z = -7.$$
c.
$$x + 3y - 7z = 1$$
d.
$$5x - 2y + 3z = -11.$$

3. Write the solutions of the following linear equations as vectors in $\mathbf{R}^4$:

a.
$$x + y + z + w = 0$$
b.
$$x + y + z + w = -1$$
c.
$$x + 3y - 7z + 2w = 1$$
d.
$$3x - 2y - 6z + 4w = 12.$$

4. Compute the following linear combinations of vectors:

a. In the vector space $\mathbf{R}^2$,
$$7\begin{pmatrix}1\\0\end{pmatrix} - 5\begin{pmatrix}0\\1\end{pmatrix}$$
and
$$3\begin{pmatrix}7\\2\end{pmatrix} - 8\begin{pmatrix}9\\-1\end{pmatrix}$$

b. In the vector space $\mathbf{R}^3$,

$$\begin{pmatrix}1\\2\\3\end{pmatrix}+2\begin{pmatrix}4\\5\\6\end{pmatrix}+3\begin{pmatrix}7\\8\\9\end{pmatrix}$$

and

$$3\begin{pmatrix}8\\1\\3\end{pmatrix}-5\begin{pmatrix}9\\2\\6\end{pmatrix}+7\begin{pmatrix}3\\1\\3\end{pmatrix}$$

c. In the vector space $\mathbf{R}^5$,

$$8\begin{pmatrix}-1\\0\\1\\2\\3\end{pmatrix}+3\begin{pmatrix}4\\-7\\-5\\1\\1\end{pmatrix}-2\begin{pmatrix}7\\-8\\0\\1\\9\end{pmatrix}$$

5. In the vector space $\mathbf{R}^3$, let

$$\mathbf{e}_1=\begin{pmatrix}1\\0\\0\end{pmatrix},\qquad \mathbf{e}_2=\begin{pmatrix}0\\1\\0\end{pmatrix},\qquad \mathbf{e}_3=\begin{pmatrix}0\\0\\1\end{pmatrix}.$$

Prove that every vector $\mathbf{x}=\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\in\mathbf{R}^3$ has a unique representation as a linear combination of the vectors $\mathbf{e}_1$, $\mathbf{e}_2$, and $\mathbf{e}_3$.

6. In the vector space $\mathbf{R}^3$, let

$$\mathbf{f}_1=\begin{pmatrix}0\\1\\1\end{pmatrix},\qquad \mathbf{f}_2=\begin{pmatrix}1\\0\\1\end{pmatrix},\qquad \mathbf{f}_3=\begin{pmatrix}1\\1\\0\end{pmatrix}.$$

Prove that every vector $\mathbf{x}=\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\in\mathbf{R}^3$ has a unique representation as a linear combination of the vectors $\mathbf{f}_1$, $\mathbf{f}_2$, and $\mathbf{f}_3$.

7. Prove that if

$$x\begin{pmatrix}1\\2\end{pmatrix}+y\begin{pmatrix}1\\3\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$$

then $x=y=0$.

1.2 Vector spaces and affine spaces in $\mathbf{R}^n$

In $\mathbf{R}^n$, the operations of vector addition and scalar multiplication satisfy the following simple properties:

1. Vector addition is *associative*: For all vectors $\mathbf{x}, \mathbf{y}, \mathbf{z}$, we have
$$(\mathbf{x}+\mathbf{y})+\mathbf{z} = \mathbf{x}+(\mathbf{y}+\mathbf{z}).$$
2. Vector addition is *commutative*: For all vectors $\mathbf{x}, \mathbf{y}$, we have
$$\mathbf{x}+\mathbf{y} = \mathbf{y}+\mathbf{x}.$$
3. The vector $\mathbf{0}$ satisfies
$$\mathbf{0}+\mathbf{x} = \mathbf{x}+\mathbf{0} = \mathbf{x}$$
for all $\mathbf{x}$. The element $\mathbf{0}$ is called the *additive identity*.
4. For every element $\mathbf{x}$ there is a element $\mathbf{y}$ such that
$$\mathbf{x}+\mathbf{y} = \mathbf{y}+\mathbf{x} = \mathbf{0}.$$
The element $\mathbf{y}$ is called an *additive inverse* of $\mathbf{x}$.
5. For every vector $\mathbf{x}$, scalar multiplication by 1 satisfies
$$1\mathbf{x} = \mathbf{x}.$$
6. For all scalars a, b and for every vector $\mathbf{x}$,
$$(ab)\mathbf{x} = a(b\mathbf{x}).$$
7. Vector addition and scalar multiplication satisfy the *distributative laws*:
$$a(\mathbf{x}+\mathbf{y}) = a\mathbf{x}+a\mathbf{y}$$
and
$$(a+b)\mathbf{x} = a\mathbf{x}+b\mathbf{x}$$
for all scalars a, b and all vectors $\mathbf{x}, \mathbf{y}$.

To prove that addition of vectors is associative, let

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}, \quad \text{and} \quad \mathbf{z} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}.$$

We have

$$\begin{aligned}(\mathbf{x}+\mathbf{y})+\mathbf{z} &= \begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix} + \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} (x_1+y_1)+z_1 \\ \vdots \\ (x_n+y_n)+z_n \end{pmatrix} \\ &= \begin{pmatrix} x_1+(y_1+z_1) \\ \vdots \\ x_n+(y_n+z_n) \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1+z_1 \\ \vdots \\ y_n+z_n \end{pmatrix} \\ &= \mathbf{x}+(\mathbf{y}+\mathbf{z}).\end{aligned}$$

Similarly,

$$\mathbf{x}+\mathbf{y} = \begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix} = \begin{pmatrix} y_1+x_1 \\ \vdots \\ y_n+x_n \end{pmatrix} = \mathbf{y}+\mathbf{x}$$

and so vector addition is commutative.

Verification of the other properties of vector addition and scalar multiplication is similarly straightforward (Exercises 14 and 15).

Lemma 1.1. *The additive inverse of a vector* $\mathbf{x}$ *in* $\mathbf{R}^n$ *is unique.*

Proof. If $\mathbf{y}$ and $\mathbf{z}$ are additive inverses of $\mathbf{x}$, then $\mathbf{x}+\mathbf{z} = \mathbf{y}+\mathbf{x} = \mathbf{0}$. It follows that

$$\mathbf{y} = \mathbf{y}+\mathbf{0} = \mathbf{y}+(\mathbf{x}+\mathbf{z}) = (\mathbf{y}+\mathbf{x})+\mathbf{z} = \mathbf{0}+\mathbf{z} = \mathbf{z}.$$

This completes the proof.

Let $-\mathbf{x}$ denote the unique additive inverse of $\mathbf{x}$. We have $-\mathbf{x} = \begin{pmatrix} -x_1 \\ \vdots \\ -x_n \end{pmatrix} \in \mathbf{R}^n$. We define *subtraction* of vectors as follows: For all $\mathbf{x},\mathbf{y} \in \mathbf{R}^n$,

$$\mathbf{x}-\mathbf{y} = \mathbf{x}+(-\mathbf{y}).$$

Let W be a subset of $\mathbf{R}^n$. The subset W is *closed under vector addition* if, for all $\mathbf{x},\mathbf{y} \in W$, we have $\mathbf{x}+\mathbf{y} \in W$. The subset W is *closed under scalar multiplication* if, for all $\mathbf{x} \in W$ and for all $c \in \mathbf{R}$, we have $c\mathbf{x} \in W$. A *vector subspace* of $\mathbf{R}^n$ is a subset W of $\mathbf{R}^n$ such that

(i) W contains the zero vector $\mathbf{0}$,
(ii) W is closed under vector addition, and
(iii) W is closed under scalar multiplication.

A vector subspace is also called, simply, a *subspace*.

For example, the set $\mathbf{R}^n$ is closed under vector addition and scalar multiplication, and so $\mathbf{R}^n$ is a vector subspace of $\mathbf{R}^n$. Similarly, the set $\{\mathbf{0}\}$, which contains only the zero vector, is closed under vector addition and scalar multiplication, and so $\{\mathbf{0}\}$ is a vector subspace of $\mathbf{R}^n$. If $\mathbf{v}$ is a nonzero vector in $\mathbf{R}^n$, then $W = \{c\mathbf{v} : c \in \mathbf{R}\}$, which is the set of all scalar multiples of $\mathbf{v}$, is closed under vector addition and scalar multiplication, is a vector subspace of $\mathbf{R}^n$ (Exercise 11).

Note that if W is closed under vector addition and scalar multiplication, then, for all $\mathbf{x}, \mathbf{y} \in \mathbf{R}^n$, we have

$$\mathbf{x} - \mathbf{y} = \mathbf{x} + (-1)\mathbf{y} \in W$$

and so W is also closed under vector subtraction.

A subset W of $\mathbf{R}^n$ is *closed under linear combinations* if, for all positive integers k and for all vectors $\mathbf{x}_1, \ldots, \mathbf{x}_k \in W$ and all scalars $c_1, \ldots, c_k$, we have $c_1\mathbf{x}_1 + c_2\mathbf{x}_2 + \cdots + c_k\mathbf{x}_k \in W$.

Lemma 1.2. *A subset W of $\mathbf{R}^n$ is a vector subspace if and only if W is nonempty and closed under linear combinations.*

Proof. Let W be nonempty and closed under linear combinations. Because W is nonempty, there exists a vector $\mathbf{x} \in W$. Because W is closed under linear combinations, $\mathbf{0} = 0\mathbf{x} \in W$. For all $\mathbf{x}_1, \mathbf{x}_2 \in W$, we have

$$\mathbf{x}_1 + \mathbf{x}_2 = 1\mathbf{x}_1 + 1\mathbf{x}_2 \in W.$$

For all $\mathbf{x} \in W$ and $c \in \mathbf{R}$, we have

$$c\mathbf{x} \in W.$$

Thus, W is closed under vector addition and scalar multiplication, and so W is a subspace.

Conversely, let W be a subspace. We have $\mathbf{0} \in W$ and so W is nonempty. We shall prove, by induction on k, that W contains every linear combination of k vectors in W.

Let $\mathbf{x}_1, \ldots, \mathbf{x}_k$ be vectors in W, and let $c_1, \ldots, c_k$ be scalars. For $k = 1$, we have $c_1\mathbf{x}_1 \in W$ because a subspace is closed under scalar multiplication.

Similarly, for $k = 2$, we have $c_1\mathbf{x}_1 \in W$ and $c_2\mathbf{x}_2 \in W$, and so $c_1\mathbf{x}_1 + c_2\mathbf{x}_2 \in W$ because a subspace is closed under scalar multiplication and vector addition.

Let $k \geq 2$, and suppose that W contains every linear combination of k vectors. Let $\mathbf{x}_1, \ldots, \mathbf{x}_k, , \mathbf{x}_{k+1}$ be vectors in W, and let $c_1, \ldots, c_k, c_{k+1}$ be scalars. By the induction assumption, W contains the linear combination

$$c_1\mathbf{x}_1 + \cdots + c_k\mathbf{x}_k$$

and W also contains $c_{k+1}\mathbf{x}_{k+1}$. Because W is closed under vector addition, W contains the linear combination

$$c_1\mathbf{x}_1 + \cdots + c_k\mathbf{x}_k + c_{k+1}\mathbf{x}_{k+1}.$$

This completes the proof.

Lemma 1.3. *The set of all linear combinations of a nonempty finite set of vectors is a vector subspace.*

Proof. Let $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_\ell\}$ be a nonempty finite set of vectors, and let W be the set of all linear combinations of vectors in S. We have

$$\mathbf{v}_i = 1 \cdot \mathbf{v}_i + \sum_{\substack{r=1 \\ r \neq i}}^{\ell} 0 \cdot \mathbf{v}_r \in W$$

for all $i = 1, \ldots, \ell$, and so $S \subseteq W$. Thus, W is nonempty. If $\mathbf{x}_1, \ldots, \mathbf{x}_k \in W$, then there exist scalars $a_{i,j}$ for $i = 1, \ldots, \ell$ and $j = 1, \ldots, k$ such that

$$\mathbf{x}_j = \sum_{i=1}^{m} a_{i,j} \mathbf{v}_i.$$

Let $c_1, \ldots, c_k$ be scalars. We have

$$\sum_{j=1}^{k} c_j \mathbf{x}_j = \sum_{j=1}^{k} c_j \sum_{i=1}^{\ell} a_{i,j} \mathbf{v}_i = \sum_{i=1}^{\ell} \sum_{j=1}^{k} c_j a_{i,j} \mathbf{v}_i = \sum_{i=1}^{\ell} b_i \mathbf{v}_i$$

where

$$b_i = \sum_{j=1}^{k} c_j a_{i,j} \in \mathbf{R}$$

for $i = 1, \ldots, \ell$, and so $\sum_{j=1}^{k} c_j \mathbf{x}_j$ is a linear combination of vectors in S. Thus, W is closed under linear combinations, and, by Lemma 1.2, the set W is a subspace. This completes the proof.

Consider the homogeneous equation

$$3x_1 - 2x_2 + x_3 = 0. \tag{1.12}$$

This equation has many solutions. For example, the vectors

$$\begin{pmatrix} 1 \\ -1 \\ -5 \end{pmatrix}, \qquad \begin{pmatrix} 9 \\ 8 \\ -11 \end{pmatrix}, \qquad \text{and} \qquad \begin{pmatrix} 0 \\ 3 \\ 6 \end{pmatrix}$$

are solutions. If $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ is a solution, then

$$x_3 = -3x_1 + 2x_2$$

and so

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ -3x_1 + 2x_2 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$$

Thus, the set of solutions of the homogeneous equation (1.12) is

$$W = \left\{ x_1 \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} : x_1, x_2 \in \mathbf{R} \right\},$$

which is the set of all linear combinations of vectors in the set $S = \left\{ \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right\}$, and so W is a subspace of $\mathbf{R}^3$.

Theorem 1.2. *The set W of solutions of the homogeneous linear equation*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0 \tag{1.13}$$

is a vector subspace of $\mathbf{R}^n$.

The solution space of a homogeneous linear equation is also called the *kernel* of the equation.

Proof. For all scalars $a_1, a_2, \ldots, a_n$ we have

$$a_1 \cdot 0 + a_2 \cdot 0 + \cdots + a_n \cdot 0 = 0$$

and so W contains the zero vector $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$.

Let $\mathbf{x}, \mathbf{y} \in W$ and $c \in \mathbf{R}$. Because $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and $\mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ are solutions of equation (1.13), we have

$$a_1x_1 + \cdots + a_nx_n = 0$$

and

$$a_1y_1 + \cdots + a_ny_n = 0.$$

Adding these equations, we obtain

$$a_1(x_1 + y_n) + \cdots + a_n(x_n + y_n) \cdot 0 = 0$$

and so $\mathbf{x} + \mathbf{y} = \begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix}$ is also a solution of (1.13). Thus, W is a nonempty set of vectors that is closed under vector addition.

Also,

$$a_1(cx_1) + \cdots + a_n(cx_n) = c\,(a_1x_1 + \cdots + a_nx_n) = c \cdot 0 = 0$$

and so $c\mathbf{x} \in W$. Thus, W is also closed under scalar multiplication, and so W is a vector subspace. This completes the proof.

Every vector $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{R}^n$ is a solution of the zero equation in n variables:

$$0 \cdot x_1 + 0 \cdot x_2 + \cdots + 0 \cdot x_n = 0.$$

Thus, the kernel of the zero equation is $\mathbf{R}^n$. If equation (1.13) is nonzero, then $a_k \neq 0$ for some $k \in \{1, \ldots, n\}$. Consider the vector $\mathbf{e}_k = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ with $x_k = 1$ and $x_j = 0$ for $j \neq k$. We have

$$a_1x_1 + \cdots + a_kx_k + \cdots a_nx_n = a_k \neq 0$$

and so $\mathbf{x}$ is not in the kernel of the equation. Thus, the kernel of a nonzero homogeneous equation is a proper subset of $\mathbf{R}^n$.

Consider the inhomogeneous equation

$$3x_1 - 2x_2 + x_3 = 6. \tag{1.14}$$

This equation has many solutions. For example, the vectors

$$\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} 9 \\ 8 \\ -5 \end{pmatrix}, \qquad \text{and} \qquad \begin{pmatrix} 0 \\ 3 \\ 12 \end{pmatrix}$$

are solutions. The vector $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ is a solution of (1.14) if and only if

$$x_3 = 6 - 3x_1 + 2x_2$$

if and only if

$$\begin{aligned} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &= \begin{pmatrix} x_1 \\ x_2 \\ 6 - 3x_1 + 2x_2 \end{pmatrix} = \begin{pmatrix} 0 + 1 \cdot x_1 + 0 \cdot x_2 \\ 0 + 0 \cdot x_1 + 1 \cdot x_2 \\ 6 - 3 \cdot x_1 + 2 \cdot x_2 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ 6 \end{pmatrix} + x_1 \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \end{aligned}$$

Thus, the set of solutions of the inhomogeneous equation (1.14) is

$$L = \left\{ \begin{pmatrix} 0 \\ 0 \\ 6 \end{pmatrix} + x_1 \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} : x_1, x_2 \in \mathbf{R} \right\}.$$

For example,

$$\begin{pmatrix}1\\-1\\1\end{pmatrix} = \begin{pmatrix}0\\0\\6\end{pmatrix} + 1\begin{pmatrix}1\\0\\-3\end{pmatrix} + (-1)\begin{pmatrix}0\\1\\2\end{pmatrix}$$
$$\begin{pmatrix}9\\8\\-5\end{pmatrix} = \begin{pmatrix}0\\0\\6\end{pmatrix} + 9\begin{pmatrix}1\\0\\-3\end{pmatrix} + 8\begin{pmatrix}0\\1\\2\end{pmatrix}$$
$$\begin{pmatrix}0\\3\\12\end{pmatrix} = \begin{pmatrix}0\\0\\6\end{pmatrix} + 0\begin{pmatrix}1\\0\\-3\end{pmatrix} + 3\begin{pmatrix}0\\1\\2\end{pmatrix}.$$

Let

$$\mathbf{v} = \begin{pmatrix}0\\0\\6\end{pmatrix} \qquad \text{and} \qquad W = \left\{ x_1\begin{pmatrix}1\\0\\-3\end{pmatrix} + x_2\begin{pmatrix}0\\1\\2\end{pmatrix} : x_1, x_2 \in \mathbf{R} \right\}.$$

Note that W is a subspace of $\mathbf{R}^3$ and that

$$L = \mathbf{v} + W = \{\mathbf{v} + \mathbf{x} : \mathbf{x} \in W\}.$$

The *translate* of a set W of vectors in $\mathbf{R}^n$ by a vector $\mathbf{v}^* \in \mathbf{R}^n$ is the set

$$\mathbf{v} + W = \{\mathbf{v}^* + \mathbf{x} : \mathbf{x} \in W\}.$$

An *affine subspace* of $\mathbf{R}^n$ is a translate of a vector subspace of $\mathbf{R}^n$. Thus, the set of solutions of the inhomogeneous linear equation (1.14) is an affine subspace of $\mathbf{R}^3$.

Because $\mathbf{0} + W = W$, every vector subspace is also an affine subspace.

For every scalar m, the set

$$W = \left\{ \begin{pmatrix}x\\mx\end{pmatrix} : x \in \mathbf{R} \right\}$$

is a vector subspace of $\mathbf{R}^2$. This the set of points $\begin{pmatrix}x\\y\end{pmatrix} \in \mathbf{R}^2$ with $y = mx$. Geometrically, this is the line through the origin with slope m. The translate of W by the vector $\begin{pmatrix}0\\b\end{pmatrix}$ is the affine subspace

$$L = \begin{pmatrix}0\\b\end{pmatrix} + W = \left\{ \begin{pmatrix}x\\mx+b\end{pmatrix} : x \in \mathbf{R} \right\}.$$

This is the set of points $\begin{pmatrix}x\\y\end{pmatrix} \in \mathbf{R}^2$ with $y = mx + b$. Geometrically, this is the line in the plane with slope m and y-intercept b.

Theorem 1.3. *Let $b \neq 0$. The set L of solutions of the nonzero inhomogeneous linear equation*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \tag{1.15}$$

is an affine subspace of $\mathbf{R}^n$. *It is not a vector subspace of* $\mathbf{R}^n$.

Proof. By Theorem 1.1, equation (1.15) has a solution $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbf{R}^n$. Thus,

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n = b.$$

Let W be the set of solutions of the associated homogeneous equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0.$$

By Theorem 1.5, W is a vector subspace of $\mathbf{R}^n$. If $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in W$, then

$$\begin{aligned} &a_1(v_1+x_1) + a_2(v_2+x_2) + \cdots + a_n(v_n+x_n) \\ &\qquad = (a_1v_1 + a_2v_2 + \cdots + a_nv_n) + (a_1x_1 + a_2x_2 + \cdots + a_nx_n) \\ &\qquad = b + 0 = b \end{aligned}$$

and so $\mathbf{v} + \mathbf{x} \in L$. Therefore, $\mathbf{v} + W \subseteq L$.

Conversely, if $\mathbf{v}' = \begin{pmatrix} v_1' \\ \vdots \\ v_n' \end{pmatrix} \in L$ and $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in L$, then

$$a_1v_1' + a_2v_2' + \cdots + a_nv_n' = b$$

and

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n = b.$$

Subtracting these equations, we obtain

$$a_1(v_1' - v_1) + \cdots + a_n(v_n' - v_n) = 0.$$

It follows that $\mathbf{x} = \mathbf{v}' - \mathbf{v} = \begin{pmatrix} v_1' - v_1 \\ \vdots \\ v_n' - v_n \end{pmatrix} \in W$ and so $\mathbf{v}' = \mathbf{v} + \mathbf{x} \in \mathbf{v} + W$. Therefore, $L \subseteq \mathbf{v} + W$. Therefore, $L = \mathbf{v} + W$ is an affine subspace of $\mathbf{R}^n$.

Note that

$$a_1 0 + a_2 0 + \cdots + a_n 0 = 0 \neq b$$

and so L does not contain the zero vector $\mathbf{0}$. Therefore, L is not a vector subspace of $\mathbf{R}^n$. This completes the proof.

Exercises

1. a. Let W be the vector subspace of solutions of the homogeneous linear equation

$$5x - 8y = 0.$$

Compute a set S of vectors in $\mathbf{R}^2$ such that W is the set of linear combinations of vectors in S.

b. Let L be the affine subspace of solutions of the inhomogeneous linear equation

$$5x - 8y = 1.$$

Compute a vector $\mathbf{v}$ such that $L = \mathbf{v} + W$.

2. a. Let W be the vector subspace of solutions of the homogeneous linear equation

$$5x - 8y - 2z = 0.$$

Compute a set S of vectors in $\mathbf{R}^3$ such that W is the set of linear combinations of vectors in S.

b. Let L be the affine subspace of solutions of the inhomogeneous linear equation

$$5x - 8y - 2z = 3.$$

Compute a vector $\mathbf{v}$ such that $L = \mathbf{v} + W$.

3. Let L be the set of solutions of the inhomogeneous linear equation

$$x_1 + 2x_2 + 3x_3 + 4x_4 = 15.$$

Write L as an affine subspace.

4. In the vector space $\mathbf{R}^2$, draw the vector subspace

$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 : x + y = 0 \right\}$$

and the affine subspaces

$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 : x + y = c \right\}$$

for $c = -2, -1, 1, 2$.

5. Consider the affine subspace

$$L = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 : x + y = 1 \right\}$$

Prove that

$$\begin{pmatrix} x \\ y \end{pmatrix} \in L$$

if and only if

$$\begin{pmatrix} x \\ y \end{pmatrix} = (1-t)\begin{pmatrix} 1 \\ 0 \end{pmatrix} + t\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

for some $t \in \mathbf{R}$.

6. In the vector space $\mathbf{R}^2$, draw the vector subspace

$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 : 5x - 2y = 0 \right\}$$

and the affine subspaces

$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 : 5x - 2y = c \right\}$$

for $c = -2, -1, 1, 2$.

7. In the vector space $\mathbf{R}^3$, draw the vector subspace

$$\left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbf{R}^3 : x + y + z = 0 \right\}$$

and the affine subspaces

$$\left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbf{R}^3 : x + y + z = c \right\}$$

for $c = -2, -1, 1, 2$.

8. Let $\mathbf{v} \in \mathbf{R}^n$ and let W be a vector subspace of $\mathbf{R}^n$. Prove that $\mathbf{v} + W = W$ if and only if $\mathbf{v} \in W$.
9. Let W be a vector subspace of $\mathbf{R}^n$, and let $\mathbf{v} \in \mathbf{R}^n$. Consider the affine subspace $L = \mathbf{v} + W$ of $\mathbf{R}^n$. Prove that if $\mathbf{x}, \mathbf{y} \in L$, then $(1-t)\mathbf{x} + t\mathbf{y} \in L$ for all scalars t.
Note: The set $\{(1-t)\mathbf{x} + t\mathbf{y} : t \in \mathbf{R}\}$ is called the *line through* $\mathbf{x}$ *and* $\mathbf{y}$.
10. Let W be a vector subspace of $\mathbf{R}^n$, and let $\mathbf{v} \in \mathbf{R}^n$. Consider the affine subspace $L = \mathbf{v} + W$ of $\mathbf{R}^n$. Prove that if $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k$ are vectors in L, and if $t_1, t_2, \ldots, t_k$ are scalars such that

$$t_1 + t_2 + \cdots + t_k = 1$$

then

$$t_1\mathbf{x}_1 + t_2\mathbf{x}_2 + \cdots + t_k\mathbf{x}_k \in L.$$

Note: The vector $t_1\mathbf{x}_1 + t_2\mathbf{x}_2 + \cdots + t_k\mathbf{x}_k \in L$ is called an *affine combination* of the vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k$.

11. Let $\mathbf{v}$ be a nonzero vector in $\mathbf{R}^n$. Prove that $W = \{c\mathbf{v} : c \in \mathbf{R}\}$ is a vector subspace of $\mathbf{R}^n$.
12. The *closed unit interval* is the set

$$[0,1] = \{t \in \mathbf{R} : 0 \leq t \leq 1\}.$$

A nonempty subset Ω of $\mathbf{R}^n$ is *convex* if, for all $\mathbf{x}_1, \mathbf{x}_2 \in \Omega$ and for all $t \in [0,1]$,

$$t\mathbf{x}_1 + (1-t)\mathbf{x}_2 \in \Omega.$$

Prove that the following sets are convex:

a. The unit interval
$$[0,1] \subseteq \mathbf{R}.$$
b. The n-dimensional *unit cube*
$$[0,1]^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{R}^n : x_j \in [0,1] \text{ for all } j = 1, \ldots, n \right\}.$$
c. The 1-*dimensional simplex*
$$\Delta_1 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 : x, y \in [0,1] \text{ and } x + y = 1 \right\}.$$
Draw the 1-dimensional simplex in $\mathbf{R}^2$.
d. The *n-dimensional simplex*
$$\Delta_n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ x_{n+1} \end{pmatrix} \in \mathbf{R}^{n+1} : x_j \in [0,1] \text{ for all } j = 1, \ldots, n, n+1 \text{ and } \sum_{j=1}^{n+1} x_j = 1 \right\}.$$
Draw the 2-dimensional simplex in $\mathbf{R}^3$.

13. Let Ω be a convex set. Let $x_1, \ldots, x_k \in \Omega$. Prove that if $t_1, \ldots, t_k \in [0,1]$ and $\sum_{j=1}^k t_j = 1$, then $\sum_{j=1}^k t_j \mathbf{x}_j \in \Omega$.
Hint: Induction on k.
14. Let $\mathbf{x}$ and $\mathbf{y}$ be vectors in $\mathbf{R}^n$, and let a and b be scalars.
   a. Prove that $(ab)\mathbf{x} = a(b\mathbf{x})$.
   b. Prove that $a(\mathbf{x} + \mathbf{y}) = a\mathbf{x} + a\mathbf{y}$.
   c. Prove that $(a+b)\mathbf{x} = a\mathbf{x} + b\mathbf{x}$.
15. Let 0 be the scalar zero and let $\mathbf{0}$ be the zero vector in $\mathbf{R}^n$.
   a. Let $\mathbf{x} \in \mathbf{R}^n$ and $a \in \mathbf{R}$. Prove that $0\mathbf{x} = \mathbf{0}$ and that $a\mathbf{0} = \mathbf{0}$.
   b. Prove that $1\mathbf{x} = \mathbf{x}$.

1.3 Systems of linear equations

A *system of linear equations* consists of a finite number of linear equations in a finite number of variables. For example,

$$\begin{aligned} 3x+2y &= 18 \\ 4x+3y &= -5 \end{aligned} \tag{1.16}$$

is a system of two equations in two variables. The vector $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 64 \\ -87 \end{pmatrix}$ is the unique solution of this system (Exercise 1).

Let m and n be positive integers. We write a system of m linear equations in n variables in the following standard form:

$$\left.\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,j}x_j + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,j}x_j + \cdots + a_{2,n}x_n &= b_2 \\ &\vdots \\ a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,j}x_j + \cdots + a_{i,n}x_n &= b_i \\ &\vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,j}x_j + \cdots + a_{m,n}x_n &= b_m. \end{aligned}\right\} \tag{1.17}$$

where $a_{i,j} \in \mathbf{R}$ and $b_i \in \mathbf{R}$ for all $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,n\}$. The ith equation in this system is

$$\sum_{j=1}^{m} a_{i,j}x_j = a_{i,1}x_1 + \cdots + a_{i,j}x_j + \cdots + a_{i,n}x_n = b_i.$$

It is standard notation in linear algebra that the coefficient of the variable x_j in the ith equation is denoted $a_{i,j}$. The system of equations is *nonzero* if $a_{i,j} \neq 0$ for at least one pair (i,j) with $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,n\}$.

A *solution* of the system of equations (1.17) is a vector $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{R}^n$ such that $\sum_{j=1}^{m} a_{i,j}x_j = b_i$ for all $i = 1,\ldots,m$. The system of equations (1.17) is *consistent* if it has at least one solution, and *inconsistent* if it has no solution. The system of equations (1.16) is consistent. The system of equations

$$\begin{aligned} x+y &= 0 \\ x+y &= 1 \end{aligned}$$

is inconsistent because $0 \neq 1$.

The set of solutions of a system of linear equations is called the *solution space* of the equations. A vector $\mathbf{x} \in \mathbf{R}^n$ is in the solution space of the system (1.17) if and only if $\mathbf{x}$ is in the solution space of each of the m equations in the system. Recall that the solution space of a nonzero equation is called a *hyperplane*, and so the solution space of a nonzero system of linear equations is the intersection of a finite number of hyperplanes.

The linear system (1.17) is *homogeneous* if $b_i = 0$ for all $i = 1, \ldots, m$ and *inhomogeneous* if $b_i \neq 0$ for some i. A homogeneous system of linear equations always has the *zero solution* $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$, that is, $x_j = 0$ for all $j = 1, \ldots, n$, and so every homogeneous system is consistent. A *nonzero solution* of a homogeneous system is a solution $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ with $x_j \neq 0$ for at least one $j \in \{1, \ldots, n\}$. The zero solution of a homogeneous system is called the *trivial solution*, and a nonzero solution of a homogeneous system is called a *nontrivial solution*.

The solution space of a system of homogeneous linear equations is also called the *kernel* of the system.

For example, the homogeneous system

$$\begin{aligned} x + y + z &= 0 \\ 4x - 3y - 10z &= 0 \end{aligned} \tag{1.18}$$

consists of two equations in three variables. Multiplying the first equation by 4, we obtain the system

$$\begin{aligned} 4x + 4y + 4z &= 0 \\ 4x - 3y - 10z &= 0. \end{aligned}$$

Subtracting the second equation from the first equation gives

$$7y + 14z = 0$$

or

$$y = -2z.$$

Substituting $y = -2z$ into $x + y + z = 0$ gives

$$x = z$$

and so every solution of (1.18) is of the form

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} z \\ -2z \\ z \end{pmatrix} = z \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}.$$

Thus, the solution space of (1.18) is the vector subspace

$$W = \left\{ z \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} : z \in \mathbf{R} \right\}.$$

Theorem 1.4. *The solution space of a system of homogeneous linear equations is a vector subspace.*

Proof. Let W be the solution space of the system of equations (1.17) with $b_i = 0$ for all $i = 1, \dots, m$. The zero vector $\mathbf{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ is a solution of this system, and so $\mathbf{0} \in W$.

If $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in W$ and $\mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in W$, then

$$a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n = 0$$

and

$$a_{i,1}y_1 + a_{i,2}y_2 + \cdots + a_{i,n}y_n = 0$$

for all $i = 1, \dots, m$. Adding these equations, we obtain

$$a_{i,1}(x_1 + y_1) + a_{i,2}(x_2 + y_2) + \cdots + a_{i,n}(x_n + y_n) = 0$$

for all $i = 1, \dots, m$, and so $\mathbf{x} + \mathbf{y} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix} \in W$. Thus, W is closed under vector addition.

Similarly, for all $c \in \mathbf{R}$ and $i = 1, \dots, m$, we have

$$\begin{aligned} &a_{i,1}(cx_1) + a_{i,2}(cx_2) + \cdots + a_{i,n}(cx_n) \\ &\qquad = c\,(a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n) \\ &\qquad = c \cdot 0 = 0 \end{aligned}$$

and so $c\mathbf{x} = \begin{pmatrix} cx_1 \\ \vdots \\ cx_n \end{pmatrix} \in W$. Thus, W is closed under scalar multiplication. This proves that W is a vector subspace.

Consider the inhomogeneous system

$$\begin{aligned} x + y + z &= 5 \\ 4x - 3y - 10z &= 6. \end{aligned} \tag{1.19}$$

Multiplying the first equation by 4, we obtain

$$\begin{aligned} 4x + 4y + 4z &= 20 \\ 4x - 3y - 10z &= 6. \end{aligned}$$

Subtracting the second equation from the first equation gives

$$7y + 14z = 14$$

or

$$y = 2 - 2z.$$

Substituting $y = 2 - 2z$ into $x + y + z = 5$ gives

$$x = 3 + z$$

and so every solution of (1.19) is of the form

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

Thus, the solution space of (1.19) is the affine subspace

$$L = \left\{ \begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix} + z \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} : z \in \mathbf{R} \right\}.$$

Theorem 1.5. *The set L of solutions of a consistent inhomogeneous system of linear equations is an affine subspace.*

Proof. Let L be the set of solutions a system of the consistent inhomogeneous system of linear equations (1.17), and let W be the set of solutions of the associated homogeneous system, that is, the system of equations (1.17) with $b_i = 0$ for all $i = 1, \ldots, m$.

Because the system (1.17) is consistent, there exists a solution $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in L$.

This means that

$$a_{i,1}v_1 + a_{i,2}v_2 + \cdots + a_{i,n}v_n = b_i \tag{1.20}$$

for all $i = 1, \ldots, m$. For all $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in W$, we have

$$a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n = 0. \tag{1.21}$$

Adding equations (1.20) and (1.21), we obtain

$$a_{i,1}(v_1 + x_1) + a_{i,2}(v_2 + x_2) + \cdots + a_{i,n}(v_n + x_n) = b_i + 0 = b_i$$

and so

$$\mathbf{v}+\mathbf{x} = \begin{pmatrix} v_1 + x_1 \\ \vdots \\ v_n + x_n \end{pmatrix} \in L.$$

Therefore,

$$\mathbf{v} + W \subseteq L. \tag{1.22}$$

If $\mathbf{v}' = \begin{pmatrix} v_1' \\ \vdots \\ v_n' \end{pmatrix} \in L$, then

$$a_{i,1}v_1' + a_{i,2}v_2' + \cdots + a_{i,n}v_n' = b_i \tag{1.23}$$

for all $i = 1, \ldots, m$. Subtracting equation (1.20) from equation (1.23), we obtain

$$a_{i,1}(v_1' - v_1) + a_{i,2}(v_2' - v_2) + \cdots + a_{i,n}(v_n' - v_n) = b_i - b_i = 0$$

and so $\mathbf{v}' - \mathbf{v} \in W$. Equivalently, $\mathbf{v}' \in \mathbf{v} + W$. Thus,

$$L \subseteq \mathbf{v} + W. \tag{1.24}$$

The relations (1.22) and (1.24) imply that $L = \mathbf{v} + W$, and so L is an affine subspace.

Exercises

Solve the following systems of linear equations.

1.

$$\begin{aligned} 3x + 2y &= 18 \\ 4x + 3y &= -5 \end{aligned}$$

2.

$$\begin{aligned} 7x + 2y &= 1 \\ 3x + y &= -5 \end{aligned}$$

3.

$$\begin{aligned} 2x - 4y &= 7 \\ -x - 3y &= 4 \end{aligned}$$

4.

$$\begin{aligned} x+y &= -2 \\ x+y &= 3 \end{aligned}$$

5.

$$\begin{aligned} 7x-8y &= 22 \\ -3x+2y &= -8 \end{aligned}$$

6.

$$\begin{aligned} 9x+5y &= -3 \\ 11x+6y &= 8 \end{aligned}$$

7.

$$\begin{aligned} 4x-y &= 13 \\ 2x+3y &= -11 \\ -x-7y &= 33 \end{aligned}$$

8.

$$\begin{aligned} x+y+z &= -7 \\ x-y+z &= 17 \end{aligned}$$

1.4 Gaussian elimination

Two systems of linear equations in n variables are *equivalent* if they have the same solutions. For example, the systems of linear equations

$$\begin{aligned} 7x-2y &= 10 \\ 3x+y &= 21 \end{aligned}$$

and

$$\begin{aligned} 4x+11y &= 115 \\ x+7y &= 67 \\ 8x-5y &= -13 \end{aligned}$$

are equivalent because (by Exercise 1) they have the unique solution: $\binom{x}{y} = \binom{4}{9}$.

There are three elementary operations that we can perform on a system of linear equations that produce new systems of linear equations with the property that the solutions of the new systems are exactly the same as the solutions of the original system of equations. These are the operations:

1. Interchange: We can interchange two equations in the system.
2. Multiplication: We can multiply an equation by a nonzero scalar.
3. Replacement: We can choose one equation in the system and add to it a nonzero scalar multiple of a different equation in the system.

Each of these operations has an elementary inverse operation of the same type.

1. Interchange: If we interchange two equations, then another interchange of the same two equations restores the original system of equations.
2. Multiplication: If we multiply an equation by a nonzero scalar c, then multiplying the new equation by c^{-1} restores the original equation.
3. Replacement: If we add c times equation i_2 to equation i_1, then adding $-c$ times equation i_2 to the new equation restores the original equation i_1.

Here are examples of the elementary operations. Starting with the system

$$\begin{aligned} 4x + 11y &= 115 \\ x + 7y &= 67 \\ 8x - 5y &= -13 \end{aligned}$$

we interchange equations 1 and 2, and obtain

$$\begin{aligned} x + 7y &= 67 \\ 4x + 11y &= 115 \\ 8x - 5y &= -13 \end{aligned}$$

Multiplication of the first equation of the new system by 3 gives

$$\begin{aligned} 3x + 21y &= 201 \\ 4x + 11y &= 115 \\ 8x - 5y &= -13 \end{aligned}$$

Addition of (-2) times the second equation to the third equation yields the system

$$\begin{aligned} 3x + 21y &= 201 \\ 4x + 11y &= 115 \\ -27y &= -243 \end{aligned}$$

Note that the last equation implies that $y = 9$ and so $x = 4$. Thus, $\mathbf{x} = \begin{pmatrix} 4 \\ 9 \end{pmatrix}$ is the unique solution of the system.

Gaussian elimination is a simple strategy to solve a system of linear equations by using the three elementary operations to "eliminate" variables. The description of the mechanics of Gaussian elimination is awkward, but the numerical examples that immediately follow the exposition should make the process clear.

Consider the system (1.17) of m equations in n variables. If the system is homogeneous and every equation in the system is the zero equation, then every n-tuple $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ is a solution of the system of equations. If the system is inhomogeneous and every equation in the system is the zero equation, then the system is inconsistent and has no solution.

Suppose that at least one equation is nonzero, and so $a_{i,j} \neq 0$ for some i and j. Let k_1 be the smallest integer such that $a_{i,k_1} \neq 0$ for some i. Equivalently, k_1 is the smallest integer such that the variable x_{k_1} occurs with a nonzero coefficient in some equation in the system. Interchange equations, if necessary, so that x_{k_1} appears with a nonzero coefficient in the first equation, and let c_1 be the coefficient of x_{k_1} in the first equation. Multiply this equation by c_1^{-1} so that the variable x_{k_1} now has coefficient 1 in the first equation. We can successively eliminate x_{k_1} from the other $m-1$ equations of the system by subtracting from each of these equations a suitable multiple of the first equation. Our new equivalent system of linear equations has the form

$$\begin{aligned} x_{k_1} + a'_{1,k_1+1}x_{k_1+1} + a'_{1,k_1+2}x_{k_1+2} + \cdots + a'_{1,n}x_n &= b'_1 \\ a'_{2,k_1+1}x_{k_1+1} + a'_{2,k_1+2}x_{k_1+2} + \cdots + a'_{2,n}x_n &= b'_2 \\ &\vdots \\ a'_{m,k_1+1}x_{k_1+1} + a'_{m,k_1+2}x_{k_1+2} + \cdots + a'_{m,n}x_n &= b'_m \end{aligned}$$

Suppose that $a'_{i,j} = 0$ for all $i \geq 2$ and $j \geq k_1 + 1$. If $b'_i \neq 0$ for some $i \geq 2$, then this system of equations is inconsistent. If $b'_i = 0$ for all $i = 2, \ldots, m$, then $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ is a solution of the system (and, by equivalence, a solution of the original system) if and only if

$$x_{k_1} = b'_1 - a'_{1,k_1+1}x_{k_1+1} - a'_{1,k_1+2}x_{k_1+2} - \cdots - a'_{1,n}x_n.$$

Suppose that $a'_{i,j} \neq 0$ for some $i \geq 2$ and $j \geq k_1 + 1$. Let $k_2 > k_1$ be the smallest integer such that $a_{i,k_2} \neq 0$ for some $i \geq 2$. If $i > 2$, then interchange equations i and 2. The variable x_{k_2} now appears with the nonzero coefficient c_2 in the second equation. Multiply this equation by c_2^{-1} so that the variable x_{k_2} has coefficient 1 in the second equation. We successively eliminate x_{k_2} from the other $m-1$ equations by subtracting from each of these equations a suitable multiple of the second equation. Our new equivalent system of equations has the form

$$\begin{array}{rcl} x_{k_1} + a''_{1,k_1+1}x_{k_1+1} + \cdots + a''_{1,k_2-1}x_{k_2-1} \quad & + & a''_{1,k_2+1}x_{k_2+1} + \cdots + a''_{1,n}x_n = b''_1 \\ x_{k_2} & + & a''_{2,k_2+1}x_{k_2+1} + \cdots + a''_{2,n}x_n = b''_2 \\ & & a''_{3,k_2+1}x_{k_2+1} + \cdots + a''_{3,n}x_n = b''_3 \\ & & \vdots \\ & & a''_{m,k_2+1}x_{k_2+1} + \cdots + a''_{m,n}x_n = b''_m \end{array}$$

Continuing inductively, we obtain a positive integer $r \leq m$ and a strictly increasing sequence of positive integers $k_1 < k_2 < \cdots < k_r \leq n$ such that the original system of m linear equations is equivalent to a system of r nonzero equations in which, for $i = 1, \ldots, r$, the ith equation has the form

$$x_{i,k_i} + \sum_{\ell=i}^{r-1} \sum_{j=k_\ell+1}^{k_{\ell+1}-1} \tilde{a}_{i,j} x_j + \sum_{j=k_r+1}^{n} \tilde{a}_{i,j} x_j = \tilde{b}_i \tag{1.25}$$

and the left sides of the remaining $m - r$ equations are 0. We can now assign any values to the variables $x_{i,j}$ for $i = 1, \ldots, r$ and $j \neq k_i$. Equation (1.25) determines the value of x_{i,k_i}.

The positive integers in the strictly increasing sequence $k_1 < k_2 < \cdots < k_r$ are called the *pivot numbers* of the system of equations.

Here are four examples of the use of these elementary operations to solve systems of linear equations.

Example 1. Solve the system of two equations with two variables:

$$\begin{cases} 9x + 11y = -1 \\ 5x + 6y = 3. \end{cases} \tag{1.26}$$

Multiply the first equation by 1/9:

$$\begin{aligned} x \ + \ \tfrac{11}{9}y &= -\tfrac{1}{9} \\ 5x + \ 6y &= \ \ 3 \end{aligned}$$

Add (-5) times the first equation to the second equation:

$$\begin{aligned} x + \ \tfrac{11}{9}y &= -\tfrac{1}{9} \\ -\tfrac{1}{9}y &= \ \tfrac{32}{9} \end{aligned}$$

Multiply the second equation by -9:

$$\begin{aligned} x + \tfrac{11}{9}y &= -\tfrac{1}{9} \\ y &= -32 \end{aligned}$$

Add (-11/9) times the second equation to the first equation:

$$\begin{aligned} x &= \ \ 39 \\ y &= -32. \end{aligned}$$

We check that the solution $\binom{x}{y} = \binom{39}{-32}$ is correct by substitution into the original system of linear equations:

$$\begin{aligned} 9x + 11y &= 9(39) + 11(-32) = 351 - 352 = -1 \\ 5x + 6y &= 5(39) + 6(-32) = 195 - 192 = 3. \end{aligned}$$

Thus, the system of equations (1.26) has a unique solution.

Example 2. Solve the system of two equations with three variables:

$$\begin{cases} 2x+3y+z=1 \\ 5x+y-4z=-1 \end{cases} \tag{1.27}$$

Multiply the first equation by 1/2:

$$\begin{aligned} x+\tfrac{3}{2}y+\tfrac{1}{2}z &= \tfrac{1}{2} \\ 5x+y-4z &= -1 \end{aligned}$$

Add (-5) times equation 1 to equation 2:

$$\begin{aligned} x+\tfrac{3}{2}y+\tfrac{1}{2}z &= \tfrac{1}{2} \\ -\tfrac{13}{2}y-\tfrac{13}{2}z &= -\tfrac{7}{2} \end{aligned}$$

Multiply equation 2 by -2/13:

$$\begin{aligned} x+\tfrac{3}{2}y+\tfrac{1}{2}z &= \tfrac{1}{2} \\ y+z &= \tfrac{7}{13} \end{aligned}$$

Add (-3/2) times equation 2 to equation 1:

$$\begin{aligned} x \quad -z &= -\tfrac{4}{13} \\ y+z &= \tfrac{7}{13} \end{aligned}$$

Solve these equations for x and y:

$$\begin{aligned} x &= -4/13+z \\ y &= 7/13-z \end{aligned}$$

We obtain

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -4/13+z \\ 7/13-z \\ z \end{pmatrix} = \begin{pmatrix} -4/13 \\ 7/13 \\ 0 \end{pmatrix} + z\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}.$$

To check that this solution of system (1.27) is correct, we substitute into the original system of linear equations:

$$\begin{aligned} 2x+3y+z &= 2\left(-\frac{4}{13}+z\right)+3\left(\frac{7}{13}-z\right)+z = -\frac{8}{13}+\frac{21}{13} = 1 \\ 5x+y-4z &= 5\left(-\frac{4}{13}+z\right)+\left(\frac{7}{13}-z\right)-4z = -\frac{20}{13}+\frac{7}{13} = -1. \end{aligned}$$

Thus, the system of equations (1.27) has infinitely many solutions, and the solutions are "parametrized" by the variable z.

Note that $\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$ is a solution of the homogeneous system

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

Example 3. Solve the system of two linear equations with four variables:

$$\begin{cases} x+y+z+w=10 \\ x-y+z-w=-2 \end{cases} \tag{1.28}$$

Add (-1) times the first equation to the second equation:

$$\begin{aligned} x+y+z+w &= 10 \\ -2y \quad -2w &= -12 \end{aligned}$$

Multiply the second equation by -1/2:

$$\begin{aligned} x+y+z+w &= 10 \\ y \qquad +w &= 6 \end{aligned}$$

Add (-1) times the second equation to the first equation:

$$\begin{aligned} x+ \qquad z \qquad &= 4 \\ y \quad +w &= 6 \end{aligned}$$

Solve these equations for x and y:

$$\begin{aligned} x &= 4-z \\ y &= 6-w. \end{aligned}$$

We obtain the solution

$$\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} 4-z \\ 6-w \\ z \\ w \end{pmatrix} = \begin{pmatrix} 4 \\ 6 \\ 0 \\ 0 \end{pmatrix} + z\begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + w\begin{pmatrix} 0 \\ -1 \\ 0 \\ 1 \end{pmatrix}.$$

We check that this solution is correct by substituting into the original system of linear equations:

$$\begin{aligned} x+y+z+w &= (4-z)+(6-w)+z+w = 10 \\ x-y+z-w &= (4-z)-(6-w)+z-w = -2. \end{aligned}$$

Thus, the system of equations (1.28) has infinitely many solutions, and the solutions are "parametrized" by the variables z and w.

Note that $\begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ -1 \\ 0 \\ 1 \end{pmatrix}$ are solutions of the homogeneous system

$$\begin{cases} x+y+z+w=0 \\ x-y+z-w=0. \end{cases}$$

Example 4. Solve the system of three linear equations with three variables:

$$\begin{cases} 3x + \ \ y - \ \ \ z = 6 \\ 4x - 2y - \ 5z = 1 \\ 6x - 8y - 13z = 4 \end{cases}$$

Multiply the first equation by 1/3:

$$\begin{aligned} x + \tfrac{1}{3}y - \tfrac{1}{3}z &= 2 \\ 4x - 2y - 5z &= 1 \\ 6x - 8y - 13z &= 4 \end{aligned}$$

Add (-4) times the first equation to the second equation:

$$\begin{aligned} x + \tfrac{1}{3}y - \tfrac{1}{3}z &= 2 \\ -\tfrac{10}{3}y - \tfrac{11}{3}z &= -7 \\ 6x - 8y - 13z &= 4 \end{aligned}$$

Add (-6) times the first equation to the third equation:

$$\begin{aligned} x + \tfrac{1}{3}y - \tfrac{1}{3}z &= 2 \\ -\tfrac{10}{3}y - \tfrac{11}{3}z &= -7 \\ -10y - 11z &= -8 \end{aligned}$$

Multiply the second equation by (-3/10):

$$\begin{aligned} x + \tfrac{1}{3}y - \tfrac{1}{3}z &= 2 \\ y + \tfrac{11}{10}z &= \tfrac{21}{10} \\ -10y - 11z &= -8 \end{aligned}$$

Add 10 times the second equation to the third equation:

$$x+\tfrac{1}{3}y-\tfrac{1}{3}z=2$$

$$y+\tfrac{11}{10}z=\tfrac{21}{10}$$

$$0=13$$

The third equation has no solution, so this system of equations is inconsistent.

Remark. Let (1.17) be an inconsistent system of linear equations. Every vector $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{R}^n$ determines numbers $\hat{b}_1, \hat{b}_2, \ldots, \hat{b}_m$ such that

$$\begin{array}{ccccccccc} a_{1,1}x_1 & + & \cdots & + & a_{1,j}x_j & + & \cdots & + & a_{1,n}x_n & = & \hat{b}_1 \\ a_{2,1}x_1 & + & \cdots & + & a_{2,j}x_j & + & \cdots & + & a_{2,n}x_n & = & \hat{b}_2 \\ \vdots & & & & & & & & & & \\ a_{i,1}x_1 & + & \cdots & + & a_{i,j}x_j & + & \cdots & + & a_{i,n}x_n & = & \hat{b}_i \\ \vdots & & & & & & & & & & \\ a_{m,1}x_1 & + & \cdots & + & a_{m,j}x_j & + & \cdots & + & a_{m,n}x_n & = & \hat{b}_m \end{array}$$

and

$$\begin{pmatrix} \hat{b}_1 \\ \vdots \\ \hat{b}_m \end{pmatrix} \neq \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

We define the "mean squared error" $\sum_{i=1}^m (b_i - \hat{b}_i)^2$.

An inconsistent system of linear equations with coefficients in the field of real numbers has no solution, but the system will always have a "best possible" approximate solution, that is, a solution that minimizes the mean-squared error. This is discussed in Chapter **??**, Section **??**.

Exercises

1. Prove the equivalence of the following systems of linear equations:

$$\begin{aligned} 7x - 2y &= 10 \\ 3x + y &= 21 \end{aligned}$$

and

$$\begin{aligned} 4x + 11y &= 115 \\ x + 7y &= 67 \\ 8x - 5y &= -13 \end{aligned}$$

2. Prove the equivalence of the following systems of equations:

$$\begin{aligned} x - y &= 0 \\ x + z &= 2 \end{aligned}$$

and

$$\begin{aligned} x + y + 2z &= 4 \\ 2x - y + z &= 2 \\ 7x - 2y - 5z &= -10 \end{aligned}$$

Use Gaussian elimination to solve the following systems of linear equations. Write the solution space as an affine subspace.

3.

$$\begin{aligned} 2x + y + z &= 0 \\ x + 2y + 3z &= 0. \end{aligned}$$

4.

$$\begin{aligned} 2x + y + z &= -1 \\ x + 2y - z &= 5 \end{aligned}$$

5.

$$\begin{aligned} 2x + y + z &= 9 \\ x + 2y - z &= 3 \end{aligned}$$

6.

$$\begin{aligned} 2x + y + z &= 4 \\ x + 2y - z &= -10 \end{aligned}$$

7.

$$\begin{aligned} 3x - y + z + 2w &= 12 \\ -2x + 3y + 7z - 10w &= -15 \end{aligned}$$

8.

$$\begin{aligned} x + 2y + 3z &= 0 \\ 4x + 5y + 6z &= 0 \\ 7x + 8y + 9z &= 0 \end{aligned}$$

9.

$$
\begin{aligned}
x+y+z&=0\\
x+2y+3z&=1\\
x+4y+9z&=2
\end{aligned}
$$

10.

$$
\begin{aligned}
3x-y&=1\\
5y+2z&=2\\
-2x+3y+z&=3
\end{aligned}
$$

11.

$$
\begin{aligned}
x+2y+3z&=7\\
3x-y-z&=3
\end{aligned}
$$

12.

$$
\begin{aligned}
x+2y&=3\\
4x+5y&=6\\
7x+8y&=9
\end{aligned}
$$

13.

$$
\begin{aligned}
x+4y+3z&=2\\
2x+y+z&=3\\
3x-2y-z&=4
\end{aligned}
$$

14.

$$
\begin{aligned}
x+4y+3z&=1\\
2x+y+z&=3\\
3x-2y-z&=4
\end{aligned}
$$

15.

$$
\begin{aligned}
8x+3y-2z&=3\\
x+5y+3z&=12\\
-7x+2y+11z&=39
\end{aligned}
$$

16.

$$
\begin{aligned}
x+2y+3z&=10\\
2x-3y+7z&=-9
\end{aligned}
$$

17.

$$\begin{aligned} -4x+6y-9z &= 20 \\ 2x+5y+11z &= -15 \end{aligned}$$

18.

$$\begin{aligned} x+5y-z+2w &= 17 \\ 3x+y+5z-4w &= -7 \end{aligned}$$

19.

$$\begin{aligned} 5x+15y+13z-6w &= 0 \\ 2x+6y+1z+6w &= 0 \\ x+3y+2z &= 0 \end{aligned}$$

20.

$$\begin{aligned} 2x+3y &= 10 \\ x+y-z &= 9 \\ 4x-5y-22z &= -27 \\ 7x+8y-5z &= 70 \end{aligned}$$

1.5 Linear systems with more variables than equations

A homogeneous system of linear equations always has the zero solution. In this section we use Gaussian elimination to prove one of the most important theorems in linear algebra: A homogeneous system of linear equations with more variables than equations always has a nonzero solution. Equivalently, the vector subspace of solutions is not the zero subspace.

We also prove that an inhomogeneous system with more variables than equations always has two solutions if it has at least one solution. Equivalently, the affine subspace of solutions contains more than one vector.

Theorem 1.6. *If $n > m$, then the homogeneous system of m linear equations in n variables*

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = 0 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = 0 \\ \quad \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n = 0 \end{cases} \tag{1.29}$$

has a nonzero solution.

Proof. The proof is by induction on the number m of equations in the system.

If $m = 1$, then $n \geq 2$ and the linear system consists of one equation with at least two variables:

$$a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = 0. \tag{1.30}$$

If $a_{1,1} = 0$, then $x_1 = 1$ and $x_j = 0$ for all $j \in \{2,3,\ldots,n\}$ is a nonzero solution of (1.30). If $a_{1,1} \neq 0$, then

$$x_1 = -\frac{1}{a_{1,1}} \sum_{j=2}^{n} a_{1,j}$$

and $x_j = 1$ for all $j \in \{2,3,\ldots,n\}$ is a nonzero solution of (1.30).

If $m = 2$, then $n \geq 3$ and the system (1.29) consists of two equations with at least three variables:

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3 + \cdots + a_{1,n}x_n &= 0 \\ a_{2,1}x_1 + a_{2,2}x_2 + a_{2,3}x_3 + \cdots + a_{2,n}x_n &= 0. \end{aligned} \tag{1.31}$$

If both $a_{1,1} = 0$ and $a_{2,1} = 0$, then $x_1 = 1$ and $x_j = 0$ for all $j \in \{2,3,\ldots,n\}$ is a nonzero solution of (1.31). Otherwise, at least one of the coefficients $a_{1,1}$ and $a_{2,1}$ is nonzero. If $a_{1,1} = 0$ and $a_{2,1} \neq 0$, then we interchange the equations. Thus, we can assume that $a_{1,1} \neq 0$. Adding $-a_{2,1}/a_{1,1}$ times the first equation to the second equation, we obtain an equivalent homogeneous system of two linear equations in n variables of the form

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3 + \cdots + a_{1,n}x_n &= 0 \\ a'_{2,2}x_2 + a'_{2,3}x_3 + \cdots + a'_{2,n}x_n &= 0. \end{aligned} \tag{1.32}$$

The second equation is a homogeneous equation in $n-1 \geq 2$ variables. Applying the case $m = 1$, we obtain a nonzero solution $\begin{pmatrix} x_2 \\ \vdots \\ x_n \end{pmatrix}$ of the second equation. Letting

$$x_1 = -\frac{1}{a_{1,1}} \sum_{j=2}^{n} a_{1,j}x_j$$

we obtain a nonzero solution $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ of the equivalent linear systems (1.32) and (1.31).

Let $n > m \geq 3$. We make the induction assumption that every homogeneous system of $m-1$ linear equations in $n-1$ variables has a nonzero solution. Consider the system (1.29) with m equations and $n > m$ variables. If the coefficient of the variable x_1 is 0 in every equation, that is, if $a_{i,1} = 0$ for all $i = 1,\ldots,m$, then $x_1 = 1$ and $x_j = 0$ for all $j = 2,\ldots,n$ is a nonzero solution of (1.29).

Suppose that $a_{i,1} \neq 0$ for some $i \in \{1,\ldots,m\}$. Interchanging equations 1 and i, we obtain an equivalent system of homogeneous equations in which the variable x_1 in the first equation has a nonzero coefficient. Subtracting a suitable multiple of the first equation from each of the other $m-1$ equations, we eliminate x_1 from each of the other $m-1$ equations, and produce an equivalent system of m equations in n

variables of the form

$$\begin{aligned} a'_{1,1}x_1 + a'_{1,2}x_2 + \cdots + a'_{1,n}x_n &= 0 \\ a'_{2,2}x_2 + \cdots + a'_{2,n}x_n &= 0 \\ &\vdots \\ a'_{m,2}x_2 + \cdots + a'_{m,n}x_n &= 0. \end{aligned} \tag{1.33}$$

Consider the following homogeneous system of $m-1$ equations in $n-1$ variables:

$$\begin{aligned} a'_{2,2}x_2 + \cdots + a'_{2,n}x_n &= 0 \\ &\vdots \\ a'_{m,2}x_2 + \cdots + a'_{m,n}x_n &= 0. \end{aligned}$$

The induction hypothesis implies that this system has a nonzero solution $\begin{pmatrix} x_2 \\ \vdots \\ x_n \end{pmatrix}$. Defining

$$x_1 = -\frac{1}{a'_{1,1}} \sum_{j=2}^{n} a'_{1,j} x_j,$$

we obtain a nonzero solution of (1.33) and so a nonzero solution $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ of (1.29). This completes the proof.

Theorem 1.7. *Let $n > m$. If the inhomogeneous system of m linear equations in n variables*

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ &\vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m \end{aligned} \tag{1.34}$$

has at least one solution, then it has at least two solutions.

Proof. Let $\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$ be a solution of the inhomogeneous system (1.34). By Theorem 1.6, the associated system (1.29) of homogeneous equations has a nonzero solution $\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$. It follows that $\begin{pmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{pmatrix}$ is also a solution of the inhomogeneous system (1.34), and $\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \neq \begin{pmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{pmatrix}$. This completes the proof.

Exercises

1. Find all solutions of each of the following homogeneous systems of linear equations.

   a.
$$2x_1 - 7x_2 = 0$$

   b.
$$\begin{aligned} x_1 + 3x_2 + 11x_3 &= 0 \\ x_1 + 5x_2 + 4x_3 &= 0 \end{aligned}$$

   c.
$$\begin{aligned} 2x_1 - 4x_2 + 6x_3 + 10x_4 &= 0 \\ 2x_1 - 3x_2 + 9x_3 + 21x_4 &= 0 \\ x_1 - x_2 + 8x_3 + 9x_4 &= 0 \end{aligned}$$

   d.
$$\begin{aligned} 2x_1 - 4x_2 + 6x_3 + 10x_4 + 2x_5 &= 0 \\ 2x_1 - 3x_2 + 9x_3 + 21x_4 - 12x_5 &= 0 \\ x_1 - x_2 + 8x_3 + 9x_4 + 7x_5 &= 0 \end{aligned}$$

2. Prove directly that a homogeneous system of 2 linear equations in 3 variables has a nonzero solution.
3. Prove that if an inhomogeneous system of 2 linear equations in 3 variables has one solution, then it has at least two solutions.
4. Let $n > m$. Prove that a homogeneous system of m linear equations in n variables has infinitely many solutions.

1.6 Vector spaces and linear independence

.

A *vector space* over the field $\mathbf{R}$ is a set V (whose elements are called *vectors*) in which it is possible to add vectors and to multiply a vector by a scalar. The operation of *vector addition* satisfies the following properties:

(A1) Vector addition is *associative*: For all vectors $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, we have

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

(A2) There exist a vector $\mathbf{0} \in V$ such that

$$\mathbf{0} + \mathbf{v} = \mathbf{v} + \mathbf{0} = \mathbf{v}$$

for all $\mathbf{v}$. The element $\mathbf{0}$ is called the *zero vector* or *additive identity* in V. If $\mathbf{0}^* \in V$ also satisfies $\mathbf{0}^* + \mathbf{v} = \mathbf{v} + \mathbf{0}^* = \mathbf{v}$ for all $\mathbf{v}$, then

$$\mathbf{0}^* = \mathbf{0}^* + \mathbf{0} = \mathbf{0}$$

and so the zero vector is unique.

(A3) For every element $\mathbf{v}$ there is a element $\mathbf{w}$ such that

$$\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v} = \mathbf{0}.$$

The element $\mathbf{w}$ is called an *additive inverse* of $\mathbf{v}$. If $\mathbf{w}^*$ is also an additive inverse of $\mathbf{v}$, then $\mathbf{v} + \mathbf{w}^* = \mathbf{0}$ and

$$\mathbf{w}^* = \mathbf{0} + \mathbf{w}^* = (\mathbf{w} + \mathbf{v}) + \mathbf{w}^* = \mathbf{w} + (\mathbf{v} + \mathbf{w}^*) = \mathbf{w} + \mathbf{0} = \mathbf{w}.$$

Thus, every element $\mathbf{v}$ has a unique additive inverse, denoted $-\mathbf{v}$. We define *subtraction* as follows: For all $\mathbf{v}, \mathbf{w}$,

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

(A4) Vector addition is *commutative*: For all $\mathbf{v}, \mathbf{w}$, we have

$$\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}.$$

The operation of *scalar multiplication* satisfies the following properties.

(SM1) Scalar multiplication is *associative*: For all vectors $\mathbf{v} \in V$ and for all scalars $a, b \in \mathbf{R}$, we have

$$(ab)\mathbf{v} = a(b\mathbf{v}).$$

(SM2) Scalar multiplication is *distributive*: For all vectors $\mathbf{v}, \mathbf{w} \in V$ and for all scalars $a, b \in \mathbf{R}$, we have

$$(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$$

and

$$a(\mathbf{v} + \mathbf{w}) = a\mathbf{v} + a\mathbf{w}.$$

(SM3) For all vectors $\mathbf{v} \in V$ we have

$$1\mathbf{v} = \mathbf{v}.$$

Lemma 1.4. *Let V be a vector space. For all $\mathbf{v} \in V$,*

$$0\mathbf{v} = \mathbf{0}.$$

Proof. Let $\mathbf{v} \in V$. The scalar 0 satisfies

$$0 = 0 + 0.$$

By distributivity of scalar multiplication,

$$0\mathbf{v} = (0+0)\mathbf{v} = 0\mathbf{v} + 0\mathbf{v}.$$

Subtracting the vector $0\mathbf{v}$, we obtain

$$\mathbf{0} = 0\mathbf{v} - 0\mathbf{v} = (0\mathbf{v} + 0\mathbf{v}) - 0\mathbf{v} = 0\mathbf{v} + (0\mathbf{v} - 0\mathbf{v}) = 0\mathbf{v} + \mathbf{0} = 0\mathbf{v}.$$

This completes the proof.

The most important vector space is $\mathbf{R}^n$ with vector addition defined by (1.8) and scalar multiplication defined by (1.10).

Let $\mathbf{v}_1, \ldots, \mathbf{v}_k$ be a finite sequence of vectors in $\mathbf{R}^n$. By Section 1.1, Exercise 15,

$$0\mathbf{v}_i = \mathbf{0}$$

for all $i \in \{1, \ldots, k\}$, and so

$$0\mathbf{v}_1 + 0\mathbf{v}_2 + \cdots + 0\mathbf{v}_k = \mathbf{0}.$$

The finite sequence of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ is *linearly dependent* if there exist scalars $x_1, \ldots, x_k$ such that

$$x_j \neq 0 \text{ for some } j \in \{1, 2, \ldots, k\}.$$

and

$$x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \cdots + x_k\mathbf{v}_k = \mathbf{0}.$$

The sequence of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k$ is *linearly independent* if it is not linearly dependent.

For example, in $\mathbf{R}^2$, the vectors $\mathbf{v}_1 = \begin{pmatrix} 6 \\ -14 \end{pmatrix}$ and $\mathbf{v}_2 = \begin{pmatrix} -15 \\ 35 \end{pmatrix}$ are linearly dependent because

$$5\mathbf{v}_1 + 2\mathbf{v}_2 = 5\begin{pmatrix} 6 \\ -14 \end{pmatrix} + 2\begin{pmatrix} -15 \\ 35 \end{pmatrix} = \begin{pmatrix} 30 \\ -70 \end{pmatrix} + \begin{pmatrix} -30 \\ 70 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \mathbf{0}.$$

The vectors $\mathbf{v}_1 = \mathbf{0}$ and $\mathbf{v}_2 = \begin{pmatrix} 6 \\ -14 \end{pmatrix}$ are linearly dependent in $\mathbf{R}^2$ because

$$1\mathbf{v}_1 + 0\,\mathbf{v}_2 = 1\begin{pmatrix} 0 \\ 0 \end{pmatrix} + 0\begin{pmatrix} 6 \\ -14 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \mathbf{0}.$$

The vectors $\mathbf{v}_1 = \begin{pmatrix} 2 \\ 5 \\ -1 \end{pmatrix}$, $\mathbf{v}_2 = \begin{pmatrix} -7 \\ 2 \\ -1 \end{pmatrix}$, and $\mathbf{v}_3 = \begin{pmatrix} 1 \\ -4 \\ 1 \end{pmatrix}$ in $\mathbf{R}^3$ are linearly dependent because

$$4\mathbf{v}_1 + 2\mathbf{v}_2 + 6\mathbf{v}_3 = 4\begin{pmatrix} 2 \\ 5 \\ -1 \end{pmatrix} + 2\begin{pmatrix} -7 \\ 2 \\ -1 \end{pmatrix} + 6\begin{pmatrix} 1 \\ -4 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \mathbf{0}.$$

In the vector space $\mathbf{R}^3$, consider the vectors

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \qquad \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \qquad \mathbf{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

If x_1, x_2, x_3 are scalars such that

$$x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + x_3\mathbf{e}_3 = \mathbf{0}$$

then

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = x_1\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + x_2\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + x_3\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

and so $x_1 = x_2 = x_3 = 0$. This proves that the sequence of vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ is linearly dependent.

Define the *Kronecker delta*

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

In the vector space $\mathbf{R}^n$, consider the sequence of vectors $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ defined by

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ldots, \mathbf{e}_j = \begin{pmatrix} \delta_{1,j} \\ \delta_{2,j} \\ \vdots \\ \delta_{n-1,j} \\ \delta_{n,j} \end{pmatrix}, \ldots, \mathbf{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \tag{1.35}$$

We have

$$\sum_{j=0}^{n} x_j \delta_{i,j} = x_i$$

for all $i = 1, \ldots, n$, and so

$$\sum_{j=0}^{n} x_j \mathbf{e}_j = \sum_{j=0}^{n} x_j \begin{pmatrix} \delta_{1,j} \\ \delta_{2,j} \\ \vdots \\ \delta_{n-1,j} \\ \delta_{n,j} \end{pmatrix} = \sum_{j=0}^{n} \begin{pmatrix} x_j\delta_{1,j} \\ x_j\delta_{2,j} \\ \vdots \\ x_j\delta_{n-1,j} \\ x_j\delta_{n,j} \end{pmatrix} = \begin{pmatrix} \sum_{j=0}^{n} x_j\delta_{1,j} \\ \sum_{j=0}^{n} x_j\delta_{2,j} \\ \vdots \\ \sum_{j=0}^{n} x_j\delta_{n-1,j} \\ \sum_{j=0}^{n} x_j\delta_{n,j} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Therefore, $\sum_{j=0}^{n} x_j \mathbf{e}_j = \mathbf{0}$ if and only if $x_j = 0$ for all $j = 1,\ldots,n$. Thus, the sequence of vectors $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ is linearly independent.

The following theorem shows that the representation of a vector as a linear combination of linearly independent vectors is unique.

Theorem 1.8. *Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ be a sequence of linearly independent vectors. If $x_1, x_2 \ldots, x_k, y_1, y_2, \ldots, y_k$ are scalars such that*

$$\sum_{i=1}^{k} x_i \mathbf{v}_i = \sum_{i=1}^{k} y_i \mathbf{v}_i$$

then

$$x_i = y_i \qquad \textit{for all } i \in \{1,2,\ldots,k\}.$$

Proof. If $\sum_{i=1}^{k} x_i \mathbf{v}_i = \sum_{i=1}^{k} y_i \mathbf{v}_i$, then

$$\sum_{i=1}^{k} (x_i - y_i)\mathbf{v}_i = \sum_{i=1}^{k} x_i \mathbf{v}_i - \sum_{i=1}^{k} y_i \mathbf{v}_i = \mathbf{0}.$$

Linear independence of the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ implies that $x_i - y_i = 0$, and, equivalently, $x_i = y_i$, for all $i \in \{1,2,\ldots,k\}$. This completes the proof.

Lemma 1.5. *Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ be a sequence of k linearly independent vectors.*

1. *Let σ be a permutation of $\{1,2,\ldots,k\}$. The sequence of vectors $\mathbf{v}_{\sigma(1)}$, $\mathbf{v}_{\sigma(2)}$, $\ldots$, $\mathbf{v}_{\sigma(k)}$ is linearly independent*
2. *The sequence of vectors $c_1\mathbf{v}_1, c_2\mathbf{v}_2, \ldots, c_k\mathbf{v}_k$ is linearly independent for every sequence $c_1, c_2, \ldots, c_k$ of nonzero scalars.*
3. *The sequence of vectors $\mathbf{v}_1 + \mathbf{v}_2, \mathbf{v}_2, \ldots, \mathbf{v}_k$ is linearly independent.*

Proof. For all scalars $x_1, \ldots, x_k$, we have

$$\mathbf{0} = \sum_{j=1}^{k} x_j \mathbf{v}_{\sigma(j)} = \sum_{j=1}^{k} x_{\sigma^{-1}(j)} \mathbf{v}_j$$

if and only if $x_{\sigma^{-1}(j)} = 0$ for all j if and only if $x_j = 0$ for all j. Thus, every permutation of a sequence of linearly independent vectors is linearly independent. This proves (1).

Similarly,

$$\mathbf{0} = \sum_{j=1}^{k} x_j (c_j \mathbf{v}_j) = \sum_{j=1}^{k} (x_j c_j) \mathbf{v}_j$$

if and only if $x_j c_j = 0$ for all j if and only if $x_j = 0$ for all j. This proves (2).

Finally,

$$\mathbf{0} = x_1(\mathbf{v}_1 + \mathbf{v}_2) + \sum_{j=2}^{k} x_j \mathbf{v}_j = x_1\mathbf{v}_1 + (x_1 + x_2)\mathbf{v}_2 + \sum_{j=3}^{k} x_j \mathbf{v}_j$$

It follows that $x_j = 0$ for $j = 3, \ldots, k$, and that $x_1 = x_1 + x_2 = 0$, hence $x_2 = 0$. This proves (3).

Theorem 1.9. *Let m and n be positive integers with $m < n$. Every sequence $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of n vectors in $\mathbf{R}^m$ is linearly dependent.*

Proof. For $j = 1, \ldots, n$, let $\mathbf{v}_j = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{m,j} \end{pmatrix} \in \mathbf{R}^m$. The vector equation

$$x_1 \mathbf{v}_1 + \cdots + x_n \mathbf{v}_n = \mathbf{0}$$

is equivalent to the equation

$$\begin{pmatrix} a_{1,1}x_1 + \cdots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n \end{pmatrix} = x_1 \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{m,1} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{m,n} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

and so the sequence of n vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ in $\mathbf{R}^m$ is linearly dependent if and only if the system of m homogeneous equations in n variables

$$\begin{aligned} a_{1,1}x_1 + \cdots + a_{1,n}x_n &= 0 \\ &\vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n &= 0 \end{aligned}$$

has a nonzero solution. By Theorem 1.6, if $n > m$, then this system does have a nonzero solution. This completes the proof.

A *subspace* of a vector space V is a nonempty subset of V that is closed under vector addition and scalar multiplication. The *zero subspace* of $\mathbf{R}^n$ is the subspace $\{\mathbf{0}\}$ consisting only of the zero vector. The vector space $\mathbf{R}^n$ is also a subspace of $\mathbf{R}^n$.

Theorem 1.10. *Let V be a vector space and let W_1 and W_2 be subspaces of V. The intersection*

$$W_1 \cap W_2 = \{\mathbf{w} : \mathbf{w} \in W_1 \text{ and } \mathbf{w} \in W_2\}$$

and the sumset

$$W_1 + W_2 = \{\mathbf{w}_1 + \mathbf{w}_2 : \mathbf{w}_1 \in W_1 \text{ and } \mathbf{w}_2 \in W_2\}$$

are subspaces of V.

Proof. Because W_1 and W_2 are subspaces, we have $\mathbf{0} \in W_1$ and $\mathbf{0} \in W_2$, and so $\mathbf{0} \in W_1 \cap W_2$ and $\mathbf{0} = \mathbf{0} + \mathbf{0} \in W_1 + W_2$. If $\mathbf{w}_1, \mathbf{w}_2 \in W_1 \cap W_2$, then $\mathbf{w}_1, \mathbf{w}_2 \in W_1$ and $\mathbf{w}_1 + \mathbf{w}_2 \in W_1$. Similarly, $\mathbf{w}_1, \mathbf{w}_2 \in W_2$ and $\mathbf{w}_1 + \mathbf{w}_2 \in W_2$. Therefore, $\mathbf{w}_1 + \mathbf{w}_2 \in W_1 \cap W_2$. If $c \in \mathbf{R}$ and $\mathbf{w} \in W_1 \cap W_2$, then $\mathbf{w} \in W_1$ and $c\mathbf{w} \in W_1$. Also, $\mathbf{w} \in W_2$ and $c\mathbf{w} \in W_2$, hence $c\mathbf{w} \in W_1 \cap W_2$. This proves that $W_1 \cap W_2$ is a subspace.

Let $\mathbf{w}, \mathbf{w}' \in W_1 + W_2$. There exist vectors $\mathbf{w}_1, \mathbf{w}_1' \in W_1$ and $\mathbf{w}_2, \mathbf{w}_2' \in W_2$ such that $\mathbf{w} = \mathbf{w}_1 + \mathbf{w}_2$ and $\mathbf{w}' = \mathbf{w}_1' + \mathbf{w}_2'$. It follows that

$$\mathbf{w} + \mathbf{w}' = (\mathbf{w}_1 + \mathbf{w}_2) + (\mathbf{w}_1' + \mathbf{w}_2') = (\mathbf{w}_1 + \mathbf{w}_1') + (\mathbf{w}_2 + \mathbf{w}_2') \in W_1 + W_2$$

and

$$c\mathbf{w} = c(\mathbf{w}_1 + \mathbf{w}_2) = c\mathbf{w}_1 + c\mathbf{w}_2 \in W_1 + W_2.$$

This completes the proof.

Theorem 1.11. *Let S be a nonempty set of vectors. The set W of all linear combinations of vectors in S is a subspace.*

We say that a nonempty subset S of vectors *generates* a subspace W, and that W *is generated by* S, if W is the set of all linear combinations of vectors in S. We often denote the subspace generated by S as $\langle S \rangle$.

Proof. We first consider the case that S is a finite set. Let $S = \{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$, and let W be the set of all linear combinations of vectors in S . Because S is nonempty, we have $k \geq 1$, and $0\mathbf{w}_1 = \mathbf{0} \in W$. Let $c_1, \ldots, c_k, c_1', \ldots, c_k'$, and c be scalars. If

$$\mathbf{w} = \sum_{i=1}^{k} c_i \mathbf{w}_i \in W \qquad \text{and} \qquad \mathbf{w}' = \sum_{i=1}^{k} c_i' \mathbf{w}_i \in W,$$

then

$$\mathbf{w} + \mathbf{w}' = \sum_{i=1}^{k} c_i \mathbf{w}_i + \sum_{i=1}^{k} c_i' \mathbf{w}_i = \sum_{i=1}^{k} (c_i + c_i') \mathbf{w}_i \in W$$

and

$$c\mathbf{w} = c \sum_{i=1}^{k} c_i \mathbf{w}_i = \sum_{i=1}^{k} c c_i \mathbf{w}_i \in W.$$

Thus, W is closed under vector addition and scalar multiplication, and so W is a vector subspace.

Suppose that the set S is infinite. If $\mathbf{w}$ and $\mathbf{w}'$ are linear combinations of elements of S, then there is a finite subset S' of S such that both $\mathbf{w}$ and $\mathbf{w}'$ are linear combinations of vectors in S'. It follows that $\mathbf{w} + \mathbf{w}'$ and $c\mathbf{w}$ are linear combinations of vectors in S', and so $\mathbf{w} + \mathbf{w}'$ is a linear combination of of vectors in S. This completes the proof.

Theorem 1.12. *Let $V = \mathbf{R}^n$. Let S be a nonempty subset of V, and let $\langle S \rangle$ be the subspace of V generated by S. Let $\mathscr{W} = \{W_i : i \in I\}$ be the set of subspaces of V that contain S. Note that $\mathscr{W} \neq \emptyset$ because $V \in \mathscr{W}$. Then*

$$\langle S \rangle = \bigcap_{i \in I} W_i.$$

Proof. The subspace $\langle S \rangle$ is a subspace of V that contains S, and so $\langle S \rangle \in \mathscr{W}$. It follows that $\bigcap_{i \in I} W_i \subseteq \langle S \rangle$.

Let $i \in I$. Because W_i is a subspace that contains S, it follows that W_i contains every linear combination of elements of S, and so $\langle S \rangle \subseteq W_i$. Therefore, $\langle S \rangle \subseteq \bigcap_{i \in I} W_i$. This completes the proof.

Theorem 1.13. *Let W be the vector subspace consisting of all linear combinations of vectors in $S = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$, and let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be vectors in W. If $n > m$, then the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly dependent.*

Proof. For all $j \in \{1, \ldots, n\}$, there exist scalars $a_{i,j}$ such that

$$\mathbf{v}_j = \sum_{i=1}^{m} a_{i,j} \mathbf{w}_i.$$

For scalars $x_1, \ldots, x_n$, we have

$$\begin{aligned} \sum_{j=1}^{n} x_j \mathbf{v}_j &= \sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{i,j} \mathbf{w}_i \\ &= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{i,j} x_j \right) \mathbf{w}_i. \end{aligned}$$

By Theorem 1.6, the homogeneous system (1.29) of m linear equations in n variables has a nonzero solution, and so there exists $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{R}^n$ such that $\sum_{j=1}^{n} x_j \mathbf{v}_j = \mathbf{0}$. This proves the linear dependence of the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$.

Corollary 1.1. *Let W be the vector subspace consisting of all linear combinations of vectors in $S = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$. If $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent vectors in W, then $n \leq m$.*

Exercises

1. Determine if the following sequences of vectors $\mathbf{v}_1, \mathbf{v}_2$ are linearly dependent or linearly independent.

   a.
   $$\mathbf{v}_1 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \qquad \mathbf{v}_2 = \begin{pmatrix} 3 \\ 0 \end{pmatrix}.$$

   b.
   $$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \qquad \mathbf{v}_2 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

   c.
   $$\mathbf{v}_1 = \begin{pmatrix} -4 \\ 7 \end{pmatrix} \qquad \mathbf{v}_2 = \begin{pmatrix} -4 \\ 7 \end{pmatrix}.$$

2. Determine if the following sequences of vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are linearly dependent or linearly independent.

   a.
$$\mathbf{v}_1 = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 0 \\ 5 \\ 0 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} 0 \\ 0 \\ 10 \end{pmatrix}.$$

   b.
$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}.$$

   c.
$$\mathbf{v}_1 = \begin{pmatrix} 5 \\ -2 \\ 1 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 1 \\ -2 \\ 5 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} 1 \\ 1 \\ -4 \end{pmatrix}.$$

3. Consider the vectors
$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad \mathbf{v}_2 = \begin{pmatrix} 3 \\ 5 \end{pmatrix}, \qquad \mathbf{v}_3 = \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$
   in $\mathbf{R}^2$. Compute scalars x_1, x_2, x_3 not all 0 such that
$$x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + x_3\mathbf{v}_3 = \mathbf{0}.$$

4. Consider the vectors
$$\mathbf{v}_1 = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix}, \qquad \mathbf{v}_2 = \begin{pmatrix} -4 \\ -3 \\ -1 \end{pmatrix}, \qquad \mathbf{v}_3 = \begin{pmatrix} 6 \\ 9 \\ 8 \end{pmatrix}, \qquad \mathbf{v}_4 = \begin{pmatrix} 10 \\ 21 \\ 9 \end{pmatrix}$$
   in $\mathbf{R}^3$. Compute scalars x_1, x_2, x_3, x_4 not all 0 such that
$$x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + x_3\mathbf{v}_3 + x_4\mathbf{v}_4 = \mathbf{0}.$$

5. Find two distinct representations of the vector $\begin{pmatrix} 7 \\ -3 \\ 2 \end{pmatrix}$ as a linear combination of the vectors $\begin{pmatrix} 5 \\ -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -4 \end{pmatrix}$.
6. Prove that the set of vectors $\{\mathbf{v}_1, \mathbf{v}_2\}$ is linearly independent if and only if the set of vectors $\{\mathbf{v}_1 + \mathbf{v}_2, \mathbf{v}_1 - \mathbf{v}_2\}$ is linearly independent
7. Prove that the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ in $\mathbf{R}^n$ are linearly dependent if $\mathbf{v}_i = \mathbf{0}$ for some $i \in \{1, \ldots, k\}$.
8. Prove that the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ in $\mathbf{R}^n$ are linearly dependent if $\mathbf{v}_i = c\mathbf{v}_j$ for some $i \neq j$ and $c \in \mathbf{R}$.

9. Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ be linearly dependent vectors in $\mathbf{R}^n$. Prove that the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k, \mathbf{w}$ are linearly dependent for all $\mathbf{w} \in \mathbf{R}^n$.
10. Let $\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2$ be three vectors in $\mathbf{R}^n$ such that the two vectors $\mathbf{v}_1 - \mathbf{v}_0$ and $\mathbf{v}_2 - \mathbf{v}_0$ are linearly independent. Prove that the two vectors $\mathbf{v}_0 - \mathbf{v}_1$ and $\mathbf{v}_2 - \mathbf{v}_1$ are linearly independent.
11. Let $\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ be $n+1$ vectors in $\mathbf{R}^n$ such that the n vectors

$$\mathbf{v}_1 - \mathbf{v}_0, \mathbf{v}_2 - \mathbf{v}_0, \ldots, \mathbf{v}_n - \mathbf{v}_0$$

are linearly independent. Let $r \in \{1, 2, \ldots, n\}$. Prove that the n vectors

$$\mathbf{v}_0 - \mathbf{v}_r, \mathbf{v}_1 - \mathbf{v}_r, \ldots, \mathbf{v}_{r-1} - \mathbf{v}_r, \mathbf{v}_{r+1} - \mathbf{v}_r, \ldots, \mathbf{v}_n - \mathbf{v}_r$$

are linearly independent.
12. Let

$$\mathbf{w}_1 = \begin{pmatrix} 2 \\ -1 \end{pmatrix} \qquad \text{and} \qquad \mathbf{w}_2 = \begin{pmatrix} -3 \\ 2 \end{pmatrix}.$$

Let

$$\mathbf{v}_1 = 2\mathbf{w}_1 + 5\mathbf{w}_2, \qquad \mathbf{v}_2 = 3\mathbf{w}_1 - \mathbf{w}_2, \qquad \mathbf{v}_3 = \mathbf{w}_1 + 7\mathbf{w}_2.$$

Compute scalars x_1, x_2, x_3 such that

$$x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + x_3\mathbf{v}_3 = \mathbf{0}.$$

13. Let $V = \mathbf{R}^n$. Let W_1 and W_2 be subspaces of V. Prove that $W_1 \cap W_2$ is a subspace of V.
14. Let W_1 be the subspace of $\mathbf{R}^2$ generated by the vector $\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and let W_2 be the subspace of $\mathbf{R}^2$ generated by the vector $\mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

   a. Compute $W_1 \cap W_2$.
   b. Prove that $W_1 \cup W_2$ is not a subspace of $\mathbf{R}^2$.

15. Let $V = \mathbf{R}^n$. Let $\{W_i : i \in I\}$ be a finite or infinite family of subspaces of V. Prove that $\bigcap_{i \in I} W_i$ is a subspace of V.

1.7 Bases and dimension of vector subspaces

A vector subspace W is *generated* by a nonempty set S of vectors if W is the set of all linear combinations of vectors in S. If $S = \{\mathbf{0}\}$, then $W = \{\mathbf{0}\}$. The vector subspace W is *finitely generated* if W is the set of linear combinations of a nonempty finite set of vectors.

Theorem 1.14. *Let S be a nonempty finite set of vectors in $\mathbf{R}^n$, and let W be the subspace of $\mathbf{R}^n$ generated by S. There exists a linearly independent subset of S that generates W.*

Proof. Let $S = \{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ be a nonempty finite set of nonzero vectors in $\mathbf{R}^n$, such that W is the set of all linear combinations of the vectors in S. Moreover, $S \neq \{\mathbf{0}\}$ because $W \neq \{\mathbf{0}\}$.

If the set S is linearly dependent, then there exist scalars $a_1, \ldots, a_k$ such that

$$\sum_{i=1}^{k} a_i \mathbf{w}_i = \mathbf{0}$$

and $a_{i_1} \neq 0$ for some $i_1 \in \{1, \ldots, k\}$. Solving this equation for $\mathbf{w}_{i_1}$, we obtain

$$\mathbf{w}_{i_1} = -\frac{1}{a_{i_1}} \sum_{\substack{i=1 \\ i \neq i_1}}^{k} a_i \mathbf{w}_i. \tag{1.36}$$

Every vector $\mathbf{w} \in W$ is a linear combination of vectors in S, and so there exist scalars $c_1, \ldots, c_k$ such that

$$\mathbf{w} = \sum_{i=1}^{k} c_i \mathbf{w}_i = \sum_{\substack{i=1 \\ i \neq i_1}}^{k} c_i \mathbf{w}_i + c_{i_1} \mathbf{w}_{i_1}. \tag{1.37}$$

Inserting (1.36) into (1.37), we obtain

$$\mathbf{w} = \sum_{\substack{i=1 \\ i \neq i_1}}^{k} c_i \mathbf{w}_i - \frac{c_{i_1}}{a_{i_1}} \sum_{\substack{i=1 \\ i \neq i_1}} a_i \mathbf{w}_i = \sum_{\substack{i=1 \\ i \neq i_1}}^{k} \left(c_i - \frac{c_{i_1} a_i}{a_{i_1}} \right) \mathbf{w}_i$$

and so W is the set of linear combinations of vectors in the set $S_1 = S \setminus \{w_{i_1}\}$.

If the set $S_1 = S \setminus \{w_{i_1}\}$ is linearly dependent, then there exists $i_2 \in \{1, \ldots, k\} \setminus \{i_1\}$ such that W is the set of linear combinations of vectors in the set $S_2 = S \setminus \{\mathbf{w}_{i_1}, \mathbf{w}_{i_2}\}$.

If the set $S_2 = S \setminus \{\mathbf{w}_{i_1}, \mathbf{w}_{i_2}\}$ is linearly dependent, then we repeat the process. Because the set S is finite and the subspace W is nonzero, we continue inductively until we obtain a set of vectors $\{\mathbf{w}_{i_1}, \ldots, \mathbf{w}_{i_r}\}$ such that W is the set of linear combinations of vectors in the set $S_r = S \setminus \{\mathbf{w}_{i_1}, \ldots, \mathbf{w}_{i_r}\}$, and the set S_r is linearly independent. Because $W \neq \{\mathbf{0}\}$, we must have $r \leq k - 1$. This completes the proof.

A set S of vectors is a *basis* for a subspace W if the set S generates W and S is linearly independent.

Corollary 1.2. *Every finitely generated subspace of $\mathbf{R}^n$ has a basis. Moreover, every finite generating set for a subspace contains a basis.*

The *cardinality* of a set is the number of elements in the set. We denote the cardinality of the set S by $|S|$.

Theorem 1.15. *Let W be a finitely generated vector subspace. If $\mathscr{B}_1$ and $\mathscr{B}_2$ are bases for W, then $|\mathscr{B}_1| = |\mathscr{B}_2|$.*

Proof. Let $m_1 = |\mathscr{B}_1|$ and $m_2 = |\mathscr{B}_2|$. The basis $\mathscr{B}_1$ generates W, and so every vector in W, and, in particular, every vector in $\mathscr{B}_2$, is a linear combination of vectors in $\mathscr{B}_1$. Because the basis $\mathscr{B}_2$ is linearly independent, it follows from Corollary 1.1 that $m_2 \le m_1$.

Similarly, the basis $\mathscr{B}_2$ generates W, and so every vector in W, and, in particular, every vector in $\mathscr{B}_1$, is a linear combination of vectors in $\mathscr{B}_2$. Because the basis $\mathscr{B}_1$ is linearly independent, Corollary 1.1 implies that $m_1 \le m_2$. Therefore, $|\mathscr{B}_1| = m_1 = m_2 = |\mathscr{B}_2|$. This completes the proof.

Theorem 1.15 is a fundamental result in linear algebra. It states that if W is a nonzero finitely generated vector subspace, then there exists a positive integer d such that every basis for W has cardinality d. The integer d is called the *dimension* of the subspace. We write $\dim(W) = d$.

We define the dimension of the zero subspace by $\dim(\{\mathbf{0}\}) = 0$.

For example, the set of vectors

$$\mathscr{E}_n = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$$

defined by (1.35) generates $\mathbf{R}^n$ and is linearly independent. Therefore, $\dim(\mathbf{R}^n) = n$. The *standard basis* of $\mathbf{R}^n$ is $\mathscr{E}_n = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$.

Theorem 1.16. *Let W_1 and W_2 be subspaces of $\mathbf{R}^n$ with $W_1 \subseteq W_2$. Let B be a basis for W_1. If $\mathbf{v} \in W_2 \setminus W_1$, then the set $B \cup \{\mathbf{v}\}$ is linearly independent.*

Proof. Let $B = \{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ and let $\mathbf{v} \in W_2 \setminus W_1$. Let $x, x_1, \ldots, x_k$ be scalars such that

$$x\mathbf{v} + \sum_{i=1}^{k} x_i \mathbf{w}_i = \mathbf{0}.$$

We must prove that $x = x_1 = x_2 = \cdots = x_k = 0$.

If $x \ne 0$, then

$$\mathbf{v} = -\frac{1}{x}\sum_{i=1}^{k} x_i \mathbf{w}_i = \sum_{i=1}^{k} \left(-\frac{x_i.}{x}\right) \mathbf{w}_i$$

is a linear combination of vectors in B, and so $\mathbf{v} \in W_1$, which is absurd. Therefore, $x = 0$. It follows that

$$\sum_{i=1}^{k} x_i \mathbf{w}_i = \mathbf{0}$$

and so $x_i = 0$ for $i = 1, \ldots, k$ by the linear independence of B. This completes the proof.

Lemma 1.6. *Every nonzero subspace W of $\mathbf{R}^n$ has a basis. Moreover,* $\dim(W) \le n$.

Proof. Every vector in W is a linear combination of vectors in the standard basis $\mathscr{E}_n$. The subspace W is nonzero. If $\mathbf{w} \in W \setminus \{\mathbf{0}\}$, then $\{\mathbf{w}\}$ is a linearly independent subset of W (Exercise 3). By Theorem 1.1, if S is any linearly independent subset of W, then $|S| \leq n$. It follows that there exists a largest (with respect to inclusion) linearly independent subset S_1 of W, Let W_1 be the subspace of W generated by S_1. If W_1 is a proper subset of W, then there exists a vector $\mathbf{v} \in W \setminus W_1$. By Theorem 1.16, the set $S = S_1 \cup \{\mathbf{v}\}$ is a linearly independent subset of W, and $|S_1| = |S| + ! > |S|$, which contradicts the maximality of S. Therefore, S is a linearly independent set that generates W, and so S is a basis for W. Therefore, $\dim(W) = |S| \leq n$. This completes the proof.

Theorem 1.17. *Let W_1 and W_2 be subspaces of $\mathbf{R}^n$ with $W_1 \subseteq W_2$. Let $\dim(W_1) = k$ and $\dim(W_2) = \ell$. If $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ is a basis for W_1, then there exist vectors $\mathbf{w}_{k+1}, \mathbf{w}_{k+2}, \ldots, \mathbf{w}_\ell$ in $\mathbf{R}^n$ such that $\{\mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{w}_{k+1}, \mathbf{w}_{k+2}, \ldots, \mathbf{w}_\ell\}$ is a basis for W_2.*

Proof. Let $\{\mathbf{w}_{k+1}, \mathbf{w}_{k+2}, \ldots, \mathbf{w}_{k+r}\}$ be a maximal subset of $W_2 \setminus W_1$ such that the set $S' = \{\mathbf{w}_1, \ldots, \mathbf{w}_k, \mathbf{w}_{k+1}, \mathbf{w}_{k+2}, \ldots, \mathbf{w}_{k+r}\}$ is linearly independent. Let W_2' be the subspace of W_2 that is generated by S'. If $W_2' \neq W_2$, then there exists a vector $\mathbf{v} \in W_2 \setminus W_2'$, and the set $S' \cup \{\mathbf{v}\}$ is linearly independent. This contradicts the maximality of the set $\{\mathbf{w}_{k+1}, \mathbf{w}_{k+2}, \ldots, \mathbf{w}_{k+r}\}$. Therefore, $W_2' = W_2$ and the uniqueness of dimension implies that $k + r = \ell$. This completes the proof.

Theorem 1.18. *Let $V = \mathbf{R}^n$, and let W_1 and W_2 be subspaces of V. Then*

$$\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2).$$

Proof. By Theorem 1.10, the sumset $W_1 + W_2$ and the intersection $W_1 \cap W_2$ are subspaces of V. Let $\dim(W_1 \cap W_2) = d_0$,and let $\dim(W_1) = d_1$ and $\dim(W_2) = d_2$. Let $\{\mathbf{w}_1, \ldots, \mathbf{w}_{d_0}$ be a basis for $W_1 \cap W_2$. By Theorem 1.17, there exists sets of vectors $\{\mathbf{w}_{1,1}, \ldots, \mathbf{w}_{1,d_1-d_0}\}$ and $\{\mathbf{w}_{2,1}, \ldots, \mathbf{w}_{2,d_2-d_0}\}$ such that

$$\{\mathbf{w}_1, \ldots, \mathbf{w}_{d_0}\} \cup \{\mathbf{w}_{1,1}, \ldots, \mathbf{w}_{1,d_1-d_0}\}$$

is a basis for W_1 and

$$\{\mathbf{w}_1, \ldots, \mathbf{w}_{d_0}\} \cup \{\mathbf{w}_{2,1}, \ldots, \mathbf{w}_{2,d_2-d_0}\}$$

is a basis for W_2. It follows that the set

$$\mathscr{B} = \{\mathbf{w}_1, \ldots, \mathbf{w}_{d_0}, \mathbf{w}_{1,1}, \ldots, \mathbf{w}_{1,d_1-d_0}, \mathbf{w}_{2,1}, \ldots, \mathbf{w}_{2,d_2-d_0}\}$$

generates the subspace $W_1 + W_2$. We shall prove that this set is linearly independent. Let $x_1, \ldots, x_{d_0}, y_1, \ldots, y_{d_1-d_0}, z_1, \ldots, z_{d_2-d_0}$ be a sequence of scalars such that

$$\sum_{i=1}^{d_0} x_i \mathbf{w}_i + \sum_{j=1}^{d_1-d_0} y_j \mathbf{w}_{1,j} + \sum_{k=1}^{d_2-d_0} z_k \mathbf{w}_{2,k} = \mathbf{0}.$$

Therefore,

$$\sum_{i=1}^{d_0} x_i \mathbf{w}_i + \sum_{j=1}^{d_1-d_0} y_j \mathbf{w}_{1,j} = -\sum_{k=1}^{d_2-d_0} z_k \mathbf{w}_{2,k} \in W_1 \cap W_2.$$

It follows that $x_i = y_j = z_k = 0$ for all i, j, and k. Therefore, the set $\mathscr{B}$ is a basis for $W_1 + W_2$, and

$$\begin{aligned}\dim(W_1 + W_2) = |\mathscr{B}| = d_0 + (d_1 - d_0) + (d_2 - d_0) &= d_1 + d_2 - d_0 \\ &= \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2).\end{aligned}$$

This completes the proof.

Exercises

1. For each of the following subspaces of $\mathbf{R}^2$, construct a basis and determine the dimension.

   a. The subspace generated by the set
   $$S = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right\}.$$

   b. The subspace generated by the set
   $$S = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}.$$

   c. The subspace generated by the set
   $$S = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}.$$

   d. The subspace generated by the set
   $$S = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\}.$$

2. For each of the following subspaces of $\mathbf{R}^3$, construct a basis and determine the dimension.

   a. The subspace generated by the set
   $$S = \left\{ \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 5 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} \right\}.$$

   b. The subspace generated by the set

$$S = \left\{ \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 5 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 3 \\ 0 \end{pmatrix} \right\}.$$

c. The subspace generated by the set

$$S = \left\{ \begin{pmatrix} 6 \\ 9 \\ -3 \end{pmatrix}, \begin{pmatrix} -4 \\ -6 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \right\}.$$

3. Let $\mathbf{v}$ be a nonzero vector in $\mathbf{R}^n$. Prove that $\{x\mathbf{v} : x \in \mathbf{R}\}$ is a one-dimensional subspace of $\mathbf{R}^n$.
4. Let W_1 and W_2 be subspaces of $\mathbf{R}^n$ with $W_1 \subseteq W_2$, Prove that $W_1 = W_2$ if and only if $\dim(W_1) = \dim(W_2)$.
5. Let S be a set, and let P be a property of certain subsets of S. A subset S' of S is *maximal with respect to property* P if (i) S' has property P, and (ii) if $S' \subseteq S'' \subseteq S$ and S'' has property P, then $S' = S''$.

   a. Let $S \neq \{\mathbf{0}\}$ be a nonempty finite set of vectors. Prove that S contains a maximal linearly independent subset.
   b. Let $S \neq \{\mathbf{0}\}$ be a nonempty finite set of vectors that generates a subspace W, and let S' be a maximal linearly independent subset of S. Prove that S' is a basis for W.

6. Let S and T be sets.

   a. Prove that $S \cap T = S$ if and only if $S \subseteq T$.
   b. Prove that $S \cup T = T$ if and only if $S \subseteq T$.

7. Let $V = \mathbf{R}^n$. Let W_1 and W_2 be subspaces of V, let $W_0 = W_1 \cap W_2$, and let $W = \langle W_1 \cup W_2 \rangle$ be the subspace of V generated by $W_1 \cup W_2$. Let

$$\begin{aligned} d_0 &= \dim(W_0) \\ d_1 &= \dim(W_1) \\ d_2 &= \dim(W_2) \\ d &= \dim(W) \end{aligned}$$

   Let $\mathscr{B}_0 = \{\mathbf{w}_1, \dots, \mathbf{w}_d\}$ be a basis for W_0. Let $\mathscr{B}_1 = \{\mathbf{w}_{1,1}, \mathbf{w}_{1,2}, \dots, \mathbf{w}_{1,d_1-d_0}\}$ be a set of vectors in W_1 such that $\mathscr{B}_0 \cup \mathscr{B}_1$ is a basis for W_1. Let $\mathscr{B}_2 = \{\mathbf{w}_{2,1}, \mathbf{w}_{2,2}, \dots, \mathbf{w}_{2,d_2-d_0}\}$ be a set of vectors in W_2 such that $\mathscr{B}_0 \cup \mathscr{B}_2$ is a basis for W_2.

   a. Prove that the set of vectors $\mathscr{B}_0 \cup \mathscr{B}_1 \cup \mathscr{B}_2$ is linearly independent and a basis for the subspace W.
   b. Prove that

$$\dim(W_1) + \dim(W_2) = \dim(W_1 \cap W_2) + \dim(\langle W_1 \cup W_2 \rangle).$$

1.8 Rings and Fields

This section introduces important vocabulary that is ubiquitous in mathematics. We begin by isolating some properties of addition and multiplication of real numbers.

A *binary operation* on a set X is a function that assigns an element of X to every ordered pair of elements of X. For example, addition and multiplication are binary operations on the set of real numbers. With the binary operation of addition, the ordered pair $(3,4)$ goes to $3+4=7$. With the binary operation of multiplication, the ordered pair $(3,4)$ goes to $3 \cdot 4 = 12$.

Let X be a set with a binary operation that we denote by $*$. Thus, for every pair (a,b) of elements in X, the binary operation assigns the element $a * b \in X$. Here are properties that a binary operation might satisfy.

(P1) The binary operation is *associative* if, for all $x,y,z \in X$, we have

$$(x * y) * z = x * (y * z).$$

(P2) There exists an element $e \in X$ such that

$$e * x = x * e = x$$

for all $x \in X$. The element e is called an *identity* with respect to the binary operation. If $f \in X$ also satisfies $f * x = x * f = x$ for all $x \in X$, then

$$f = f * e = e$$

and so the identity element in X is unique.

(P3) Let X have an identity element e. Let $x \in X$. An element $y \in X$ is called an *inverse* of x if

$$x * y = y * x = e.$$

If z is also an inverse of x, then $x * z = e$ and

$$z = e * z = (y * x) * z = y * (x * z) = y * e = y.$$

Thus, if $x \in X$ has an inverse, then the inverse is unique.

(P4) The binary operation is *commutative* if, for all $x,y \in X$, we have

$$x * y = y * x.$$

With the binary operation of addition, the set $\mathbf{R}$ of real numbers satisfies properties (P1) – (P4). Let $x,y,z \in \mathbf{R}$. Associativity of addition is expressed by $(x+y)+z = x+(y+z)$ The identity element is 0, and the additive inverse of the real number x is the real number $-x$. Addition is commutative: $x+y = y+x$.

With the binary operation of multiplication, the set $\mathbf{R} \setminus \{0\}$ of nonzero real numbers satisfies properties (P1) – (P4). Let $x,y,z \in \mathbf{R} \setminus \{0\}$. Associativity of multiplication is expressed by $(xy)z = x(yz)$ The identity element is 1, and the additive inverse of the nonzero real number x is the real number $1/x$. Multiplication is commutative: $xy = yx$.

A *semigroup* is a set X with an associative binary operation, that is, X satisfies property (P1).

A *monoid* is a semigroup X that has an identity element, that is, X satisfies properties (P1) and (P2). The set of nonzero integers is a multiplicative monoid with identity 1.

A *group* is a set X with a binary operation that satisfies properties (P1), (P2). and (P3). The group X is *commutative* or *abelian* if it also satisfies property (P4).

The set of real numbers is an additive abelian group and the set of nonzero real numbers is a multiplicative abelian group. The set $\mathbf{Z}$ of integers and the set $\mathbf{Q}$ of rational numbers are also additive abelian groups. The set $\mathbf{R}_{>0}$ of positive real numbers is a multiplicative abelian group.

A *ring* is a set R with two binary operations, usually denoted by addition and multiplication, that satisfy the following properties.

(R1) With respect to addition, R is an additive abelian group with identity element 0.

(R2) With respect to multiplication, the set of nonzero elements of R, that is, $R \setminus \{0\}$, is a monoid with identity element 1.

(P3) Multiplication and addition satisfy *distributivity*: For all $x, y, z \in R$,

$$x(y+z) = xy + x \qquad \text{and} \qquad (x+y)z = xz + yz.$$

The ring R is *commutative* is multipication in R is commutative. The ring R is *noncommutative* is multipication in R is not commutative.

For example, with the usual operations of addition and multiplication, the integers $\mathbf{Z}$, the rational numbers $\mathbf{Q}$, and the real numbers $\mathbf{R}$ are commutative rings. The set $\{0\}$ with addition defined by $0+0=0$ and multiplication defined by $0 \cdot 0 = 0$ is also a ring, called the *zero ring*.

Let R be a ring, and let $x, y \in R$. We denote the additive inverse of y by $-y$. We define subtraction by

$$x - y = x + (-y).$$

Because 0 is the additive identity, we have

$$0 = 0 + 0$$

By distributivity,

$$0x = (0+0)x = 0x + 0x.$$

Subtracting $0x$ from both sides of this equation, we obtain

$$0 = 0x - 0x = (0x + 0x) - 0x = 0x + (0x - 0x) = 0x + 0 = 0x$$

and so $0x = 0$ for all $x \in R$. Similarly, $x0 = 0$ for all $x \in R$.

An element x in a ring R is a *unit* if there exists $y \in R$ such that $xy = yx = 1$. The element y is called a *multiplicative inverse* of x.

If y and z are multiplicative inverses of x, then $xy = zx = 1$ and

$$z = z1 = z(xy) = (zx)y = 1y = y$$

and so every unit x has a unique multiplicative inverse, denoted x^{-1}.

A *field* is a commutative ring that satisfies the following property:

(R4) Every nonzero element of R has an inverse.

The rings **Q** and **R** are fields, but the ring **Z** is not a field. We often use the boldface letter **F** to denote an arbitrary field.

In linear algebra, an element of a field is called a *scalar*.

A *complex number* is a number of the form $x+yi$, where $x, y \in \mathbf{R}$ and $i^2 = -1$. Let **C** denote the set of complex numbers. We define addition and multiplication of complex numbers as follows: If $z_1 = x_1 + y_1 i \in \mathbf{C}$ and $z_2 = x_2 + y_2 i \in \mathbf{C}$, then

$$z_1 + z_2 = (x_1 + y_1 i) + (x_2 + y_2 i) = (x_1 + x_2) + (y_1 + y_2)i$$

and

$$z_1 z_2 = (x_1 + y_1 i)(x_2 + y_2 i) = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + y_1 x_2)i.$$

The additive and multiplicative identities in **C** are $0 = 0 + 0i$ and $1 = 1 + 0i$.

A complex number $z = x+yi$ is nonzero if and only if $(x,y) \neq (0,0)$. Equivalently, $z = x+yi \neq 0$ if and only if $x^2 + y^2 > 0$.

The additive inverse of $z = x+yi$ is $-z = (-x)+(-y)i$. The multiplicative inverse of a nonzero complex number $z = x+yi$ is

$$z^{-1} = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2} i.$$

A straightforward (and long) calculation shows that addition and multiplication of complex numbers satisfy properties (P1)–(P4) and (R1)-(R4), and so the set **C** of complex numbers is a field.

In this chapter we studied solutions of linear equations with coefficients in the field of real numbers. It is important to note that the only properties of real numbers that we used are the properties of a field, and so our results also apply to linear equations with coefficients in the field **C** of complex numbers, with coefficients in the field **Q** of rational numbers, and, more generally, to linear equations with coefficients in any field **F**. In this chapter, we could have considered vector spaces over an arbitrary field. The only topics whose definitions depend on the real numbers are affine subspace and convex sets.

Exercises

1. Prove that the set **C** of complex numbers is a field.
2. In the field **C**, prove the following:

   a.

$$i^2 = -1$$

b.
$$\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)^2 = i$$

c.
$$\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^3 = -1$$

3. Prove that the set
$$\{x + y\sqrt{2} : x \in \mathbf{Q} \text{ and } y \in \mathbf{Q}\}$$
is a field.

4. Let $\mathbf{F}_2 = \{0, 1\}$. Define addition in $\mathbf{F}_2$ by
$$0 + 0 = 1 + 1 = 0 \qquad \text{and} \qquad 1 + 0 = 0 + 1 = 1.$$
Define multiplication in $\mathbf{F}_2$ by
$$0 \cdot 0 = 1 \cdot 0 = 0 \cdot 1 = 0 \qquad \text{and} \qquad 1 \cdot 1 = 1.$$
The addition and multiplication tables in $\mathbf{F}_2$ are
$$\begin{array}{c|c|c} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 1 & & 0 \end{array} \qquad \text{and} \qquad \begin{array}{c|c|c} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ \hline 1 & 0 & 1 \end{array}$$
Prove that $\mathbf{F}_2$ is a field.

5. Let $\mathbf{F}_3 = \{0, 1, 2\}$. The addition table for $\mathbf{F}_3$ is
$$\begin{array}{c|c|c|c} + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ \hline 1 & 1 & 2 & 0 \\ \hline 2 & 2 & 0 & 1 \end{array}$$
The multiplication table for $\mathbf{F}_3$ is
$$\begin{array}{c|c|c|c} \cdot & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 2 \\ \hline 2 & 0 & 2 & 1 \end{array}$$
Prove that $\mathbf{F}_3$ is a field.

6. Let R be a ring that is not necessarily commutative. For $a, b \in R$, define the *Lie bracket*
$$[a, b] = ab - ba \in R.$$

a. Prove that $[a,b] = 0$ if and only if the ring elements a and b commute.
b. Prove that $[a,b] = -[b,a]$.
c. Prove that
$$[[a,b],c] + [[b,c],a] + [[c,a],b] = 0$$
for all $a,b,c \in R$.

1.9 Additional topics

1.9.1 Affine subspaces

Let $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ be a finite sequence of vectors in $\mathbf{R}^n$. The vector $\mathbf{w}$ is an *affine combination* of vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ if there exist scalars $t_0, t_1, \ldots, t_k$ such that
$$\sum_{i=0}^{k} t_i = 1$$
and
$$\mathbf{w} = \sum_{i=0}^{k} t_i \mathbf{v}_i.$$

Recall that the translate of a set W of vectors in $\mathbf{R}^n$ by a vector $\mathbf{v}^* \in \mathbf{R}^n$ is the set
$$\mathbf{v}^* + W = \{\mathbf{v}^* + \mathbf{x} : \mathbf{x} \in W\}$$
and that an affine subspace of $\mathbf{R}^n$ is a translate of a vector subspace of $\mathbf{R}^n$.

Theorem 1.19. *A nonempty subset L of $\mathbf{R}^n$ is an affine subspace if and only if it is closed under affine combinations, that is, if and only if every affine combination of vectors in L is a vector in L.*

Proof. If L is an affine subspace of $\mathbf{R}^n$, then there is a subspace W of V and a vector $\mathbf{v}^* \in V$ such that $L = \mathbf{v}^* + W$. Let $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_k$ be vectors in L. There exist vectors $\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_k$ such that $\mathbf{x}_i = \mathbf{w}_i + \mathbf{v}$ for all $i = 0, 1, \ldots, k$. Let $t_0, t_1, \ldots, t_k$ be scalars such that $\sum_{i=0}^{k} t_i = 1$. We have
$$\sum_{i=0}^{k} t_i \mathbf{w}_i \in W$$
and
$$\sum_{i=0}^{k} t_i \mathbf{x}_i = \sum_{i=0}^{k} t_i (\mathbf{w}_i + \mathbf{v}^*) = \sum_{i=0}^{k} t_i \mathbf{w}_i + \sum_{i=0}^{k} t_i \mathbf{v}^* = \sum_{i=0}^{k} t_i \mathbf{v}_i + \mathbf{v}^* \in L.$$

Thus, every affine subspace is a nonempty subset of $\mathbf{R}^n$ that is closed under affine combinations.

Conversely, let L be a nonempty subset of $\mathbf{R}^n$ that is closed under affine combinations. Let $\mathbf{v}^* \in L$. We shall show that $W = L - \mathbf{v}^*$ is a vector subspace of $\mathbf{R}^n$, and so $L = \mathbf{v}^* + W$ is an affine subspace.

We have $\mathbf{0} = \mathbf{v}^* - \mathbf{v}^* \in W$. Let $\mathbf{w}_1, \mathbf{w}_2 \in W$. There exist vectors $\mathbf{x}_1, \mathbf{x}_2 \in L$ such that $\mathbf{w}_1 = \mathbf{x}_1 - \mathbf{v}^*$ and $\mathbf{w}_2 = \mathbf{x}_2 - \mathbf{v}^*$. Because

$$1 + 1 - 1 = 1$$

we have the affine combination

$$\mathbf{x}_1 + \mathbf{x}_2 - \mathbf{v}^* \in L$$

and so

$$\mathbf{w}_1 + \mathbf{w}_2 = (\mathbf{x}_1 - \mathbf{v}^*) + (\mathbf{x}_2 - \mathbf{v}^*) = (\mathbf{x}_1 + \mathbf{x}_2 - \mathbf{v}^*) - \mathbf{v}^* \in L - \mathbf{v}^* = W.$$

Thus, W is closed under vector addition. Similarly, for every scalar t, we have

$$t\mathbf{w}_1 + \mathbf{v}^* = t(\mathbf{w}_1 + \mathbf{v}^*) + (1-t)\mathbf{v}^* \in L$$

and so $t\mathbf{w}_1 \in W$. Thus, W is also closed under scalar multiplication, and so W is a vector subspace. . This completes the proof.

Lemma 1.7. *Let $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ be a finite sequence of vectors in $\mathbf{R}^n$. The set L of all affine combinations of $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ is an affine subspace.*

Proof. By Theorem 1.20, it suffices to prove that every affine combination of vectors in L is a vector in L.

Let $\mathbf{x}_j \in L$ for $j \in \{1, \ldots, \ell\}$. For each j, there exist scalars $t_{i,j}$ for $i \in \{0, 1, \ldots, k\}$ such that

$$\sum_{i=0}^{k} t_{i,j} = 1 \qquad \text{and} \qquad \mathbf{x}_j = \sum_{i=0}^{k} t_{i,j}\mathbf{v}_i.$$

Let $s_1, \ldots, s_\ell$ be scalars such that

$$\sum_{j=1}^{\ell} s_j = 1.$$

We must prove that

$$\mathbf{x} = \sum_{j=1}^{\ell} s_j \mathbf{x}_j \in L.$$

Let

$$u_i = \sum_{j=1}^{\ell} s_j t_{i,j}$$

for $i \in \{0, 1, \ldots, k\}$. We have

$$\sum_{i=0}^{k} u_i = \sum_{i=0}^{k}\sum_{j=1}^{\ell} s_j t_{i,j} = \sum_{j=1}^{\ell} s_j \sum_{i=0}^{k} t_{i,j} = \sum_{j=1}^{\ell} s_j = 1$$

and so

$$\mathbf{x} = \sum_{j=1}^{\ell} s_j \mathbf{x}_j = \sum_{j=1}^{\ell} s_j \sum_{i=0}^{k} t_{i,j}\mathbf{v}_i = \sum_{i=0}^{k}\left(\sum_{j=1}^{\ell} s_j t_{i,j}\right)\mathbf{v}_i = \sum_{i=0}^{k} u_i \mathbf{v}_i$$

is an affine combination of $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$. Therefore, $\mathbf{x} \in L$. This completes the proof.

Theorem 1.20. *Let $\mathscr{L}$ be a nonempty set of vectors in the vector space V. The set L of all affine combinations of finite sequences of vectors in $\mathscr{L}$ is an affine subspace of V.*

Proof. Let $\mathbf{x}_i \in L$ for $i \in \{1, \ldots, \ell\}$, and let $\mathbf{x}$ be an affine combination of the sequence of vectors $\mathbf{x}_1, \ldots, \mathbf{x}_\ell$. For each $i \in \{1, \ldots, \ell\}$, there is a finite sequence of vectors $\mathbf{v}_{i,1}, \ldots, \mathbf{v}_{i,k_i} \in L$ such that $\mathbf{x}_i$ is an affine combination of the vectors in this sequence. The set

$$\mathscr{L}' = \left\{\mathbf{v}_{i,j} : i \in \{1, \ldots, \ell\} \text{ and } j \in \{1, \ldots, k_i\}\right\}$$

is a finite subset of $\mathscr{L}$, and each vector $\mathbf{x}_i$ is an affine combination of a finite sequence of vectors in $\mathscr{L}'$. By Lemma 1.7, the vector $\mathbf{x}$ is also an affine combination of vectors in this sequence, and so $\mathbf{x} \in L$. This completes the proof.

The *line* through distinct vectors $\mathbf{x}_1$ and $\mathbf{x}_2$ in $\mathbf{R}^n$ is the affine subspace generated by $\mathbf{x}_1$ and $\mathbf{x}_2$, that is, the set of all affine combinations of $\mathbf{x}_1$ and $\mathbf{x}_2$:

$$\{t_1\mathbf{x}_1 + t_2\mathbf{x}_2 : t_1, t_2 \in \mathbf{R} \text{ and } t_1 + t_2 = 1\}.$$

We can also write this in the form

$$\{t\mathbf{x}_1 + (1-t)\mathbf{x}_2 : t \in \mathbf{R}\}.$$

For example, in the vector space $\mathbf{R}^2$, the line through the vectors $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$ is

$$\begin{aligned} L &= \left\{t\begin{pmatrix}1\\0\end{pmatrix} + (1-t)\begin{pmatrix}0\\1\end{pmatrix} : t \in \mathbf{R}\right\} = \left\{\begin{pmatrix}t\\1-t\end{pmatrix} : t \in \mathbf{R}\right\} \\ &= \left\{\begin{pmatrix}x\\y\end{pmatrix} : y = 1-x\right\}. \end{aligned}$$

Thus, L is the line $x + y = 1$.

In the vector space $\mathbf{R}^3$, the line through the vectors $\begin{pmatrix}1\\3\\-2\end{pmatrix}$ and $\begin{pmatrix}4\\-1\\7\end{pmatrix}$ is

$$L = \left\{ t \begin{pmatrix} 1 \\ 3 \\ -2 \end{pmatrix} + (1-t) \begin{pmatrix} 4 \\ -1 \\ 7 \end{pmatrix} : t \in \mathbf{R} \right\} = \left\{ \begin{pmatrix} 4-3t \\ -1+4t \\ 7-9t \end{pmatrix} : t \in \mathbf{R} \right\}$$
$$= \left\{ \begin{pmatrix} 4 \\ -1 \\ 7 \end{pmatrix} + t \begin{pmatrix} -3 \\ 4 \\ -9 \end{pmatrix} : t \in \mathbf{R} \right\}.$$

Theorem 1.21. *A nonempty subset L of $\mathbf{R}^n$ is an affine subspace if and only if L contains the line through every pair of points in L.*

Proof. An affine subspace is closed under affine combinations, and so contains the line through every pair of distinct points.

Conversely, let L be a nonempty subset of $\mathbf{R}^n$ that contains the line through every pair of distinct points in L. We shall prove by induction on k that L contains every affine combination of the form

$$\mathbf{y} = t_1\mathbf{x}_1 + \cdots + t_k\mathbf{v}_k \tag{1.38}$$

where $t_1, \ldots, t_k$ are scalars such that $\sum_{i=1}^k t_i = 1$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \in L$.

We have $\mathbf{y} \in L$ for $k = 2$ because L contains every line. Let $k \geq 3$, and assume that L contains all affine combinations of $k-1$ vectors in L. In the affine representation (1.38), we must have $t_j \neq 1$ for some $j \in \{1, \ldots, k\}$. It follows that

$$1 - t_j \neq 0$$

and

$$\sum_{\substack{1=1 \\ i\neq j}}^{k} \frac{t_i}{1-t_j} = 1.$$

The induction hypothesis implies that

$$\frac{1}{1-t_j} \sum_{\substack{1=1 \\ i\neq j}}^{k} t_i\mathbf{x}_i = \sum_{\substack{1=1 \\ i\neq j}}^{k} \frac{t_i}{1-t_j}\mathbf{x}_i \in L.$$

Because L contains every line, we have

$$\begin{aligned} \mathbf{y} = \sum_{i=1}^{k} t_i\mathbf{x}_i &= t_j\mathbf{x}_j + \sum_{\substack{1=1 \\ i\neq j}}^{k} t_i\mathbf{x}_i \\ &= t_j\mathbf{x}_j + (1-t_j)\left(\frac{1}{1-t_j} \sum_{\substack{1=1 \\ i\neq j}}^{k} t_i\mathbf{x}_i \right) \in L. \end{aligned}$$

This completes the proof.

A finite sequence of vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ is *affinely dependent* if there exist scalars $t_0, t_1, \ldots, t_k$ such that

$$t_0 + t_1 + \cdots + t_k = 0$$

$$t_j \neq 0 \text{ for some } j \in \{0, 1, \ldots, k\}$$

and

$$t_0\mathbf{v}_0 + t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_k\mathbf{v}_k = \mathbf{0}.$$

In this case, we have

$$\sum_{\substack{i=0 \\ i\neq j}}^{k} t_i = -t_j$$

and so

$$\sum_{\substack{i=0 \\ i\neq j}}^{k} \left(-\frac{t_i}{t_j}\right) = 1$$

and

$$\mathbf{v}_j = \sum_{\substack{i=0 \\ i\neq j}}^{k} \left(-\frac{t_i}{t_j}\right) \mathbf{v}_i.$$

Thus, if a sequence of vectors is affinely dependent, then some vector in the sequence is an affine combination of the other vectors in the sequence.

Conversely, if $\mathbf{v}_j$ is an affine combination of the sequence of vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_k$, then there exist scalars $t_0, t, \ldots, t_{j-1}, t_{j+1}, \ldots, t_k$ such that

$$\sum_{\substack{i=0 \\ i\neq j}}^{k} t_i = 1 \qquad \text{and} \qquad \sum_{\substack{i=0 \\ i\neq j}}^{k} \mathbf{v}_i = \mathbf{v}_j.$$

Setting $t_j = -1$, we obtain

$$\sum_{i=0}^{k} t_i = 1 \qquad \text{and} \qquad \sum_{i=0}^{k} \mathbf{v}_i = \mathbf{0}$$

and so the sequence of vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ is affinely dependent. Thus, if one vector in a sequence of vectors is an affine combination of the other vectors in the sequence, then the sequence of vectors is affinely dependent.

A sequence of vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ is *affinely independent* if it is not affinely dependent. We have proved the following.

Lemma 1.8. *The sequence of vectors* $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ *is affinely independent if and only if no vector in the sequence is an affine combination of the other vectors in the sequence.*

Consider the vectors

$$\begin{pmatrix} -1 \\ -2 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \quad \begin{pmatrix} 3 \\ 1 \end{pmatrix}. \tag{1.39}$$

If

$$t_0 \begin{pmatrix} -1 \\ -2 \end{pmatrix} + t_1 \begin{pmatrix} 0 \\ -1 \end{pmatrix} + t_2 \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} -t_0 + 3t_2 \\ -2t_0 - t_1 + t_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

then

$$-t_0 + 3t_2 = -2t_0 - t_1 + t_2 = 0$$

and so

$$t_0 = 3t_2, \qquad t_1 = -5t_2, \qquad \text{and} \qquad t_0 + t_1 + t_2 = -t_2.$$

If

$$t_0 + t_1 + t_2 = 0$$

then $t_0 = t_1 = t_2 = 0$. It follows that the vectors in (1.39) are affinely independent. Note that

$$3 \begin{pmatrix} -1 \\ -2 \end{pmatrix} - 5 \begin{pmatrix} 0 \\ -1 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

and so the vectors in (1.39) are linearly dependent.

The vectors

$$\begin{pmatrix} 1 \\ 7 \end{pmatrix}, \quad \begin{pmatrix} -9 \\ 2 \end{pmatrix}, \quad \begin{pmatrix} -3 \\ 5 \end{pmatrix}$$

are affinely dependent because

$$3 + 2 + (-5) = 0$$

and

$$3 \begin{pmatrix} 1 \\ 7 \end{pmatrix} + 2 \begin{pmatrix} -9 \\ 2 \end{pmatrix} - 5 \begin{pmatrix} -3 \\ 5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Theorem 1.22. *The following are equivalent:*

(i) The sequence of vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ *is affinely independent.*

(ii) The sequence of vectors

$$\mathbf{v}_0 - \mathbf{v}_r, \mathbf{v}_1 - \mathbf{v}_r, \ldots, \mathbf{v}_{r-1} - \mathbf{v}_r, \mathbf{v}_{r+1} - \mathbf{v}_r, \ldots, \mathbf{v}_k - \mathbf{v}_r$$

is linearly independent for all $r \in \{0, 1, \ldots, k\}$.

(iii) The sequence of vectors

$$\mathbf{v}_0 - \mathbf{v}_r, \mathbf{v}_1 - \mathbf{v}_r, \ldots, \mathbf{v}_{r-1} - \mathbf{v}_r, \mathbf{v}_{r+1} - \mathbf{v}_r, \ldots, \mathbf{v}_k - \mathbf{v}_r$$

is linearly independent for some $r \in \{0, 1, \ldots, k\}$.

Proof. Let $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ be an affinely independent sequence of vectors, let $r \in \{0, 1, \ldots, k\}$, and let $t_0, t_1, \ldots, t_{r-1}, t_{r+1}, \ldots, t_k$ be scalars such that

$$\sum_{\substack{i=0\\i\neq r}}^{k} t_i(\mathbf{v}_i - \mathbf{v}_r) = \mathbf{0}.$$

Defining

$$t_r = -\sum_{\substack{i=0\\i\neq r}}^{k} t_i,$$

we obtain

$$\sum_{i=0}^{k} t_i = 0$$

and

$$\begin{aligned}\sum_{i=0}^{k} t_i\mathbf{v}_i &= \sum_{\substack{i=0\\i\neq r}}^{k} t_i\mathbf{v}_i + t_r\mathbf{v}_r = \sum_{\substack{i=0\\i\neq r}}^{k} t_i\mathbf{v}_i - \left(\sum_{\substack{i=0\\i\neq r}}^{k} t_i\right)\mathbf{v}_r\\ &= \sum_{\substack{i=0\\i\neq r}}^{k} t_i\mathbf{v}_i - \sum_{\substack{i=0\\i\neq r}}^{k} t_i\mathbf{v}_r = \sum_{\substack{i=0\\i\neq r}}^{k} t_i(\mathbf{v}_i - \mathbf{v}_r) = \mathbf{0}.\end{aligned}$$

The affine independence of $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ implies that $t_i = 0$ for all $i = 0, 1, \ldots, k$, and so the sequence of vectors in (ii) is linearly independent for all $r \in \{0, 1, \ldots, k\}$. Thus, (i) implies (ii). Clearly, (ii) implies (iii).

Suppose that (iii) holds for some $r \in \{0, 1, \ldots, k\}$. Let $t_0, t_1, \ldots, t_k$ be scalars such that

$$t_0 + t_1 + \cdots + t_k = 0,$$

and

$$t_0\mathbf{v}_0 + t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_k\mathbf{v}_k = \mathbf{0}.$$

We have

$$t_r = -\sum_{\substack{i=0\\i\neq r}}^{k} t_i$$

and so

$$\begin{aligned}\mathbf{0} &= \sum_{i=0}^{k} t_i\mathbf{v}_i = \sum_{\substack{i=0\\i\neq r}}^{k} t_i\mathbf{v}_i + t_r\mathbf{v}_r = \sum_{\substack{i=0\\i\neq r}}^{k} t_i\mathbf{v}_i - \left(\sum_{\substack{i=0\\i\neq r}}^{k} t_i\right)\mathbf{v}_r\\ &= \sum_{\substack{i=0\\i\neq r}}^{k} t_i(\mathbf{v}_i - \mathbf{v}_r).\end{aligned}$$

The linear independence of the sequence of vectors

$$\mathbf{v}_0 - \mathbf{v}_r, \mathbf{v}_1 - \mathbf{v}_r, \ldots, \mathbf{v}_{r-1} - \mathbf{v}_r, \mathbf{v}_{r+1} - \mathbf{v}_r, \ldots, \mathbf{v}_k - \mathbf{v}_r$$

implies that $t_i = 0$ for all $i \neq r$. It follows that $t_r = 0$, and so the sequence of vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ is affinely independent. Thus, (iii) implies (i). This completes the proof.

We observe that the representation of a vector as an affine combination of a sequence of vectors is not necessarily unique. For example,

$$\begin{pmatrix} 43 \\ 28 \end{pmatrix} = 7\begin{pmatrix} 1 \\ 7 \end{pmatrix} - 3\begin{pmatrix} -9 \\ 2 \end{pmatrix} - 3\begin{pmatrix} -3 \\ 5 \end{pmatrix} = 4\begin{pmatrix} 1 \\ 7 \end{pmatrix} - 5\begin{pmatrix} -9 \\ 2 \end{pmatrix} + 2\begin{pmatrix} -3 \\ 5 \end{pmatrix}$$

are distinct affine combinations of the vectors $\begin{pmatrix} 1 \\ 7 \end{pmatrix}$, $\begin{pmatrix} -9 \\ 2 \end{pmatrix}$, and $\begin{pmatrix} -3 \\ 5 \end{pmatrix}$.

Lemma 1.9. *Let L be the affine subspace generated by a finite sequence $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ of affinely independent vectors. Let $\mathbf{w} \in L$. If $a_0, a_1, \ldots, a_k$ and $b_0, b_1, \ldots, b_k$ are scalars such that*

$$\sum_{i=0}^{k} a_i = \sum_{i=0}^{k} b_i = 1$$

and

$$\mathbf{w} = \sum_{i=0}^{k} a_i \mathbf{v}_i = \sum_{i=0}^{k} b_i \mathbf{v}_i$$

then $a_i = b_i$ for all $i = 0, 1, \ldots, k$.

Proof. We have

$$\mathbf{0} = \mathbf{w} - \mathbf{w} = \sum_{i=0}^{k} (a_i - b_i)\mathbf{v}_i$$

and

$$\sum_{i=0}^{k} (a_i - b_i) = \sum_{i=0}^{k} a_i - \sum_{i=0}^{k} b_i = 1 - 1 = 0.$$

The affine independence of $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$ implies that $a_i = b_i$ for all $i = 0, 1, \ldots, k$. This completes the proof.

It follows from Lemma 1.9 that if $\mathbf{w}$ is a vector in the affine subspace generated by an affinely independent sequence of vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$, then $\mathbf{w}$ has a unique representation as a linear combination

$$\mathbf{w} = \sum_{i=0}^{k} a_i \mathbf{v}_i$$

whose coordinates satisfy the affine equation

$$\sum_{i=0}^{k} a_i = 1.$$

The scalars $a_0, a_1, \ldots, a_k$ are called the *barycentric coordinates* of $\mathbf{w}$ with respect to the sequence of vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k$, .

For example, in $\mathbf{R}^3$, the vectors

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \qquad \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \qquad \mathbf{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

are affinely independent, and the affine space they generate is the hyperplane

$$L = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : x + y + z = 0 \right\}.$$

Let L be the affine subspace in $\mathbf{R}^2$ generated by the affinely independent sequence of vectors

$$\begin{pmatrix} -1 \\ -2 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 3 \\ 1 \end{pmatrix}. \tag{1.40}$$

Let us determine if the vectors $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 5 \\ 4 \end{pmatrix}$ are in L, and, if so, compute their barycentric coordinates.

We have $\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L$ if and only if there exist scalars a_0, a_1, a_2 such that

$$a_0 + a_1 + a_2 = 1$$

and

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = a_0 \begin{pmatrix} -1 \\ -2 \end{pmatrix} + a_1 \begin{pmatrix} 0 \\ -1 \end{pmatrix} + a_2 \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} -a_0 + 3a_2 \\ -2a_0 - a_1 + a_2 \end{pmatrix}.$$

It follows that

$$a_0 = 3a_2 - 1 \qquad \text{and} \qquad a_1 = -5a_2 + 1$$

and so

$$-a_2 = a_0 + a_1 + a_2 = 1$$

Therefore,

$$a_0 = 2, \quad a_1 = -4, \quad \text{and} \quad a_2 = 3$$

are the barycentric coordinates of the vector $\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in L$.

For all $m, b \in \mathbf{R}$, the line in $\mathbf{R}^2$ defined by the equation $y = mx + b$ is the set of vectors

$$\begin{aligned} L &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : y = mx + b \right\} \\ &= \left\{ \begin{pmatrix} x \\ mx + b \end{pmatrix} : x \in \mathbf{R} \right\} \\ &= \left\{ \begin{pmatrix} 0 \\ b \end{pmatrix} + x \begin{pmatrix} 1 \\ m \end{pmatrix} : x \in \mathbf{R} \right\} \\ &= \mathbf{v} + W, \end{aligned}$$

where $\mathbf{v} = \begin{pmatrix} 0 \\ b \end{pmatrix}$ and W is the vector subspace generated by $\begin{pmatrix} 1 \\ m \end{pmatrix}$. Thus, the line L is an affine subspace of $\mathbf{R}^2$. We can also write

$$\begin{aligned} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ mx + b \end{pmatrix} &= \begin{pmatrix} x \\ x(m+b) \end{pmatrix} + \begin{pmatrix} 0 \\ (1-x)b \end{pmatrix} \\ &= x \begin{pmatrix} 1 \\ m + b \end{pmatrix} + (1-x) \begin{pmatrix} 0 \\ b \end{pmatrix} \end{aligned}$$

and so L is also the set of all affine combinations of the affinely independent vectors $\begin{pmatrix} 1 \\ m+b \end{pmatrix}$ and $\begin{pmatrix} 0 \\ b \end{pmatrix}$.

For example, the line $y = 2x + 3$ in $\mathbf{R}^2$ is the affine subspace $L = \begin{pmatrix} 0 \\ 3 \end{pmatrix} + W$, where W is the vector subspace generated by the vector $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$. The affine space L is also the set of all affine combinations of the affinely independent vectors $\begin{pmatrix} 1 \\ 5 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 3 \end{pmatrix}$.

Let V be a finite-dimensional vector space over the field $\mathbf{R}$, and let L be an affine subspace of V. Let $\mathbf{v}^* \in L$, and consider the vector subspace $W = L - \mathbf{v}^*$. By Exercise 9, the subspace W is independent of the choice of the vector $\mathbf{v}^* \in L$. If $\dim(V) = n$, then $\dim(W) \leq n$. We define the *affine dimension* of L as follows: For any vector $\mathbf{v}^* \in L$,

$$\operatorname{affdim}(L) = \dim(W) = \dim(L - \mathbf{v}^*).$$

Lemma 1.10. *Let L be an affine subspace of the finite-dimensional vector space V. If $\mathscr{L}$ is a maximal affinely independent subset of L, then $\operatorname{affdim}(L) = |\mathscr{L}| - 1$.*

Proof. Let $\mathbf{v}^* \in L$ and let $W = L - \mathbf{v}^*$ be the associated vector subspace of L. Let $\dim(W) = k$. If $\mathscr{L}_0 = \{\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_h\}$ is an affinely independent subset of L, then, by Theorem 1.22, the set $\{\mathbf{w}_1 - \mathbf{w}_0, \ldots, \mathbf{w}_h - \mathbf{w}_0\}$ is a linearly independent subset of W, and so $|\mathscr{L}_0| - 1 = h \leq k = \dim(W)$.

Conversely, let $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ be a basis for W. The set $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is a linearly independent subset of W, and, by Theorem 1.22, the set $\mathscr{L}_1 = \{\mathbf{v}^*, \mathbf{v}_1 + \mathbf{v}^*, \ldots, \mathbf{v}_k + \mathbf{v}^*\}$ is an affinely independent subset of L. Therefore, $|\mathscr{L}_1| - 1 = k = \dim(W)$, and so $\mathscr{L}_1$ is a maximal affinely independent set of vectors in L.

Let $\{\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_h\}$ be an affinely independent subset of L. The set $\{\mathbf{w}_1 - \mathbf{w}_0, \ldots, \mathbf{w}_h - \mathbf{w}_0\}$ is a linearly independent subset of W. If $h < k = \dim(W)$, then there exist vectors $\mathbf{w}_{h+1}, \mathbf{w}_{h+2}, \ldots, \mathbf{w}_k \in V$ such that

$$\{\mathbf{w}_1 - \mathbf{w}_0, \ldots, \mathbf{w}_h - \mathbf{w}_0, \mathbf{w}_{h+1} - \mathbf{w}_0, \mathbf{w}_{h+2} - \mathbf{w}_0, \ldots, \mathbf{w}_k - \mathbf{w}_0\}$$

is a basis for W, and

$$\mathscr{L} = \{\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_h, \mathbf{w}_{h+1}, \mathbf{w}_{h+2}, \ldots, \mathbf{w}_k\}$$

is a maximal affinely independent set L.

Exercises

1. Compute the line in $\mathbf{R}^2$ generated by the vectors $\mathbf{x}_1 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$ and $\mathbf{x}_2 = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$.

   Solution:

$$\begin{aligned} L &= \left\{ t \begin{pmatrix} 1 \\ 3 \end{pmatrix} + (1-t) \begin{pmatrix} 3 \\ 4 \end{pmatrix} : t \in \mathbf{R} \right\} = \left\{ \begin{pmatrix} 3-2t \\ 4-3t \end{pmatrix} : t \in \mathbf{R} \right\} \\ &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : y = \frac{5}{2} + \frac{1}{2}x \right\}. \end{aligned}$$

   Thus, L is the line $x - 2y = -5$.
2. Prove that the sequence of vectors

$$\begin{pmatrix} -1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 5 \end{pmatrix}, \quad \begin{pmatrix} 4 \\ 11 \end{pmatrix}$$

   is affinely dependent.
3. Let L be the affine subspace generated by the vectors

$$\begin{pmatrix} -1 \\ -2 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

   For each of the following vectors $\mathbf{v}$, determine if $\mathbf{v} \in L$:

$$\begin{pmatrix} 17 \\ 16 \end{pmatrix}, \qquad \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} 3 \\ -2 \end{pmatrix}, \qquad \begin{pmatrix} -7 \\ -8 \end{pmatrix}.$$

4. Prove that the sequence of vectors

$$\begin{pmatrix} -1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 5 \end{pmatrix}, \quad \begin{pmatrix} 4 \\ 11 \end{pmatrix}$$

   is affinely independent.

5. Prove that the sequence of vectors
$$\begin{pmatrix}1\\0\\0\end{pmatrix}, \quad \begin{pmatrix}0\\1\\0\end{pmatrix}, \quad \begin{pmatrix}0\\0\\1\end{pmatrix}$$
is affinely independent.
6. Determine if the sequence of vectors
$$\begin{pmatrix}1\\1\\0\end{pmatrix}, \quad \begin{pmatrix}1\\0\\1\end{pmatrix}, \quad \begin{pmatrix}0\\1\\1\end{pmatrix}$$
is affinely dependent or affinely independent.
7. Prove that the sequence of vectors $\mathbf{v}_1, \mathbf{v}_2$ is linearly independent if and only if the sequence of vectors $\mathbf{0}, \mathbf{v}_1, \mathbf{v}_2$ is affinely independent.
8. Prove that if three vectors in $\mathbf{R}^2$ are collinear, then they are affinely dependent.
9. Let L be an affine subspace, and let $\mathbf{v}^*, \mathbf{w}^* \in L$. Prove that
$$L - \mathbf{v}^* = L - \mathbf{w}^*.$$
10. Let V be a vector space over the field $\mathbf{R}$, and let L be a nonempty subset of V. Prove that L is an affine subspace if and only if there exists a vector subspace W such that, for all $\mathbf{x} \in L$, we have $\mathbf{y} \in L$ if and only if $\mathbf{y} - \mathbf{x} \in W$.
11. Let $\mathscr{L}$ be a affinely independent subset of a real vector space V, and let L be the affine subspace generated by $\mathscr{L}$, that is, the set of all affine combinations of element of L. Prove that if $\mathbf{v} \in V \setminus L$, then the set $\mathscr{L} \cup \{\mathbf{v}\}$ is affinely independent.

1.9.2 Convex sets

Let V be a real vector space, and let $u, v \in V$. The *line segment* joining u and v is the set
$$[u, v] = \{(1-t)u + tv : 0 \leq t \leq 1\}.$$
If $u = v$, then $[u, v] = \{u\}$. A set K is *convex* if K contains every line segment joining two points in K. Equivalently, K is convex if $(1-t)u + tv \in K$ for all $u, v \in K$ and $t \in [0, 1]$. For example, V and $\emptyset$ are convex subsets of V.

Let h be a nonzero vector in $\mathbf{R}^n$ and let $\lambda \in \mathbf{R}$. The hyperplane
$$H = \{v \in \mathbf{R}^n : (v, h) = \lambda\}$$
is convex because, if $u, v \in H$ and $(u, h) = (v, h) = \lambda$, then
$$((1-t)u + tv, h) = (1-t)(u, h) + t(v, h) = (1-t)\lambda + t\lambda = \lambda.$$

The half space $H^- = \{v \in \mathbf{R}^n : (v,h) \leq \lambda\}$ is also convex because, if $u, v \in H^-$ and $(u,h) = (v,h) \leq \lambda$, then

$$((1-t)u + tv, h) = (1-t)(u,h) + t(v,h) \leq (1-t)\lambda + t\lambda = \lambda.$$

Similarly, the half space H^+ is convex.

Let $\mathbf{x}_1, \ldots, \mathbf{x}_k$ be elements of a real vector space V. The point $\mathbf{x}$ is a *convex combination* of $\mathbf{x}_1, \ldots, \mathbf{x}_k$ if there exist nonnegative real numbers $t_1, \ldots, t_k$ such that $\mathbf{x} = \sum_{i=1}^k t_i \mathbf{x}_i$ and $\sum_{i=1}^k t_i = 1$.

Theorem 1.23. *A subset K of V is convex if and only if K contains every convex combination of every finite subset of K.*

Proof. Let k be a positive integer. The vector $v \in V$ will be called a k-convex combination of the vectors $v_1, \ldots, v_k$ if there exist nonnegative real numbers $t_1, \ldots, t_k$ such that $v = \sum_{i=1}^k t_i v_i$ and $\sum_{i=1}^k t_i = 1$.

A convex set is, by definition, a set that contains all of its 2-convex combinations. If a set K contains every convex combination of every finite subset of K, then K contains every 2-convex combination and so K is a convex set.

Conversely, let K be a convex set. We shall prove by induction on k that K contains every k-convex combination of vectors in K. Because the only 1-convex combination of vectors in K is $v = 1 \cdot v$ for $v \in K$, the set K contains all of its 1-convex combinations. Because K is convex, it contains all of its 2-convex combinations.

Suppose that $k \geq 2$ and that the set K contains all of its k-convex combinations. Let $v_1, \ldots, v_{k+1} \in V$ and let $t_1, \ldots, t_{k+1} \in \mathbf{R}$ satisfy $\sum_{i=1}^{k+1} t_i = 1$ and $0 \leq t_i \leq 1$ for all $i = 1, \ldots, k+1$. If $t_j = 1$ for some j, then $t_i = 0$ for all $i \neq j$ and $\sum_{i=1}^{k+1} t_i v_i = t_j v_j = v_j \in V$. If $t_i < 1$ for all i, then $t_i/(1 - t_{k+1}) \geq 0$ for $i = 1, \ldots, k$ and

$$\sum_{i=1}^k \frac{t_i}{1 - t_{k+1}} = \frac{1}{1 - t_{k+1}} \sum_{i=1}^k t_i = \frac{1 - t_{k+1}}{1 - t_{k+1}} = 1.$$

The induction hypothesis implies that

$$v' = \sum_{i=1}^k \left(\frac{t_i}{1 - t_{k+1}} \right) v_i \in K.$$

Because K is convex, we have

$$\begin{aligned}(1 - t_{k+1})v' + t_{k+1}v_{k+1} &= (1 - t_{k+1}) \sum_{i=1}^k \left(\frac{t_i}{1 - t_{k+1}} \right) v_i + t_{k+1}v_{k+1} \\ &= \sum_{i=1}^{k+1} t_i v_i \in K.\end{aligned}$$

This completes the induction.

Theorem 1.24. *The intersection of a family of convex sets in a real vector space V is a convex set in V.*

Proof. Let $\{A_i\}_{i \in I}$ be a family of convex sets in V, and let $A = \bigcap_{i \in I} A_i$. If $\mathbf{x}, \mathbf{y} \in A$, then $\mathbf{x}, \mathbf{y} \in A_i$ for all $i \in I$, and so $[\mathbf{x}, \mathbf{y}] \in A_i$ for all $i \in I$. It follows that $[\mathbf{x}, \mathbf{y}] \in A$, and so A is convex.

Corollary 1.3. *Let K be a subset of a real vector space V. If K is the intersection of a family of hyperplanes and half spaces in V, then K is convex.*

A *polyhedral cone* is the intersection of a finite number of half spaces in a finite dimensional real vector space. By Corollary 1.3, every polyhedral cone is convex.

Theorem 1.25. *If $A_1, \ldots, A_h$ are convex sets in a real vector space V, and if $\lambda_1, \ldots, \lambda_h \in \mathbf{R}$, then the set $\lambda * A_1 + \cdots + \lambda_h * A_h$ is convex.*

Thus, linear combinations of convex sets are convex.

Proof. Let $K = \lambda * A_1 + \cdots + \lambda_h * A_h$. We have $u, v \in K$ if and only if there exist $u_i, v_i \in A_i$ for $i = 1, \ldots, h$ such that $u = \sum_{i=1}^h \lambda_i u_i$ and $v = \sum_{i=1}^h \lambda_i v_i$. If $0 \leq t \leq 1$, then $(1-t)u_i + tv_i \in A_i$ for $i = 1, \ldots, h$ and

$$(1-t)u + tv = (1-t)\sum_{i=1}^h \lambda_i u_i + t\sum_{i=1}^h \lambda_i v_i = \sum_{i=1}^h \lambda_i \left((1-t)u_i + tv_i\right) \in K.$$

Thus, the set K is convex.

Corollary 1.4. *If A is convex and $\lambda \in \mathbf{R}$, then the dilation $\lambda * A$ is convex.*

Proof. Let $h = 1$ in Theorem 1.25.

Corollary 1.5. *If $A_1, \ldots, A_h$ are convex sets in a real vector space V, then the sumset $A_1 + \cdots + A_h$ is convex. If A is convex and h is a positive integer, then the iterated sumset hA is convex.*

Proof. Let $\lambda_i = 1$ for $i = 1, \ldots, h$ in Theorem 1.25.

It is a simple but fundamental observation in additive number theory that the h-fold sum of a convex set is the same as the h-fold dilation of a convex set.

Theorem 1.26. *If K is a convex set in $\mathbf{R}^n$ and h is a positive integer, then*

$$hK = h * K.$$

Proof. Let $x_1, x_2, \ldots, x_h$ be a sequence of h not necessarily distinct elements of K. Since K is convex, it follows that

$$\frac{1}{h}x_1 + \frac{1}{h}x_2 + \cdots + \frac{1}{h}x_h \in K$$

and so

$$x_1 + x_2 + \cdots + x_h = h * \left(\frac{1}{h}x_1 + \frac{1}{h}x_2 + \cdots + \frac{1}{h}x_h\right) \in h * K.$$

This proves that $hK \subseteq h * K$.

Conversely, if $y \in h * K$, then $y = hx$ for some $x \in K$ and so

$$y = \underbrace{x + x + \cdots + x}_{h \text{ summands}} \in hK.$$

This proves that $h * K \subseteq hK$.

The set of all convex combinations of finite subsets of X, denoted $\operatorname{conv}(X)$, is called the *convex hull* of X. The dimension of X is the dimension of the affine hull of X.

Let $\mathbf{R}^d$ denote d-dimensional Euclidean space. Let $\mathbf{x} = (x_1, \ldots, x_d) \in \mathbf{R}^d$ and $\mathbf{y} = (y_1, \ldots, y_d) \in \mathbf{R}^d$. We have the usual inner product $(\mathbf{x}, \mathbf{y}) = x_1 y_1 + \cdots + x_d y_d$. The *line segment* between $\mathbf{x}$ and $\mathbf{y}$ is the set

$$[\mathbf{x}, \mathbf{y}] = \{(1-t)\mathbf{x} + t\mathbf{y} : 0 \leq t \leq 1\}.$$

A set K in $\mathbf{R}^d$ is *convex* if K contains the line segment between each pair of points in K, that is, $[\mathbf{x}, \mathbf{y}] \subseteq K$ for all $\mathbf{x}, \mathbf{y} \in K$.

Let X be a subset of $\mathbf{R}^d$. The space $\mathbf{R}^d$ is convex and contains X. The *convex hull* of X is the set

$$\operatorname{conv}(X) = \bigcap_{\substack{X \subseteq K \\ K \text{ convex}}} K.$$

By Theorem 1.24, $\operatorname{conv}(X)$ is convex, and is the smallest convex subset of $\mathbf{R}^d$ that contains X.

Lemma 1.11. *Let X be a subset of $\mathbf{R}^d$. The convex hull of X is the set of all convex combinations of finite subsets of X.*

Proof. We begin by proving that if K is a convex set that contains X, then K contains every convex combination of every finite subset F of X. The proof is by induction on $k = |F|$. If $k = 1$ and $\mathbf{x} \in X$, then $1 \cdot \mathbf{x} = \mathbf{x} \in K$. Let $k = 2$. If $\mathbf{x}_1, \mathbf{x}_2 \in X$ and if t_1 and t_2 are nonnegative real numbers such that $t_1 + t_2 = 1$, then

$$t_1 \mathbf{x}_1 + t_2 \mathbf{x}_2 \in [\mathbf{x}_1, \mathbf{x}_2] \subseteq K.$$

Let $k \geq 3$, and suppose that every convex combination of $k-1$ elements of X belongs to K. Let $\mathbf{x}_1, \ldots, \mathbf{x}_{k-1}, \mathbf{x}_k \in X$, let $t_1, \ldots, t_{k-1}, t_k$ be nonnegative real numbers such that $\sum_{i=1}^k t_i = 1$, and let $\mathbf{x} = \sum_{i=1}^k t_i \mathbf{x}_i$. If $t_1 = 0$, then $\mathbf{x}$ is a convex combination of $k-1$ elements of X, and so $\mathbf{x} \in K$. Suppose that $t_1 \neq 0$, and let $t = \sum_{i=1}^{k-1} t_i$. Then $t > 0$ and $t_k = 1 - t$. Since $\sum_{i=1}^{k-1} \frac{t_i}{t} = 1$, it follows that

$$\mathbf{x}' = \sum_{i=1}^{k-1} \frac{t_i}{t} \mathbf{x}_i$$

is a convex combination of $k-1$ elements of X, and so $\mathbf{x}' \in \operatorname{conv}(X)$. Therefore,

$$\mathbf{x} = t\mathbf{x}' + t_k\mathbf{x}_k \in K.$$

Thus, every convex set that contains X contains every convex combination of elements of X, and so the convex hull of X contains every convex combination of elements of X.

Let K^* be the set of all convex combinations of finite subsets of X. It suffices to prove that K^* is convex. Let $\mathbf{u}, \mathbf{v} \in K^*$. There is a finite subset $F = \{x_1, \ldots, x_k\}$ of X such that both $\mathbf{u}$ and $\mathbf{v}$ are convex combinations of elements of F. This means that there exist nonnegative real numbers $r_1, \ldots, r_k, s_1, \ldots, s_k$ such that

$$\sum_{i=1}^{k} r_i = \sum_{i=1}^{k} s_i = 1$$

and

$$\mathbf{u} = \sum_{i=1}^{k} r_i \mathbf{x}_i \quad \text{and} \quad \mathbf{v} = \sum_{i=1}^{k} s_i \mathbf{x}_i.$$

If $0 \leq t \leq 1$, then

$$\sum_{i=1}^{k} (tr_i + (1-t)s_i) = t\sum_{i=1}^{k} r_i + (1-t)\sum_{i=1}^{k} s_i = 1$$

and so

$$t\mathbf{u} + (1-t)\mathbf{v} = \sum_{i=1}^{k} (tr_i + (1-t)s_i)\,\mathbf{x}_i$$

is a convex combination of F. It follows that the line segment $[\mathbf{u}, \mathbf{v}]$ is contained in K^*. This completes the proof.

Theorem 1.27 (Radon). *Let A be a finite subset of an affine space X of dimension d. If $|A| \geq d+2$, then there is a partition of A into disjoint subsets A_1 and A_2 such that $conv(A_1) \cap conv(A_2) \neq \emptyset$. Moreover, this partition is unique if and only if $k = d+2$ and any $d+1$ points of A are affinely independent.*

A partition $A = A_1 \cup A_2$ with $\mathrm{conv}(A_1) \cap \mathrm{conv}(A_2) \neq \emptyset$ will be called a *Radon partition* of A.

Proof. Let $A = \{a_1, \ldots, a_k\}$, where $|A| = k \geq d+2$. If X is an affine space of dimension d, then X is a subset of $\mathbf{R}^n$ for some positive integer n, and X is the affine hull of a set of $d+1$ affinely independent points in $\mathbf{R}^n$. Every subset of X of cardinality at least $d+2$ is affinely dependent, and so A is affinely dependent. This means that there is a sequence of real numbers $\lambda_1, \ldots, \lambda_k$ not all 0 such that

$$\sum_{i=1}^{r} \lambda_i = 0$$

and

$$\sum_{i=1}^{r} \lambda_i a_i = 0.$$

Equivalently,

$$\lambda = \sum_{i=1}^{r} \lambda_i = -\sum_{i=r+1}^{k} \lambda_i$$

and

$$\lambda = \sum_{i=1}^{r} \lambda_i a_i = -\sum_{i=r+1}^{k} \lambda_i a_i.$$

We can renumber the elements of A so that $\lambda_i > 0$ for $i = 1, \ldots, r$ and $\lambda_1 \le 0$ for $i = r+1, \ldots, k$, where $1 \le r \le k-1$ and $\lambda_{r+1} < 0$. Let $A_1 = \{a_1, a_2, \ldots, a_r\}$ and $A_2 = \{a_{r+1}, \ldots, a_k\}$. Then

$$\sum_{i=1}^{r} \frac{\lambda_i}{\lambda} = \sum_{i=r+1}^{k} \left(-\frac{\lambda_i}{\lambda}\right) = 1$$

and

$$\sum_{i=1}^{r} \frac{\lambda_i}{\lambda} a_i = \sum_{i=r+1}^{k} \left(-\frac{\lambda_i}{\lambda}\right) a_i \in \operatorname{conv}(A_1) \cap \operatorname{conv}(A_2).$$

Thus, $A = A_1 \cup A_2$ is a Radon partition of A.

We shall prove that this partition is unique if and only if $|A| = k = d+2$ and any $d+1$ points of A are affinely independent. Let $k \ge d+3$, and let A' be a subset of A of cardinality $d+2$. Then $B = A \setminus A' \ne \emptyset$. Because $|A'| = d+2$, the set A' has a Radon partition $A' = A'_1 \cup A'_2$. It follows that

$$\operatorname{conv}\left(A'_1 \cup B\}\right) \cap \operatorname{conv}(A'_2) \supseteq \operatorname{conv}(A'_1) \cap \operatorname{conv}(A'_2) \ne \emptyset$$

and

$$\operatorname{conv}(A'_1) \cap \left(A'_2 \cup B\}\right) \supseteq \operatorname{conv}(A'_1) \cap \operatorname{conv}(A'_2) \ne \emptyset$$

and so

$$A = \left(A'_1 \cup B\right) \cup A'_2 = A'_1 \cup \left(A'_2 \cup B\right)$$

are two different Radon partitions of A.

Suppose that $|A| = d+2$. If $A' = \{a_1, \ldots, a_{d+1}\}$ is an affinely dependent subset of A, then A' is contained in an affine space of dimension $d-1$. Because

$$d+1 = (d-1)+2$$

the set A' has a Radon partition $A' = A'_1 \cup A'_2$. Then

$$\operatorname{conv}\left(A'_1 \cup \{a_{d+2}\}\right) \cap \operatorname{conv}(A'_2) \supseteq \operatorname{conv}(A'_1) \cap \operatorname{conv}(A'_2) \ne \emptyset$$

and

$$\operatorname{conv}(A'_1) \cap \operatorname{conv}\left(A'_2 \cup \{a_{d+2}\}\right) \supseteq \operatorname{conv}(A'_1) \cap \operatorname{conv}(A'_2) \ne \emptyset.$$

It follows that the partitions $A = (A'_1 \cup \{a_{d+2}\}) \cup A'_2$ and $A = A'_1 \cup (A'_2 \cup \{a_{d+2}\})$ are two different Radon partitions of A.

Suppose that $|A| = k = d+2$ and every subset of A of cardinality $d+1$ is affinely independent. Let $A = A_1 \cup A_2 = B_1 \cup B_2$ be two Radon partitions of A. There exists partitions $\{1,2,\ldots,k\} = I_1 \cup I_2 = J_1 \cup J_2$ such that

$$A_1 = \{a_i : i \in I_1\}, \quad A_2 = \{a_i : i \in I_2\}, \quad \operatorname{conv}(A_1) \cap \operatorname{conv}(A_2) \neq \emptyset$$

and

$$B_1 = \{a_j : j \in J_1\}, \quad B_2 = \{b_j : j \in J_2\}, \quad \operatorname{conv}(B_1) \cap \operatorname{conv}(B_2) \neq \emptyset.$$

Thus, there exist nonnegative real numbers $\lambda_1, \ldots, \lambda_k$, $\mu_1, \ldots, \mu_k$ with

$$\sum_{i\in I_1} \lambda_i = \sum_{i\in I_2} \lambda_i = \sum_{j\in J_1} \mu_j = \sum_{j\in J_2} \mu_j = 1$$

such that

$$\sum_{i\in I_1} \lambda_i a_i = \sum_{i\in I_2} \lambda_i a_i \tag{1.41}$$

and

$$\sum_{j\in J_1} \mu_j a_j = \sum_{j\in J_2} \mu_j a_j. \tag{1.42}$$

If $\lambda_r = 0$ for some $r \in I_1 \cup I_2$, then

$$\sum_{i\in I_1\setminus\{r\}} \lambda_i a_i - \sum_{i\in I_2\setminus\{r\}} \lambda_i a_i = 0$$

is a nontrivial affine dependence relation on the set $A \setminus \{a_r\}$, which contradicts the assumption that every subset of A of cardinality $k-1 = d+1$ is affinely independent. Therefore, $\lambda_i > 0$ for all $i \in I_1 \cup I_2$. Similarly, $\mu_j > 0$ for all $j \in J_1 \cup J_2$.

Without loss of generality we can assume that $k \in I_2 \cap J_2$. Let $I'_2 = I_2 \setminus \{k\}$ and $J'_2 = J_2 \setminus \{k\}$. We shall prove that $I_1 = J_1$ and $I'_2 = J'_2$. Rewriting equations (1.41) and (1.42), we obtain

$$\lambda_k a_k = \sum_{i\in I_1} \lambda_i a_i - \sum_{i\in I'_2} \lambda_i a_i$$
$$\mu_k a_k = \sum_{j\in J_1} \mu_j a_j - \sum_{j\in J'_2} \mu_j a_j$$

and so

$$\mu_k \left(\sum_{i\in I_1} \lambda_i a_i - \sum_{i\in I'_2} \lambda_i a_i \right) = \lambda_k \left(\sum_{j\in J_1} \mu_j a_j - \sum_{j\in J'_2} \mu_j a_j \right).$$

Equivalently,

$$\sum_{i=1}^{k-1} \nu_i a_i = \sum_{i\in I_1} \mu_k\lambda_i a_i - \sum_{i\in I_2'} \mu_k\lambda_i a_i - \sum_{j\in J_1} \lambda_k\mu_j a_j + \sum_{j\in J_2'} \lambda_k\mu_j a_j = 0 \qquad (1.43)$$

where

$$\nu_i = \begin{cases} \mu_k\lambda_i - \lambda_k\mu_i & \text{if } i \in I_1 \cap J_1 \\ \mu_k\lambda_i + \lambda_k\mu_i & \text{if } i \in I_1 \cap J_2' \\ -\mu_k\lambda_i + \lambda_k\mu_i & \text{if } i \in I_2' \cap J_2' \\ -\mu_k\lambda_i - \lambda_k\mu_i & \text{if } i \in I_2' \cap J_1. \end{cases}$$

Equation (1.43) is an affine dependence relation because

$$\begin{aligned} \sum_{i=1}^{k-1} \nu_i &= \sum_{i\in I_1} \mu_k\lambda_i - \sum_{i\in I_2'} \mu_k\lambda_i - \sum_{j\in J_1} \lambda_k\mu_j + \sum_{j\in J_2'} \lambda_k\mu_j \\ &= \mu_k - \mu_k(1-\lambda_k) - \lambda_k + \lambda_k(1-\mu_k) \\ &= 0. \end{aligned}$$

However, the set $A \setminus \{a_k\} = \{a_i : i = 1,\ldots,k-1\}$ is affinely independent, and so $\nu_i = 0$ for all $i = 1,\ldots,k-1$. Because $\lambda_i > 0$ and $\mu_i > 0$ for all $i = 1,\ldots,k$, it follows that $\mu_k\lambda_i + \lambda_k\mu_i > 0$ and $-\mu_k\lambda_i - \lambda_k\mu_i < 0$ for all $i = 1,\ldots,k$, and so $I_1 \cap J_2' = I_2' \cap J_1 = \emptyset$. Equivalently, $I_1 = J_1$ and $I_2' = J_2'$. Thus, $A_1 = B_1$ and $A_2 = B_2$, and so the set A has a unique Radon partition. This completes the proof.

Theorem 1.28 (Tverberg). *Let $r \geq 2$ and let X be a finite subset of $\mathbf{R}^n$. If $|X| \geq (r-1)n + r$, then there is a partition of X into pairwise disjoint subsets $X_1, X_2, \ldots, X_r$ such that $\bigcap_{i=1}^r \mathrm{conv}(X_i)$ is nonempty.*

Theorem 1.29 (Carathéodory). *Let A be subset of an n-dimensional real vector space.*

(a) The convex hull of A is the union of the convex hulls of all subsets of A of cardinality at most $n+1$.
(b) The positive hull of A is the union of the positive hulls of all subsets of A of cardinality at most n.

Proof. Let $K = \mathrm{conv}(A)$ and let $x \in K$. We must prove that x is a convex combination of at most $n+1$ elements of A. Let k be the smallest positive integer such that x is the convex combination of k elements of A. There exist elements $x_1,\ldots,x_k \in V$ and nonnegative real numbers $t_1,\ldots,t_k$ such that $\sum_{i=1}^k t_i = 1$ and $\sum_{i=1}^k t_i x_i = x$. Moreover, the minimality of k implies that $t_i > 0$ for all i. Suppose that $k \geq n+2$. By Exercise **??**, there exist real numbers $s_1,\ldots,s_k$, not all 0, such that $\sum_{i=1}^k s_i = 0$ and $\sum_{i=1}^k s_i x_i = 0$. Choose $j \in \{1,\ldots,k\}$ such that $s_j \neq 0$ and

$$\frac{t_i}{s_i} \geq \frac{t_j}{s_j}$$

for all $i \in \{1,\ldots,k\}$ such that $s_i \neq 0$. Then

$$x_j = -\sum_{\substack{i=1 \\ i \neq j}}^{k} \frac{s_i}{s_j} x_i$$

and

$$x = \sum_{i=1}^{k} t_i x_i = \sum_{\substack{i=1 \\ i \neq j}}^{k} t_i x_i - \sum_{\substack{i=1 \\ i \neq j}}^{k} \frac{s_i t_j}{s_j} x_i = \sum_{\substack{i=1 \\ i \neq j}}^{k} \left(t_i - \frac{s_i t_j}{s_j} \right) x_i.$$

If $s_i = 0$, then $t_i - (s_i t_j / s_j) = t_i \geq 0$. If $s_i > 0$, then

$$t_i - \frac{s_i t_j}{s_j} = s_i \left(\frac{t_i}{s_i} - \frac{t_j}{s_j} \right) \geq 0.$$

Also,

$$\sum_{\substack{i=1 \\ i \neq j}}^{k} \left(t_i - \frac{s_i t_j}{s_j} \right) = (1 - t_j) + t_j = 1$$

and so x is a convex combination of $k-1$ elements of A, which contradicts the minimality of k. Therefore, $k \leq n+1$.

Exercises

1. Prove that every affine subspace of a real vector space is convex.
2. Prove that every cone in a real vector space is convex.
3. Prove that the union of convex sets is not necessarily convex.
4. Prove that every hyperplane is the intersection of half spaces.
5. Let A be a subset of a real vector space. Prove that $\operatorname{conv}(\operatorname{conv}(A)) = \operatorname{conv}(A)$.
6. For every nonnegative integer j, let $A_j = \{2^j n : n \in \mathbf{Z} \setminus \{0\}\}$.

   a. Prove that $\operatorname{conv}(A_j) = \mathbf{R}$ for all $j \in \mathbf{N}_0$.
   b. Prove that $A_j \supseteq A_{j+1}$ for all $j \in \mathbf{N}_0$. and $\bigcap_{j=0}^{\infty} A_j = \emptyset$.

7. a. Prove that the function $y = f(x)$ is concave up if and only if the set $\{(x,y) \in \mathbf{R}^2 : y \geq f(x)\}$ is convex.
   b. Prove that the function $y = f(x)$ is concave down if and only if the set $\{(x,y) \in \mathbf{R}^2 : y \leq f(x)\}$ is convex.
8. This exercise proves the *Gauss-Lucas theorem*: The convex hull of the zeros of a complex polynomial contains the zeros of the derivative of the polynomial. Equivalently, let $p(z)$ be a nonzero polynomial with complex coefficients, and let $A = \{a_1, \ldots, a_k\}$ be the set of roots of $p(z)$. If $w \in \mathbf{C}$ and $p'(w) = 0$, then $w \in \operatorname{conv}(A)$.

   a. Prove the Gauss-Lucas theorem for polynomials of degrees 1 and 2.
   b. Prove that if $w \in \mathbf{C}$ and $p'(w) = p(w) = 0$, then $w \in \operatorname{conv}(A)$.

c. Let $p(z) = \alpha \prod_{i=1}^{k}(z - a_i)^{m_i}$, where $m_1, \ldots, m_k \in \mathbf{N}$. Prove that if $p'(w) = 0$ and $p(w) \neq 0$, then

$$\frac{p'(w)}{p(w)} = \sum_{i=1}^{k} \frac{m_i}{w - a_i} = 0$$

and so

$$\sum_{i=1}^{k} \frac{m_i w}{|w - a_i|^2} = \sum_{i=1}^{k} \frac{m_i a_i}{|w - a_i|^2}.$$

d. Let $p'(w) = 0$ and $p(w) \neq 0$. Prove that

$$\lambda_i = \frac{m_i |w - a_i|^{-2}}{\sum_{i=1}^{k} m_i |w - a_i|^{-2}} > 0$$

for $i = 1, \ldots, k$, and so

$$w = \sum_{i=1}^{k} \lambda_i a_i \in \operatorname{conv}(A).$$

Chapter 2
Matrices

2.1 Matrices and interchange of summation

Let m and n be positive integers. An $m \times n$ *matrix* is a rectangular array of scalars $a_{i,j}$ of the following form:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,j} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,j} & \cdots & a_{2,n} \\ \vdots & & & & \vdots & \\ a_{i,1} & a_{i,2} & \cdots & a_{i,j} & \cdots & a_{i,n} \\ \vdots & & & & \vdots & \\ a_{m,1} & a_{m,2} & \cdots & a_{m,j} & \cdots & a_{m,n} \end{pmatrix}. \tag{2.1}$$

The numbers $a_{i,j}$ are called the *coordinates* of the matrix. In an $m \times n$ matrix, there are n columns with m coordinates in each column, and there are m rows with n coordinates in each row. We abbreviate equation (2.1) by writing simply $A = (a_{i,j})$.

If $m = n$, then A is called a *square matrix*.

For example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

is a 2×3 rectangular matrix, and

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

is a 2×2 square matrix

Let $A = (a_{i,j})$ be an $m \times n$ matrix and let $B = (b_{i,j})$ be a $p \times q$ matrix. We have $A = B$ if and only if $m = p$, $n = q$, and $a_{i,j} = b_{i,j}$ for all $i = 1, \ldots, m$ and $j = 1, \ldots, n$.

An $m \times 1$ matrix is an m-dimensional *column vector*, and a $1 \times n$ matrix is an n-dimensional *row vector*. We usually write a row vector with its coordinates separated by commas. Thus, we write (x_1, x_2, x_3) instead of $\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}$.

Let A be the $m \times n$ matrix (2.1). For $i \in \{1, 2, \ldots, m\}$, the ith row is the n-dimensional row vector

$$\text{row}_i = (a_{i,1}, a_{i,2}, \ldots a_{i,j}, \ldots, a_{i,n})$$

and the ith *row sum* of A is the sum of the coordinates on the ith row:

$$\text{rowsum}_i(A) = \sum_{j=1}^{n} a_{i,j}.$$

For $j \in \{1, 2, \ldots, n\}$, the jth column is the m-dimensional column vector

$$\text{col}_j = \begin{pmatrix} a_{1,j} \\ a_{2,j} \\ \vdots \\ a_{1,j} \end{pmatrix}$$

and the jth *column sum* of A is the sum of the coordinates on the jth column:

$$\text{colsum}_j(A) = \sum_{i=1}^{m} a_{i,j}.$$

For the matrix $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, we have rows and row sums

$$\text{row}_1(A) = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \quad \text{and} \quad \text{row}_2(A) = \begin{pmatrix} 4 & 5 & 6 \end{pmatrix}$$

and

$$\text{rowsum}_1(A) = 6 \quad \text{and} \quad \text{rowsum}_2(A) = 15$$

and columns and column sums

$$\text{col}_1(A) = \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \quad \text{col}_2(A) = \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \quad \text{and} \quad \text{col}_3(A) = \begin{pmatrix} 3 \\ 6 \end{pmatrix}$$

and

$$\text{colsum}_1(A) = 5, \quad \text{colsum}_2(A) = 7, \quad \text{and} \quad \text{colsum}_3(A) = 9.$$

Note that

$$\text{rowsum}_1(A) + \text{rowsum}_2(A) = 21 = \text{colsum}_1(A) + \text{colsum}_2(A) + \text{colsum}_3(A).$$

Theorem 2.1 (Interchange of summation). *Let m and n be positive integers. For every set of scalars $\{a_{i,j} : i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}\}$,*

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{i,j} = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{i,j}.$$

Proof. Consider the $m \times n$ matrix $A = (a_{i,j})$. We can obtain the sum of the mn coordinates of A either by adding the m row sums or by adding the n column sums. Thus,

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{i,j} = \sum_{i=1}^{m} \text{rowsum}_i(A) = \sum_{j=1}^{n} \text{colsum}_j(A) = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{i,j}.$$

This completes the proof.

Exercises

1. Compute the row and column sums of the following matrices:

   a.
   $$\begin{pmatrix} 1. & 2 \\ 3 & 4 \end{pmatrix}$$

   b.
   $$\begin{pmatrix} 2 & -7 & 3 & 0 \\ 11 & -10 & 0 & 1 \\ -8 & 4 & -1 & -2 \end{pmatrix}$$

   c.
   $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

   d.
   $$\begin{pmatrix} 1/5 & 1/5 & 15 & 1/5 & 1/5 \\ 1/5 & 1/5 & 15 & 1/5 & 1/5 \\ 1/5 & 1/5 & 15 & 1/5 & 1/5 \\ 1/5 & 1/5 & 15 & 1/5 & 1/5 \\ 1/5 & 1/5 & 15 & 1/5 & 1/5 \\ 1/5 & 1/5 & 15 & 1/5 & 1/5 \end{pmatrix}.$$

2. The $m \times n$ matrix A is *row stochastic* if all of its row sums are equal to 1, that is $\text{rowsum}_i(A) = 1$ for all $i = 1, \ldots, m$.
   The $m \times n$ matrix A is *column stochastic* if all of its column sums are equal to 1, that is $\text{colsum}_j(A) = 1$ for all $j = 1, \ldots, n$.
   The $m \times n$ matrix A is *doubly stochastic* if it is both row stochastic and column stochastic.
   Prove that if an $m \times n$ matrix is doubly stochastic, then $m = n$.

2.2 Matrix algebra

2.2.1 Matrix addition and scalar multiplication

Consider the $m \times n$ matrix

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,j} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,j} & \cdots & a_{2,n} \\ \vdots & & & \vdots & & \\ a_{i,1} & a_{i,2} & \cdots & a_{i,j} & \cdots & a_{i,n} \\ \vdots & & & \vdots & & \\ a_{m,1} & a_{m,2} & \cdots & a_{m,j} & \cdots & a_{m,n} \end{pmatrix}.$$

We may also write

$$A = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$$

where $\mathbf{v}_j = \mathrm{col}_j(A) \in \mathbf{R}^m$ for $j = 1, \ldots, n$.

The jth column of A is a *zero column* if $\mathrm{col}_j(A) = \mathbf{0}$, that is, if $a_{i,j} = 0$ for all $i = 1, \ldots, m$. The ith row of A is a *zero row* if every coordinate in the row is 0, that is, if $a_{i,j} = 0$ for all $j = 1, \ldots, n$. The $m \times n$ *zero matrix* is the matrix $Z_{m,n} = (z_{i,j})$ such that $z_{i,j} = 0$ for all $i = 1, \ldots, m$ and $j = 1, \ldots, n$. We denote the square $n \times n$ zero matrix by Z_n. In the zero matrix, every row is a zero row and every column is a zero column. For example,

$$Z_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \text{and} \qquad Z_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

We define the sum of $m \times n$ matrices by pairwise addition of coordinates: If

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ a_{2,1} & \cdots & a_{2,n} \\ \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,n} \\ b_{2,1} & \cdots & b_{2,n} \\ \vdots & & \vdots \\ b_{m,1} & \cdots & b_{m,n} \end{pmatrix}$$

then

$$A + B = \begin{pmatrix} a_{1,1} + b_{1,1} & \cdots & a_{1,n} + b_{1,n} \\ a_{2,1} + b_{2,1} & \cdots & a_{2,n} + b_{2,n} \\ \vdots & & \vdots \\ a_{m,1} + b_{m,1} & \cdots & a_{m,n} + b_{m,n} \end{pmatrix}. \tag{2.2}$$

Note that we can add matrices if and only if they have the same number of rows and the same number of columns. Thus, if A is an $m \times n$ matrix and B is an $p \times q$ matrix, then $A + B$ is defined if and only if $m = p$ and $n = q$.

We define *scalar multiplication* of an $m \times n$ matrix $A = (a_{i,j})$ by a scalar c by multiplying each coordinate of the matrix by the scalar: If $A = (a_{i,j})$ is an $m \times n$ matrix and c is a scalar, then

$$cA = c\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ a_{2,1} & \cdots & a_{2,n} \\ \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} = \begin{pmatrix} ca_{1,1} & \cdots & ca_{1,n} \\ ca_{2,1} & \cdots & ca_{2,n} \\ \vdots & & \vdots \\ ca_{m,1} & \cdots & ca_{m,n} \end{pmatrix} \tag{2.3}$$

Note that

$$1 \cdot A = A$$

and that multiplying a matrix by the scalar 0 always yields the zero matrix.

For $m \times n$ matrices A and B, we define

$$-B = (-1)B$$

and

$$A - B = A + (-1)B.$$

For example, if

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 3 & -1 & 0 \\ -5 & -7 & 8 \end{pmatrix}$$

then

$$A + B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} + \begin{pmatrix} 3 & -1 & 0 \\ -5 & -7 & 8 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 3 \\ -1 & -2 & 14 \end{pmatrix}$$

$$A - B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} - \begin{pmatrix} 3 & -1 & 0 \\ -5 & -7 & 8 \end{pmatrix} = \begin{pmatrix} -2 & 3 & 3 \\ 9 & 12 & -2 \end{pmatrix}$$

and

$$7A = 7\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 7 & 14 & 21 \\ 28 & 35 & 42 \end{pmatrix}.$$

Let $\mathrm{Mat}_{m,n}(\mathbf{R})$ be the set of $m \times n$ matrices with real coordinates.

Theorem 2.2. *Let $A, B, C \in Mat_{m,n}(\mathbf{R})$ and let $Z_{m,n} \in Mat_{m,n}(\mathbf{R})$ be the $m \times n$ zero matrix. Matrix addition satisfies the following properties:*

(i) Associativity:

$$(A + B) + C = A + (B + C).$$

(ii) Commutativity:

$$A + B = B + A.$$

(iii) Existence of an additive identity:

$$A + Z_{m,n} = A.$$

(iii) Existence of an additive inverse:

$$A+(-A)=Z_{m,n}.$$

Proof. The (i,j)th coordinate of $A+B$ is $(A+B)_{i,j}=a_{i,j}+b_{i,j}$ and the (i,j)th coordinate of C is $C_{i,j}=c_{i,j}$. Therefore, the (i,j)th coordinate of $(A+B)+C$ is

$$((A+B)+C)_{i,j}=(A+B)_{i,j}+C_{i,j}=(a_{i,j}+b_{i,j})+c_{i,j}.$$

Similarly, the (i,j)th coordinate of $A+(B+C)$ is

$$(A+(B+C))_{i,j}=A_{i,j}+(B+C)_{i,j}=a_{i,j}+(b_{i,j}+c_{i,j}).$$

Because addition of numbers in a field is associative,

$$(a_{i,j}+b_{i,j})+c_{i,j}=a_{i,j}+(b_{i,j}+c_{i,j})$$

and so $((A+B)+C)_{i,j}=(A+(B+C))_{i,j}$ for all $i=1,\ldots,m$ and $j=1,\ldots,n$. Therefore, $(A+B)+C=A+(B+C)$ and matrix addition is associative.

Because addition of numbers in a field is commutative, we have

$$(A+B)_{i,j}=a_{i,j}+b_{i,j}=b_{i,j}+a_{i,j}=(B+A)_{i,j}$$

and so

$$A+B=B+A.$$

Because $Z_{m,n}$ is the zero matrix,

$$(A+Z_{m,n})_{i,j}=a_{i,j}+z_{i,j}=a_{i,j}+0=a_{i,j}$$

and so $A+Z_{m,n}=A$. Similarly,

$$(A+(-A))_{i,j}=A_{i,j}+(-A)_{i,j}=a_{i,j}+(-a_{i,j})=a_{i,j}-a_{i,j}=0$$

and so $A+(-A)=Z_{m,n}$. This completes the proof.

Theorem 2.3. *Let $A,B\in Mat_{m,n}(\mathbf{R})$ and let c and c' be scalars. Scalar multiplication of matrices satisfies the following:*

(i) Associativity:

$$(cc')A=c(c'A)$$

(ii) Distributivity:

$$c(A+B)=cA+cB$$

and

$$(c+c')A=cA+c'A.$$

Proof. Exercise 8.

Let $\delta_{i,j}$ be the Kronecker delta. Define the matrix $E^{(i,j)}=\left(e_{p,q}^{(i,j)}\right)$, where

$$e_{p,q}^{(i,j)} = \delta_{i,p}\delta_{j,q} = \begin{cases} 1 & \text{if } (p,q) = (i,j) \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 2.4. *The set* $\mathrm{Mat}_{m,n}(\mathbf{R})$ *of* $m \times n$ *matrices is a vector space of dimension* mn *with addition defined by* (2.2) *and scalar multiplication defined by* (2.3). *A basis for the vector space* $\mathrm{Mat}_{m,n}(\mathbf{R})$ *is the set of matrices*

$$\mathscr{B} = \left\{ E^{(i,j)} : i \in \{1,\ldots,m\} \text{ and } j \in \{1,\ldots,n\} \right\}.$$

Proof. Theorems 2.2 and 2.3 imply that $\mathrm{Mat}_{m,n}(\mathbf{R})$ is a vector space. Every matrix $A = (a_{i,j}) \in \mathrm{Mat}_{m,n}(\mathbf{R})$ has a unique representation in the form

$$A = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} E^{(i,j)}$$

and so $\mathscr{B}$ is a basis for $\mathrm{Mat}_{m,n}(\mathbf{R})$. This completes the proof.

If A_1 and A_2 are $m \times n$ matrices and c_1 and c_2 are numbers, then the scalar multiples c_1A_1 and c_2A_2 are also $m \times n$ matrices, and so $c_1A_1 + c_2A_2$ is an $m \times n$ matrix. We call $c_1A_1 + c_2A_2$ a *linear combination* of A_1 and A_2. More generally, if $A_1, A_2, \ldots, A_k$ are $m \times n$ matrices and $c_1, \ldots, c_k$ are numbers, then the $m \times n$ matrix $c_1A_1 + c_2A_2 + \cdots + c_kA_k$ is a *linear combination* of the matrices $A_1, A_2, \ldots, A_k$. For example,

$$7\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} + 4\begin{pmatrix} 6 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 31 & 34 & 37 \\ 40 & 43 & 46 \end{pmatrix}.$$

2.2.2 Matrix multiplication

The $n \times n$ *identity matrix* is the square matrix $I_n = (\delta_{i,j})$, where $\delta_{i,j}$ is the *Kronecker delta*, defined by

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

For example,

$$I_1 = \begin{pmatrix} 1 \end{pmatrix}, \qquad I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Multiplication of matrices A and B is defined only if the number of columns of A equals the number of rows of B. Let A and B be $m \times n$ and $n \times p$ matrices, respectively:

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,k} & \cdots & a_{1,n} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & \cdots & a_{i,k} & \cdots & a_{i,n} \\ \vdots & & \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,k} & \cdots & a_{m,n} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,j} & \cdots & b_{1,p} \\ \vdots & & \vdots & & \vdots \\ b_{k,1} & \cdots & b_{k,j} & \cdots & b_{k,p} \\ \vdots & & \vdots & & \vdots \\ b_{n,1} & \cdots & b_{n,j} & \cdots & b_{n,p} \end{pmatrix}.$$

The matrix product $AB = C = (c_{i,j})$ is the $m \times p$ matrix whose (i, j)th coordinate is defined by

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}$$

for $i = 1, \ldots, m$ and $j = 1, \ldots, p$. Thus, the (i, j)th coordinate of the product matrix AB is the "product" of the ith row of A and the jth column of B:

$$c_{i,j} = \mathrm{row}_i(A) \cdot \mathrm{col}_j(B) = (a_{i,1} \ \cdots \ a_{i,k} \ \cdots \ a_{i,n}) \begin{pmatrix} b_{1,j} \\ \vdots \\ b_{2,k} \\ \vdots \\ b_{n,j} \end{pmatrix}$$

The rule for the shape of a product of matrices is

$$\boxed{(m \times n)(n \times p) = m \times p}$$

For example, if A is the 2×4 matrix

$$A = \begin{pmatrix} 2 & -3 & 1 & 0 \\ 5 & 0 & -4 & 1 \end{pmatrix}$$

and B is the 4×3 matrix

$$B = \begin{pmatrix} 1 & 2 & 4 \\ 0 & -2 & 7 \\ 3 & 1 & 0 \\ -1 & 5 & 3 \end{pmatrix}$$

then

$$\boxed{(2 \times 4)(4 \times 3) = 2 \times 3}$$

and the product matrix AB is the 2×3 matrix

$$AB = \begin{pmatrix} 2 & -3 & 1 & 0 \\ 5 & 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 4 \\ 0 & -2 & 7 \\ 3 & 1 & 0 \\ -1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 11 & -13 \\ -8 & 11 & 23 \end{pmatrix}.$$

Note that the product BA is undefined because B has 3 columns and A has 2 rows.

Matrix addition is commutative but matrix multiplication is not necessarily commutative. For example, let

$$A = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 5 & 0 \\ 0 & 7 \end{pmatrix}.$$

We have

$$A + B = B + A = \begin{pmatrix} 5 & 2 \\ 3 & 7 \end{pmatrix}$$

but

$$AB = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 7 \end{pmatrix} = \begin{pmatrix} 0 & 14 \\ 15 & 0 \end{pmatrix}$$

$$BA = \begin{pmatrix} 5 & 0 \\ 0 & 7 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 10 \\ 21 & 0 \end{pmatrix}$$

and

$$AB \neq BA.$$

Similarly, if

$$A = \begin{pmatrix} 5 & 4 \\ 4 & 3 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 11 & -3 \\ -7 & -2 \end{pmatrix}$$

then

$$A + B = B + A = \begin{pmatrix} 16 & 1 \\ -3 & 1 \end{pmatrix}$$

but

$$AB = \begin{pmatrix} 27 & -23 \\ 23 & -18 \end{pmatrix} \neq \begin{pmatrix} 43 & 35 \\ -43 & -34 \end{pmatrix} = BA.$$

Recall that $I_n = (\delta_{i,j})$ is the $n \times n$ identity matrix.

Theorem 2.5. *Matrix multiplication satisfies the following properties:*

(i) Associativity: If A is a $m \times n$ matrix, if B is an $n \times p$ matrix, and if C is an $p \times q$ matrix, then $(AB)C$ and $A(BC)$ are $m \times q$ matrices, and

$$(AB)C = A(BC).$$

(ii) Left and right identities: If A is an $m \times n$ matrix, then

$$I_m A = A I_n = A.$$

(iii) Distributivity: If A is an $m \times n$ matrix and if B and C are $n \times p$ matrices, then

$$A(B + C) = AB + AC.$$

If A and B are $m \times n$ matrices and if C is an $n \times p$ matrices, then

$$(A + B)C = AC + BC.$$

(iv) If A is an $m \times n$ matrix and B is an $n \times p$ matrix, then, for every scalar c,

$$c(AB) = (cA)B = A(cB).$$

Proof. In this proof, we denote the (i, j)th coordinate of a matrix M by $M_{i,j}$. To prove associativity, we must show that

$$((AB)C)_{i,j} = (A(BC))_{i,j}$$

for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, q\}$.

Let $A = (a_{i,j})$, $B = (b_{i,j})$, and $C = (c_{i,j})$. Observe that AB is an $m \times p$ matrix, and so $(AB)C$ is an $m \times q$ matrix. Similarly, BC is an $n \times q$ matrix, and so $A(BC)$ is also an $m \times q$ matrix. Using only the definition of matrix multiplication, we obtain, for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, q\}$,

$$\begin{aligned}
((AB)C)_{i,j} &= \sum_{k=1}^{p} (AB)_{i,k} c_{k,j} \\
&= \sum_{k=1}^{p} \sum_{\ell=1}^{n} a_{i,\ell} b_{\ell,k} c_{k,j} \\
&= \sum_{\ell=1}^{n} \sum_{k=1}^{p} a_{i,\ell} b_{\ell,k} c_{k,j} \\
&= \sum_{\ell=1}^{n} a_{i,\ell} \sum_{k=1}^{p} b_{\ell,k} c_{k,j} \\
&= \sum_{\ell=1}^{n} a_{i,\ell} (BC)_{\ell,j} \\
&= (A(BC))_{i,j}.
\end{aligned}$$

This proves (i).

To prove (ii), it suffices to observe that

$$(I_m A)_{i,j} = \sum_{k=1}^{m} \delta_{i,k} a_{k,j} = a_{i,j}$$

and

$$(A I_n)_{i,j} = \sum_{k=1}^{n} a_{i,k} \delta_{k,j} = a_{i,j}$$

The proofs of (iii) and (iv) are Exercises 9 and 10.

For example, if

$$A = \begin{pmatrix} 5 & 4 \\ 4 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 11 & -3 \\ -7 & -2 \end{pmatrix}, \qquad \text{and} \qquad C = \begin{pmatrix} 2 & 1 \\ 0 & 5 \end{pmatrix},$$

then

$$(AB)C = \begin{pmatrix} 27 & -23 \\ 23 & -18 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 54 & -88 \\ 46 & -67 \end{pmatrix}$$

and

$$A(BC) = \begin{pmatrix} 5 & 4 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 22 & -4 \\ -14 & -17 \end{pmatrix} = \begin{pmatrix} 54 & -88 \\ 46 & -67 \end{pmatrix}.$$

For every positive integer n, let $\mathrm{Mat}_n(\mathbf{R})$ denote the set of $n \times n$ matrices with coefficients in the field $\mathbf{R}$.

Theorem 2.6. *Let $n \geq 2$. With the binary operations of matrix addition and matrix multiplication, $Mat_n(\mathbf{R})$ is a noncommutative ring.*

Proof. Recall the definition of a ring in Section 1.8. The set $\mathrm{Mat}_n(\mathbf{R})$ is closed under both matrix addition and matrix multiplication. By Theorem 2.2, the set $\mathrm{Mat}_n(\mathbf{R})$ is an additive abelian group.

Because the product of $n \times n$ matrices is an $n \times n$ matrix, it follows that the set $\mathrm{Mat}_n(\mathbf{R})$ is closed under matrix multiplication. It follows from Theorem 2.5 that $\mathrm{Mat}_n(\mathbf{R})$ is a ring. We have already observed that matrix multiplication is not commutative. This completes the proof.

Let A be an $n \times n$ matrix. For every positive integer k, we define the kth power of A, denoted A^k, as the product of k copies of A. Thus,

$$\begin{aligned} A^1 &= A \\ A^2 &= A \cdot A \\ A^3 &= A \cdot A \cdot A \end{aligned}$$

and, in general,

$$A^k = \underbrace{A \cdots A}_{k \text{ factors}}.$$

We define

$$A^0 = I_n.$$

Because matrix multiplication is associative, we have

$$A^{k+\ell} = A^k A^\ell$$

for all nonnegative integers k and ℓ. For example, if

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \tag{2.4}$$

then

$$A^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}, \qquad A^3 = \begin{pmatrix} 37 & 54 \\ 81 & 118 \end{pmatrix}, \qquad A^4 = \begin{pmatrix} 199 & 290 \\ 435 & 634 \end{pmatrix}.$$

Note that $A^4 = A \cdot A^3 = A^2 \cdot A^2$.

For every polynomial

$$p(x) = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_1 x + c_0$$

and every $n \times n$ matrix A, we define the *matrix polynomial*

$$p(A) = c_k A^k + c_{k-1} A^{k-1} + \cdots + c_1 A + c_0 I_n.$$

For example, if A is the 2×2 matrix A defined by (2.4), and if

$$p(x) = x^3 - 2x^2 + 5x + 4$$

then

$$\begin{aligned} p(A) &= A^3 - 2A^2 + 5A + 4I_2 \\ &= \begin{pmatrix} 37 & 54 \\ 81 & 118 \end{pmatrix} - 2\begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix} + 5\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + 4\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 28 & 44 \\ 66 & 94 \end{pmatrix}. \end{aligned}$$

2.2.3 The transpose of a matrix

The *transpose* of the $m \times n$ matrix $A = (a_{i,j})$ is the $n \times m$ matrix $A^t = (a^t_{i,j})$ defined by

$$a^t_{i,j} = a_{j,i}.$$

For example, if $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, then $A^t = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$.

An n-dimensional column vector is an $n \times 1$ matrix. An n-dimensional row vector is an $1 \times n$ matrix. The transpose of an n-dimensional column vector is an n-dimensional row vector. The transpose of an n-dimensional row vector is an n-dimensional column vector. For example, the transpose of the column vector $\mathbf{v} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ is the row vector $\mathbf{v}^t = (1,2,3)$. The transpose of the row vector $\mathbf{w} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ is the row vector $\mathbf{w}^t = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$.

The transpose of the $m \times n$ matrix A is the $n \times m$ matrix A^t obtained by interchanging the rows and columns of A. Thus, for $j = 1, \ldots, m$, the jth row of A^t is $\mathrm{row}_j(A^t) = \mathrm{col}_j(A)$, and, for $i = 1, \ldots, n$, the ith column of A^t is $\mathrm{col}_i(A^t) = \mathrm{row}_i(A)$.

Theorem 2.7. *If $A, B \in Mat_{m,n}(\mathbf{R})$, then*

$$(A+B)^t = A^t + B^t.$$

If $A \in Mat_{m,p}(\mathbf{R})$ and $B \in Mat_{p,n}(\mathbf{R})$, then $B^tA^t \in Mat_{n,m}(\mathbf{R})$ and

$$(AB)^t = B^tA^t.$$

If $A \in Mat_n(\mathbf{R})$ is invertible, then A^t is invertible and

$$\left(A^t\right)^{-1} = \left(A^{-1}\right)^t.$$

Proof. Let $A = (a_{i,j}) \in \mathrm{Mat}_{m,n}(\mathbf{R})$ and $B = (b_{i,j}) \in \mathrm{Mat}_{m,n}(\mathbf{R})$. Let $A+B = C = (c_{i,j})$, then $c_{i,j} = a_{i,j} + b_{i,j}$ and

$$(A+B)^t = C^t = (c^t_{i,j}) = (c_{j,i}) \in \mathrm{Mat}_{n,m}(\mathbf{R}).$$

We have

$$c_{j,i} = a_{j,i} + b_{j,i} = a^t_{i,j} + b^t_{i,j}$$

and so

$$(A+B)^t = \left(a^t_{i,j} + b^t_{i,j}\right) = \left(a^t_{i,j}\right) + \left(b^t_{i,j}\right) = A^t + B^t.$$

Let $A = (a_{i,j}) \in \mathrm{Mat}_{m,p}(\mathbf{R})$ and $B = (b_{j,j}) \in \mathrm{Mat}_{p,n}(\mathbf{R})$. Let $C = AB = (c_{i,j}) \in \mathrm{Mat}_{m,n}(\mathbf{R})$. We have

$$(AB)_{i,j} = c_{i,j} = \sum_{k=1}^{p} a_{i,k}b_{k,j}$$

and

$$(AB)^t_{i,j} = c_{j,i} = \sum_{k=1}^{p} a_{j,k}b_{k,i} = \sum_{k=1}^{p} b^t_{i,k}a^t_{k,j} = \left(B^tA^t\right)_{i,j}.$$

This proves that $(AB)^t = BA$.

If A is invertible, then there exists a matrix A^{-1} such that $AA^{-1} = A^{-1}A = I_n$. Therefore,

$$I_n = I^t_n = \left(AA^{-1}\right)^t = \left(A^{-1}\right)^t A^t$$

and

$$I_n = I^t_n = \left(A^{-1}A\right)^t = A^t \left(A^{-1}\right)^t$$

It follows that A^t is invertible and $(A^t)^{-1} = \left(A^{-1}\right)^t$. This completes the proof.

An $n \times n$ matrix A is *symmetric* if $A^t = A$ and *skew-symmetric* if $A^t = -A$. For example, the matrix

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix}$$

are symmetric, and the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & 1 & 2 \\ -1 & 0 & 3 \\ -2 & -3 & 0 \end{pmatrix}.$$

are skewsymmetric.

Theorem 2.8. *Let A be an $n \times n$ matrix. The matrix*

$$\frac{1}{2}\left(A + A^t\right)$$

is symmetric, the matrix

$$\frac{1}{2}\left(A - A^t\right)$$

is skew-symmetric, and

$$A = \frac{1}{2}\left(A + A^t\right) + \frac{1}{2}\left(A - A^t\right).$$

If B is a symmetric matrix and C is a skew-symmetric matrix such that $A = B + C$, then

$$B = \frac{1}{2}\left(A + A^t\right) \qquad \textit{and} \qquad C = \frac{1}{2}\left(A - A^t\right).$$

Proof. Exercises 15, 16, and 17.

Exercises

1. Consider the matrices

$$A = \begin{pmatrix} 7 & 1 \\ 0 & -2 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 8 & -3 \\ -1 & 4 \end{pmatrix}.$$

   Compute the following 2×2 matrices:

$$5A, \quad A + B, \quad 5A - 6B, \quad AB, \quad BA, \quad AB - BA.$$

2. Consider the matrices

$$C = \begin{pmatrix} 9 & -1 & 4 \\ 3 & 0 & 2 \end{pmatrix} \qquad \text{and} \qquad D = \begin{pmatrix} 1 & -13 \\ -2 & 5 \\ 0 & 8 \end{pmatrix}.$$

   Compute CD and DC.
3. Let

$$A = \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}.$$

   a. Compute A^k for $k = 2, 3, 4, 5, 6$.
   b. Let $p(x) = 2x^2 - x + 5$. Compute the matrix polynomial $p(A)$.
4. Consider the matrices

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

Prove that

$$P_{1,2}^2 = P_{1,3}^2 = P_{2,3}^2 = I_3$$

and that

$$P_{1,2}P_{1,3} \neq P_{1,3}P_{1,2}.$$

5. This exercise shows that the product of two nonzero matrices may be the zero matrix.

   a. Let $F_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $F_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Compute F_1F_2 and F_2F_1.
   b. Let $F_3 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ and $F_4 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$. Compute F_1F_2 and F_2F_1.

6. a. Consider the 3×3 matrices

$$G = \begin{pmatrix} 4 & 9 & 0 \\ -1 & -2 & 0 \\ 0 & 0 & -3 \end{pmatrix} \qquad H = \begin{pmatrix} 6 & 5 & 0 \\ 5 & 4 & 0 \\ 0 & 0 & 7 \end{pmatrix}$$

   Compute GH.
   b. Consider the 2×2 matrices

$$G' = \begin{pmatrix} 4 & 9 \\ -1 & -2 \end{pmatrix} \qquad H' = \begin{pmatrix} 6 & 5 \\ 5 & 4 \end{pmatrix}$$

   Compute $G'H'$.
   c. What do you observe when you compare GH and $G'H'$.

7. Let I_n denote the $n \times n$ identity matrix. Prove that if A is an $m \times n$ matrix, then $AI_n = I_mA = A$.
8. Prove Theorem 2.3.
9. Prove that if A is an $m \times n$ matrix and if B and C are $n \times p$ matrices, then

$$A(B+C) = AB + AC.$$

   Prove that if A and B are $m \times n$ matrices and if C is an $n \times p$ matrices, then

$$(A+B)C = AC + BC.$$

10. Prove that if A is an $m \times n$ matrix and B is an $n \times p$ matrix, then, for every scalar c,

$$c(AB) = (cA)B = A(cB).$$

11. Define $f_0 = 0, f_1 = f_2 = 1$ and, for every $k \geq 2$, define

$$f_{k+1} = f_{k-1} + f_k.$$

The sequence of positive integers $(f_k)_{k=1}^{\infty}$ is called the *Fibonacci sequence*.

a. Compute the first 11 terms of the Fibonacci sequence $f_0, f_1, \ldots, f_{10}$
b. Prove that
$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} f_{k-1} \\ f_k \end{pmatrix} = \begin{pmatrix} f_k \\ f_{k+1} \end{pmatrix}$$
for all $k \geq 2$.
c. Let $F = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Compute F^k for $k \in \{1, \ldots, 9\}$.
d. Prove that
$$F^n = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix}$$
for all $n \geq 1$.

12. Let
$$A = \begin{pmatrix} 2 & -3 & 7 \\ 0 & 9 & -1 \end{pmatrix}.$$
Compute the following matrices:
$$A^t, \quad AA^t, \quad \left(AA^t\right)^t, \quad A^tA \quad \left(A^tA\right)^t.$$

13. Let
$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$
Compute the matrices $A + A^t$, $A - A^t$, and
$$\frac{1}{2}(A + A^t) + \frac{1}{2}(A - A^t).$$

14. Let
$$B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$
Compute the matrices $B + B^t$, $B - B^t$, and
$$\frac{1}{2}(B + B^t) + \frac{1}{2}(B - B^t).$$

15. Let $A = (a_{i,j})$ be an $n \times n$ matrix. Prove that the matrix
$$\frac{1}{2}\left(A + A^t\right)$$
is symmetric and that the matrix
$$\frac{1}{2}\left(A - A^t\right)$$

is skew-symmetric.

16. Let $A = (a_{i,j})$ be an $n \times n$ matrix. Prove that

$$A = \frac{1}{2}\left(A + A^t\right) + \frac{1}{2}\left(A - A^t\right).$$

17. Let $A = (a_{i,j})$ be an $n \times n$ matrix. Prove that if B is a symmetric matrix and C is a skew-symmetric matrix such that $A = B + C$, then

$$B = \frac{1}{2}\left(A + A^t\right) \qquad \text{and} \qquad C = \frac{1}{2}\left(A - A^t\right).$$

Hint: $A = B + C$ implies that $A^t = B^t + C^t = B - C$.

18. Let

$$A = \begin{pmatrix} 5 & 9 \\ 7 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} -3 & 0 \\ 0 & -3 \end{pmatrix}, \quad C = \begin{pmatrix} -3 & 0 \\ 0 & 8 \end{pmatrix}, \quad D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}.$$

a. Compute AB and BA.
b. Compute AC and CA.
c. Prove that $AD = DA$ if and only if $d_1 = d_2$.

19. Let

$$A = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 5 & -9 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 5 & -9 & 2 \\ 0 & 0 & 4 & 3 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Prove that $A^2 = 0$, $B^3 = 0$, and $C^4 = 0$.

20. Let

$$A = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 5 & -9 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 5 & -9 & 2 \\ 0 & 1 & 4 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Prove that $A^n \neq 0$, $B^n \neq 0$, and $C^n \neq 0$ for every positive integer n.

21. Let $x, y, z \in \mathbf{R}$. Prove that

$$\begin{pmatrix} 0 & x & z \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

22. A square matrix A is *nilpotent* if $A^k = 0$ for some positive integer k. Prove that if A is an $n \times n$ strictly upper triangular matrix, then A is nilpotent and $A^n = 0$.

23. Let $f(t) = t^2 - 14t + 52$, and let $A = \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix}$ and $B = \begin{pmatrix} 5 & 7 \\ -1 & 9 \end{pmatrix}$. Compute the matrix polynomials $f(A)$ and $f(B)$.

24. Prove that the matrix $A = \begin{pmatrix} 8 & -6 \\ 5 & -3 \end{pmatrix}$ is a root of the polynomial $f(t) = t^2 - 5t + 6$.

25. Let $A = \begin{pmatrix} 3 & 5 \\ 2 & 3 \end{pmatrix}$. Find a number $c \in \mathbf{R}$ such that, if $f(t) = t^2 - 6t + c$, then the matrix polynomial $f(A)$ is the zero matrix.
26. An $n \times n$ matrix $D = (d_{i,j})$ is diagonal if $d_{i,j} = 0$ for all $i \neq j$. Let $\mathrm{diag}(d_{1,1}, \ldots, d_{n,n})$ denote the $n \times n$ diagonal matrix whose ith diagonal coordinate is $d_{i,i}$. For example, the identity matrix is $I_n = \mathrm{diag}(1, \ldots, 1)$, and $\mathrm{diag}(1,2,3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. Prove that diagonal matrices commute, that is, if D_1 and D_2 are diagonal matrices, then $D_1 D_2 = D_2 D_1$.
27. Let $D = \mathrm{diag}(d_{i,i})$ be an $n \times n$ diagonal matrix and let $A = (a_{i,j})$ be an $n \times n$ matrix.
    a. Prove that DA is the matrix whose i row is the ith row of A multiplied by $d_{i,i}$.
    b. Prove that AD is the matrix whose j column is the jth column of A multiplied by $d_{j,j}$.

2.3 Understanding matrix multiplication

A special case of matrix multiplication is the product of a matrix and a vector. If $\mathbf{v}$ is an m-dimensional row vector, that is, a $1 \times m$ matrix, and if A is an $m \times n$ matrix, then $\mathbf{v}A$ is a $1 \times n$ matrix, that is, an n-dimensional row vector. For example, if

$$\mathbf{v} = (-7, 9) \qquad \text{and} \qquad A = \begin{pmatrix} 2 & -3 & 1 \\ 5 & 0 & -4 \end{pmatrix}$$

then

$$\mathbf{v}A = (-7, 9) \begin{pmatrix} 2 & -3 & 1 \\ 5 & 0 & -4 \end{pmatrix} = (31, 21, -43).$$

Observe that the row vector $(31, 21, -43)$ is the following linear combination of the rows of the matrix A:

$$(31, 21, -43) = -7(2, -3, 1) + 9(5, 0, -4).$$

This is a general phenomenon: The product of a row vector with a matrix is always a linear combination of the rows of the matrix. The coefficients in the linear combination are the coordinates of the row vector. Let $\mathbf{x} = (x_1, \ldots, x_m)$ be an m-dimensional row vector. Let $A = (a_{i,j})$ be an $m \times n$ matrix, and, for $i = 1, \ldots, m$, let $\mathrm{row}_i(A) = (a_{i,1}, \ldots, a_{i,n})$ be the n-dimensional row vector that is the ith row of A. If

$$\mathbf{x}A = \mathbf{y} = (y_1, \ldots, y_n)$$

then

$$y_j = \sum_{i=1}^{m} x_i a_{i,j}$$

and so

$$\begin{aligned}(y_1,\dots,y_n) &= \left(\sum_{i=1}^{m} x_i a_{i,1},\dots,\sum_{i=1}^{m} x_i a_{i,n}\right)\\ &= \sum_{i=1}^{m} (x_i a_{i,1},\dots,x_i a_{i,n})\\ &= \sum_{i=1}^{m} x_i\,(a_{i,1},\dots,a_{i,n})\\ &= \sum_{i=1}^{m} x_i\,\mathrm{row}_i(A).\end{aligned}$$

Similarly, the product of a matrix with a column vector is always a linear combination of the columns of the matrix. Let $\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}$ be an n-dimensional column vector. Let $A=(a_{i,j})$ be an $m\times n$ matrix, and, for $j=1,\dots,n$, let $\mathrm{col}_j(A)=\begin{pmatrix} a_{1,j}\\ \vdots\\ a_{m,j}\end{pmatrix}$ be the m-dimensional column vector that is the jth column of A. If $A\mathbf{x}=y=\begin{pmatrix} y_1\\ \vdots\\ y_m\end{pmatrix}$, then

$$y_i=\sum_{j=1}^{n} a_{i,j}x_j$$

for $i=1,\dots,m$, and so

$$\begin{aligned}\begin{pmatrix} y_1\\ \vdots\\ y_m\end{pmatrix} &= \begin{pmatrix} \sum_{j=1}^{n} a_{1,j}x_j\\ \vdots\\ \sum_{j=1}^{n} a_{m,j}x_j\end{pmatrix} = \sum_{j=1}^{n}\begin{pmatrix} a_{1,j}x_j\\ \vdots\\ a_{m,j}x_j\end{pmatrix}\\ &= \sum_{j=1}^{n} x_j\begin{pmatrix} a_{1,j}\\ \vdots\\ a_{m,j}\end{pmatrix} = \sum_{j=1}^{n} x_j\,\mathrm{col}_j(A).\end{aligned}$$

For example,

$$\begin{pmatrix} 2 & -3 & 1\\ 5 & 0 & -4\\ 7 & -2 & 9\end{pmatrix}\begin{pmatrix} -2\\ 7\\ 9\end{pmatrix} = \begin{pmatrix} -16\\ -46\\ 53\end{pmatrix} = -2\begin{pmatrix} 2\\ 5\\ 7\end{pmatrix} + 7\begin{pmatrix} -3\\ 0\\ -2\end{pmatrix} + 9\begin{pmatrix} 1\\ -4\\ 9\end{pmatrix}.$$

It is a fundamental computational fact in linear algebra that the product of a matrix and a column vector is a linear combination of the columns of the matrix, and that every linear combination of the columns of a matrix can be represented as the product of the matrix and a column vector. The *column space* of the $m \times n$ matrix A is the set of all linear combinations of the columns of A. This subset of $\mathbf{R}^m$ is the set

$$\{A\mathbf{x} : \mathbf{x} \in \mathbf{R}^n\}.$$

Similarly, the product of a row vector and a matrix is a linear combination of the rows of the matrix, and every linear combination of the rows of a matrix can be represented as the product of a row vector and the matrix. The *row space* of the $m \times n$ matrix A is the transpose of the set of all linear combinations of the rows of A.

Theorem 2.9. *Let A be an $m \times n$ matrix. The row space of A is the column space of A^t.*

Proof. A vector $\mathbf{y} \in \mathbf{R}^n$ is in the row space of A if and only if there exists $\mathbf{x} \in \mathbf{R}^m$ such that $\mathbf{y}^t = \mathbf{x}^t A$ if and only if there exists $\mathbf{x} \in \mathbf{R}^m$ such that

$$\mathbf{y} = \left(\mathbf{y}^t\right)^t = (\mathbf{x}^t A)^t = A^t \mathbf{x}$$

if and only if $\mathbf{y}$ is in the column space of A^t.

We also interpret matrix multiplication from this point of view. If A is an $m \times p$ matrix and B is an $p \times n$ matrix, then the matrix product AB is an $m \times n$ matrix. The ith row of AB is a linear combination of the rows of B: It is the product of the p-dimensional row vector $\mathrm{row}_i(A)$ and the matrix B, that is,

$$\mathrm{row}_i(AB) = \mathrm{row}_i(A)B.$$

Similarly, the jth column of AB is a linear combination of the columns of A: It is the product of the matrix A and the p-dimensional column vector $\mathrm{col}_j(B)$, that is,

$$\mathrm{col}_j(AB) = A\,\mathrm{col}_j(B).$$

We summarize this discussion as follows.

Theorem 2.10. *Let $A = (a_{i,k})$ be an $m \times p$ matrix and let $B = (b_{k,j})$ be an $p \times n$ matrix. For $i = 1, \ldots, m$ and $j = 1, \ldots, n$,*

$$row_i(AB) = row_i(A)B = \sum_{k=1}^{n} a_{i,k}\, row_k(B)$$

and

$$col_j(AB) = A\, col_j(B) = \sum_{k=1}^{p} b_{k,j}\, col_k(A).$$

Here is an example. If

$$A = \begin{pmatrix} 2 & -3 & 1 \\ 5 & 0 & -4 \\ 7 & -2 & 9 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -2 & 3 \\ 7 & 11 \\ 9 & -4 \end{pmatrix}$$

then

$$AB = \begin{pmatrix} 2 & -3 & 1 \\ 5 & 0 & -4 \\ 7 & -2 & 9 \end{pmatrix} \begin{pmatrix} -2 & 3 \\ 7 & 11 \\ 9 & -4 \end{pmatrix} = \begin{pmatrix} -16 & -31 \\ -46 & 31 \\ 53 & -37 \end{pmatrix}.$$

Each row of AB is a linear combination of the rows of B as follows:

$$\begin{aligned} \mathrm{row}_1(AB) = \mathrm{row}_1(A)B &= (2,-3,1) \begin{pmatrix} -2 & 3 \\ 7 & 11 \\ 9 & -4 \end{pmatrix} \\ &= 2(-2,3) - 3(7,11) + 1(9,-4) \\ &= (-4,6) + (-21,-33) + (9,-4) \\ &= (-16,-31) \end{aligned}$$

$$\begin{aligned} \mathrm{row}_2(AB) = \mathrm{row}_2(A)B &= (5,0,4) \begin{pmatrix} -2 & 3 \\ 7 & 11 \\ 9 & -4 \end{pmatrix} \\ &= 5(-2,3) + 0(7,11) - 4(9,-4) \\ &= (-10,15) + (0,0) + (-36,16) \\ &= (-46,31) \end{aligned}$$

$$\begin{aligned} \mathrm{row}_3(AB) = \mathrm{row}_3(A)B &= (7,-2,9) \begin{pmatrix} -2 & 3 \\ 7 & 11 \\ 9 & -4 \end{pmatrix} \\ &= 7(-2,3) - 2(7,11) + 9(9,-4) \\ &= (-14,21) + (-14,-22) + (81,-36) \\ &= (53,-37). \end{aligned}$$

Each column of AB is a linear combination of the columns of A as follows:

$$\begin{aligned} \mathrm{col}_1(AB) = A\,\mathrm{col}_1(B) &= \begin{pmatrix} 2 & -3 & 1 \\ 5 & 0 & -4 \\ 7 & -2 & 9 \end{pmatrix} \begin{pmatrix} -2 \\ 7 \\ 9 \end{pmatrix} \\ &= -2 \begin{pmatrix} 2 \\ 5 \\ 7 \end{pmatrix} + 7 \begin{pmatrix} -3 \\ 0 \\ -2 \end{pmatrix} + 9 \begin{pmatrix} 1 \\ -4 \\ 9 \end{pmatrix} = \begin{pmatrix} -16 \\ -46 \\ 53 \end{pmatrix} \end{aligned}$$

$$\mathrm{col}_2(AB) = A\,\mathrm{col}_2(B) = \begin{pmatrix} 2 & -3 & 1 \\ 5 & 0 & -4 \\ 7 & -2 & 9 \end{pmatrix} \begin{pmatrix} 3 \\ 11 \\ -4 \end{pmatrix}$$
$$= 3\begin{pmatrix} 2 \\ 5 \\ 7 \end{pmatrix} + 11\begin{pmatrix} -3 \\ 0 \\ -2 \end{pmatrix} - 4\begin{pmatrix} 1 \\ -4 \\ 9 \end{pmatrix} = \begin{pmatrix} -31 \\ 31 \\ -37 \end{pmatrix}.$$

Let $A = (a_{i,j})$ be an $m \times n$ matrix. The ith *row sum* of A is

$$\mathrm{rowsum}_i(A) = \sum_{j=1}^{n} a_{i,j}$$

and the jth *column sum* of A is

$$\mathrm{colsum}_j(A) = \sum_{i=1}^{m} a_{i,j}.$$

An $m \times n$ matrix $A = (a_{i,j})$ is *nonnegative* if $a_{i,j} \geq 0$ for all $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,n\}$.

An $m \times n$ matrix $A = (a_{i,j})$ is *positive* if $a_{i,j} > 0$ for all $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,n\}$.

An $m \times n$ nonnegative matrix $A = (a_{i,j})$ is *row stochastic* if every row sum equals 1, that is,

$$\mathrm{rowsum}_i(A) = 1$$

for all $i \in \{1,\ldots,m\}$. An $m \times n$ nonnegative matrix $A = (a_{i,j})$ is *column stochastic* if every column sum equals 1, that is,

$$\mathrm{colsum}_j(A) = 1$$

for all $j \in \{1,\ldots,n\}$. An $m \times n$ nonnegative matrix $A = (a_{i,j})$ is *doubly stochastic* if it is both row and column stochastic.

Exercises

1. Let

$$A = \begin{pmatrix} 3 & -2 & 5 \\ 7 & 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathbf{x} = \begin{pmatrix} 4 \\ -1 \\ 6 \end{pmatrix}.$$

   a. Compute $A\mathbf{x}$.
   b. Compute the column vectors

$$4\begin{pmatrix} 3 \\ 7 \end{pmatrix}, \qquad -\begin{pmatrix} -2 \\ 1 \end{pmatrix} \qquad \text{and} \qquad 6\begin{pmatrix} 5 \\ 0 \end{pmatrix}.$$

c. Show that

$$A\mathbf{x} = 4\begin{pmatrix}3\\7\end{pmatrix} - \begin{pmatrix}-2\\1\end{pmatrix} + 6\begin{pmatrix}5\\0\end{pmatrix}.$$

2. Let

$$A = \begin{pmatrix}3 & -2 & 5\\7 & 1 & 0\end{pmatrix} \qquad \text{and} \qquad \mathbf{y} = \begin{pmatrix}-4\\9\end{pmatrix}.$$

a. Compute $\mathbf{y}^t A$.
b. Compute the row vectors

$$-4\begin{pmatrix}3 & -2 & 5\end{pmatrix} \qquad \text{and} \qquad 9\begin{pmatrix}7 & 1 & 0\end{pmatrix}.$$

c. Show that

$$\mathbf{y}^t A = -4\begin{pmatrix}3 & -2 & 5\end{pmatrix} + 9\begin{pmatrix}7 & 1 & 0\end{pmatrix}.$$

3. Let

$$A = \begin{pmatrix}1 & 2 & 3\\4 & 5 & 6\\7 & 8 & 9\end{pmatrix} \qquad \text{and} \qquad \mathbf{x} = \begin{pmatrix}2\\-3\\-1\end{pmatrix}.$$

a. Compute $A\mathbf{x}$.
b. Compute the column vectors

$$2\begin{pmatrix}1\\4\\7\end{pmatrix}, \qquad -3\begin{pmatrix}2\\5\\8\end{pmatrix} \qquad \text{and} \qquad -\begin{pmatrix}3\\6\\9\end{pmatrix}.$$

c. Show that

$$A\mathbf{x} = 2\begin{pmatrix}1\\4\\7\end{pmatrix} - 3\begin{pmatrix}2\\5\\8\end{pmatrix} - \begin{pmatrix}3\\6\\9\end{pmatrix}.$$

4. Let

$$A = \begin{pmatrix}1 & 2 & 3\\4 & 5 & 6\\7 & 8 & 9\end{pmatrix} \qquad \text{and} \qquad \mathbf{y} = \begin{pmatrix}7\\-5\\2\end{pmatrix}.$$

a. Compute $\mathbf{y}^t A$.
b. Compute the row vectors

$$7\begin{pmatrix}1 & 2 & 3\end{pmatrix}, \qquad -5\begin{pmatrix}4 & 5 & 6\end{pmatrix}, \qquad \text{and} \qquad 2\begin{pmatrix}7 & 8 & 9\end{pmatrix}.$$

c. Show that

$$\mathbf{y}^t A = 7\begin{pmatrix}1 & 2 & 3\end{pmatrix} - 5\begin{pmatrix}4 & 5 & 6\end{pmatrix} + 2\begin{pmatrix}7 & 8 & 9\end{pmatrix}.$$

5. Let A be an $m \times n$ matrix and let B by an $n \times p$ matrix.

a. Prove that if the kth row of A is the zero row, then the kth row of AB is the zero row.

b. Prove that if the ℓth column of B is the zero column, then the kth row of AB is the zero column.

6. Let

$$A = \begin{pmatrix} 7 & 3 & 0 \\ -1 & -2 & 11 \\ 0 & 5 & 2 \end{pmatrix} \qquad \text{and} \qquad x = \begin{pmatrix} 3 \\ -4 \\ 2 \end{pmatrix}$$

a. Compute the column vector Ax as a linear combination of the columns of A.
b. The transpose of the column vector x is the row vector x^t. Compute the row vector x^tA as a linear combination of the rows of A.

7. a. Compute the row and column sums of the matrix

$$A = \begin{pmatrix} 5 & 0 & -3 \\ 2 & -9 & -1 \end{pmatrix}.$$

b. Show that

$$\text{rowsum}_1(A) + \text{rowsum}_2(A) = \text{colsum}_1(A) + \text{colsum}_2(A) + \text{colsum}_3(A).$$

8. Let A be an $m \times n$ matrix. Prove that

$$\sum_{i=1}^{m} \text{rowsum}_i(A) = \sum_{j=1}^{n} \text{colsum}_j(A).$$

9. Prove that a doubly stochastic matrix must be a square matrix. Equivalently, prove that if an $m \times n$ nonnegative matrix $A = (a_{i,j})$ is doubly stochastic, then $m = n$.
10. Let A be a positive $m \times n$ matrix. Define the $n \times n$ diagonal matrix

$$R(A) = \text{diag}\left(\frac{1}{\text{rowsum}_1(A)}, \ldots, \frac{1}{\text{rowsum}_n(A)} \right).$$

Let $A = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 1 & 1 \end{pmatrix}$.

a. Compute $R(A)$.
b. Compute $R(A)\,A$.
c. Prove that the matrix $R(A)\,A$ is row stochastic.
d. Prove that $R(A)\,A = A$ if and only if A is row stochastic.

11. Let A be a positive $m \times n$ matrix. Define the $n \times n$ diagonal matrix

$$C(A) = \text{diag}\left(\frac{1}{\text{colsum}_1 A)}, \ldots, \frac{1}{\text{colsum}_n A)} \right).$$

Let $A = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 1 & 1 \end{pmatrix}$.

a. Compute $C(A)$.
b. Compute $A\,C(A)$.
c. Prove that the matrix $A\,C(A)$ is column stochastic.
d. Prove that $A\,C(A) = A$ if and only if A is column stochastic.

12. Let A be a nonnegative $m \times n$ matrix. Let $\mathbf{j}_n$ be the n-dimensional vector all of whose coordinates are equal to 1.

    a. Prove that
    $$A\mathbf{j}_n = \begin{pmatrix} \text{rowsum}_1(A) \\ \vdots \\ \text{rowsum}_m(A) \end{pmatrix}.$$

    b. Prove that
    $$A\mathbf{j}_n = \mathbf{j}_m$$
    if and only if the matrix A is row stochastic.

13. Let A be a nonnegative $m \times n$ matrix. Let $\mathbf{j}_n$ be the n-dimensional vector all of whose coordinates are equal to 1.

    a. Prove that
    $$\mathbf{j}_m^t A = \left(\text{colsum}_1(A), \cdots, \text{colsum}_n(A)\right).$$

    b. Prove that
    $$\mathbf{j}_m^t A = \mathbf{j}_n^t$$
    if and only if the matrix A is column stochastic.

14. Let $c_1, \ldots, c_n$ be a sequence of n real numbers. Define the $n \times n$ matrix $A = (a_{i,j})$ as follows:
    $$a_{1,j} = c_j \qquad \text{for } j \in \{1, \ldots, n\},$$
    For $i \in \{2, \ldots, n\}$, let
    $$a_{i,1} = a_{i-1,n}$$
    and
    $$a_{i,j} = a_{i-1,j-1} \qquad \text{for } j \in \{2, \ldots, n\}.$$
    The matrix A is called a *circulant matrix*. The $n \times n$ circulant matrices for $n = 2, 3, 4$ have the following forms:
    $$\begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix}, \qquad \begin{pmatrix} c_1 & c_2 & c_3 \\ c_3 & c_1 & c_2 \\ c_2 & c_3 & c_1 \end{pmatrix}, \qquad \begin{pmatrix} c_1 & c_2 & c_3 & c_4 \\ c_4 & c_1 & c_2 & c_3 \\ c_3 & c_4 & c_1 & c_2 \\ c_2 & c_3 & c_4 & c_1 \end{pmatrix}.$$

    a. Let A be the $n \times n$ circulant matrix constructed from the sequence $c_1, \ldots, c_n$, and let $s = \sum_{i=1}^n c_i$. Prove that
    $$\text{rowsum}_i(A) = \text{colsum}_i(A) = s$$

for all $i, j \in \{1, \ldots, n\}$.

b. A $n \times n$ matrix is *persymmetric* if it is symmetric with respect to its northeast to southwest diagonal, that is, if

$$a_{i,j} = a_{n+1-j,n+1-i}$$

for all $i, j \in \{1, \ldots, n\}$. Prove that a circulant matrix is persymmetric.

15. Let $\mathrm{Mat}_n(\mathbf{R})$ be the set of all $n \times n$ matrices with coordinates in the field $\mathbf{R}$. For all $p = 1, \ldots, n$ and $q = 1, \ldots, n$, define the matrix $E^{(p,q)} = \left(e_{i,j}^{(p,q)}\right)$ whose (i, j)th coordinate is

$$e_{i,j}^{(p,q)} = \delta_{i,p}\delta_{j,q} = \begin{cases} 1 & \text{if } i = p \text{ and } j = q \\ 0 & \text{otherwise.} \end{cases}$$

Let $A = (a_{i,j}) \in \mathrm{Mat}_n(\mathbf{R})$.

a. Prove that

$$A = \sum_{p=1}^{n} \sum_{q=1}^{n} a_{p,q} E^{(p,q)}.$$

b. Prove that $AE^{(p,q)}$ is the $n \times n$ matrix whose qth column is the pth column of A, and whose jth column is the zero column for all $j \neq q$.

c. Prove that $E^{(p,q)}A$ is the $n \times n$ matrix whose pth row is the qth row of A, and whose ith row is the zero row for all $i \neq p$.

d. Prove that $E^{(p,k)}AE^{(\ell,q)}$ is the $n \times n$ matrix whose (p,q)th coordinate is $a_{k,\ell}$ and whose other coordinates are zero. Equivalently, prove that

$$E^{(p,k)}AE^{(\ell,q)} = a_{k,\ell}E^{(p,q)}.$$

e. Prove that if $a_{k,\ell} \neq 0$ for some k and ℓ, then

$$\mathrm{diag}\left(a_{k,\ell}^{-1}, \ldots, a_{k,\ell}^{-1}\right) E^{(p,k)}AE^{(\ell,q)} = a_{k,\ell}^{-1}E^{(p,k)}AE^{(\ell,q)} = E^{(p,q)}.$$

16. Let $\mathscr{I}$ be a set of matrices in $\mathrm{Mat}_n(\mathbf{R})$ such that, if $A, B \in \mathscr{I}$, then $A + B \in \mathscr{I}$, and if $A \in \mathscr{I}$ and $C \in \mathrm{Mat}_n(\mathbf{R})$, then $AC \in \mathscr{I}$ and $CA \in \mathscr{I}$. Prove that if $\mathscr{I}$ contains a matrix $A \neq 0$, then $\mathscr{I} = \mathrm{Mat}_n(\mathbf{R})$.

2.4 Linear transformations

Let $A = (a_{i,j})$ be an $m \times n$ matrix, and let $\mathbf{x}$ be a vector in $\mathbf{R}^n$. The product $\mathbf{y} = A\mathbf{x}$ is a vector in $\mathbf{R}^m$. Thus, the matrix A determines a function $T_A : \mathbf{R}^n \to \mathbf{R}^m$ defined by $T_A(\mathbf{x}) = A\mathbf{x}$. Let $\mathbf{x}, \mathbf{x}' \in \mathbf{R}$ and $c \in \mathbf{R}$. Using properties of matrix multiplication (Theorem 2.5), we see that

$$T_A(\mathbf{x} + \mathbf{x}') = A(\mathbf{x} + \mathbf{x}') = A\mathbf{x} + A\mathbf{x}' = T_A(\mathbf{x}) + T_A(\mathbf{x}')$$

and

$$T_A(c\mathbf{x}) = A(c\mathbf{x}) = cA\mathbf{x} = cT_A(\mathbf{x}).$$

Let V and W be vector spaces. A function $T : V \to W$ is a *linear transformation* if, for all vectors $\mathbf{x}, \mathbf{x}' \in V$ and for all scalars $c \in \mathbf{R}$,

$$T(\mathbf{x} + \mathbf{x}') = T(\mathbf{x}) + T(\mathbf{x}')$$

and

$$T(c\mathbf{x}) = cT(\mathbf{x}).$$

We have proved the following.

Theorem 2.11. *For every $m \times n$ matrix A, the function $T_A : \mathbf{R}^n \to \mathbf{R}^m$ defined by $T_A(\mathbf{x}) = A\mathbf{x}$ is a linear transformation.*

2.5 The inverse of a matrix

The $n \times n$ identity matrix is $I_n = (\delta_{i,j})$, where $\delta_{i,j}$ is the Kronecker delta. Let A be an $m \times n$ matrix. An $n \times m$ matrix B is a *left inverse* for A if $BA = I_n$. An $n \times m$ matrix C is a *right inverse* for A if $AC = I_m$.

For example, if

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad \text{and} \qquad V = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

then

$$UV = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

and so U is a left inverse of V and V is a right inverse of U.

Note that

$$VU = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq I_3$$

and so V is not a left inverse of U and U is not a right inverse of V.

Lemma 2.1. *Let A be an $m \times n$ matrix. If the $n \times m$ matrix B is a left inverse of A and the $n \times m$ matrix C is a right inverse of A, then $m = n$ and $B = C$.*

Proof. Because $BA = I_n$ and $AC = I_m$, the associativity of matrix multiplication implies that

$$B = BI_m = B(AC) = (BA)C = I_nC = C.$$

Because B is an $n \times m$ matrix and C is an $m \times n$ matrix, the equation $B = C$ implies that $m = n$. This completes the proof.

An $n \times n$ matrix A is called *invertible* if it has a right inverse and a left inverse. By Lemma 2.1, if A is invertible, then there exists a unique matrix B such that $BA = AB = I_n$. The $n \times n$ matrix B is called the *inverse* of A, and denoted A^{-1}.

For example, we have

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \qquad \text{and} \qquad A^{-1} = \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}.$$

We have

$$B = \begin{pmatrix} 1 & 5 & -2 \\ 0 & 1 & 8 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad B^{-1} = \begin{pmatrix} 1 & -5 & \\ 0 & 1-8 & \\ 0 & 0 & 1 \end{pmatrix}.$$

If

$$C = \begin{pmatrix} 3 & -2 \\ 4 & -3 \end{pmatrix}$$

then

$$C^2 = \begin{pmatrix} 3 & -2 \\ 4 & -3 \end{pmatrix} \begin{pmatrix} 3 & -2 \\ 4 & -3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

and so $C = C^{-1}$.

Lemma 2.2. *The* 2×2 *matrix* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *is invertible if and only if* $\Delta = ad - bc \neq 0$. *In this case,*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix}.$$

Proof. We have

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} \\ &= \Delta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

If $\Delta \neq 0$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix}.$$

Conversely, if the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible, then there exists a matrix $\begin{pmatrix} w & x \\ y & z \end{pmatrix}$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Equivalently,

$$\begin{aligned} aw + by &= 1 \\ ax + bz &= 0 \\ cw + dy &= 0 \\ cx + dz &= 1. \end{aligned}$$

The first equation implies that $a \neq 0$ or $b \neq 0$. If $a \neq 0$, then

$$x = -\frac{b}{a}z$$

and

$$cx + dz = -\frac{bc}{a}z + dz = \frac{ad - bc}{a}z = 1$$

and so $\Delta = ad - bc \neq 0$. The cased $b \neq 0$ is similar. This completes the proof.

Lemma 2.3. *(i) If A is an invertible $n \times n$ matrix, then A^{-1} is invertible, and*

$$\left(A^{-1}\right)^{-1} = A.$$

(ii) If A and B are invertible $n \times n$ matrices, then AB is invertible, and

$$(AB)^{-1} = B^{-1}A^{-1}.$$

(iii) If $k \geq 2$ and $A_1, A_2, \ldots, A_{k-1}, A_k$ are invertible $n \times n$ matrices, then $A_1A_2 \cdots A_k$ is invertible, and $(A_1A_2 \cdots A_{k-1}A_k)^{-1} = A_k^{-1}A_{k-1}^{-1} \cdots A_2^{-1}A_1^{-1}$.

Proof. If A is an invertible, then the matrix equation $AA^{-1} = A^{-1}A = I_n$ implies that A^{-1} is invertible and that $\left(A^{-1}\right)^{-1} = A$. This proves (i).

Suppose that A and B are invertible. Using the associativity of matrix multiplication, we have

$$\begin{aligned} (AB)\left(B^{-1}A^{-1}\right) &= A\left(B\left(B^{-1}A^{-1}\right)\right) = A\left(\left(BB^{-1}\right)A^{-1}\right) \\ &= A\left(I_nA^{-1}\right) = AA^{-1} = I_n. \end{aligned}$$

Similarly, $\left(B^{-1}A^{-1}\right)(AB) = I_n$, and so AB is invertible and $(AB)^{-1} = B^{-1}A^{-1}$. This proves (ii).

We shall prove part (iii) of the Lemma by induction on $k \geq 2$. The case $k = 2$ is exactly part (ii) of the Lemma. Let $k \geq 3$ and assume that part (iii) is true for every sequence of $k-1$ invertible $n \times n$ matrices. Let $A_1, \ldots, A_{k-1}, A_k$ be a sequence of k invertible $n \times n$ matrices, and let $B = A_1A_2 \cdots A_{k-1}$ be the product of the first $k-1$ matrices. By the induction hypothesis, $B^{-1} = (A_1A_2 \cdots A_{k-1})^{-1} = A_{k-1}^{-1} \cdots A_2^{-1}A_1^{-1}$, and so

$$\begin{aligned}(A_1A_2\cdots A_{k-1}A_k)^{-1} &= (BA_k)^{-1}\\ &= A_k^{-1}B^{-1}\\ &= A_k^{-1}(A_1A_2\cdots A_{k-1})^{-1}\\ &= A_k^{-1}\left(A_{k-1}^{-1}\cdots A_2^{-1}A_1^{-1}\right)\\ &= A_k^{-1}A_{k-1}^{-1}\cdots A_2^{-1}A_1^{-1}.\end{aligned}$$

This completes the proof.

A *matrix group* is a set G of $n\times n$ matrices that is a group with respect to the operation of matrix multiplication. Equivalently, a set $G \subseteq \mathrm{Mat}_n(\mathbf{R})$ is a matrix group if

(i) G contains the identity matrix I_n.
(ii) If G contains the matrices A and B, then G also contains their product AB.
(iii) Every matrix in G is invertible. If $A \in G$, then $A^{-1} \in G$.

For example, the set $GL_n(\mathbf{R})$ of all invertible $n\times n$ matrices with real coordinates is a group. It suffices to observe that if $A \in GL_n(\mathbf{R})$ and $B \in GL_n(\mathbf{R})$, then $(AB)^{-1} = B^{-1}A^{-1} \in GL_n(\mathbf{R})$, and so $AB \in GL_n(\mathbf{R})$. We call $GL_n(\mathbf{R})$ the *general linear group*.

Exercises

1. Let $A = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}$ and $B = \begin{pmatrix} 4 & 9 \\ 7 & 8 \end{pmatrix}$. Compute the inverses of the following matrices;
$$A, \quad B, \quad AB, \quad BA, \quad ABA.$$
2. Prove that the set of matrices
$$G = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbf{R} \right\}$$
is an abelian group under matrix multiplication. Define the function $f : \mathbf{Z} \to G$ by
$$f(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$
Prove that $f(x+y) = f(x)f(y)$ for all $x,y \in \mathbf{R}$.
3. The *general linear group* $GL_2(\mathbf{R})$ is the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbf{R})$ such that $ad - bc \neq 0$.
   a. Prove that if $A, B \in GL_2(\mathbf{R})$, then $AB \in GL_2(\mathbf{R})$.
   b. Prove that if $A \in GL_2(\mathbf{R})$, then A is invertible and $A^{-1} \in GL_2(\mathbf{R})$. Compute A^{-1}.

4. Let $SL_2(\mathbf{R})$ be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbf{R})$ such that $ad-bc = 1$.

   a. Prove that if $A,B \in SL_2(\mathbf{R})$, then $AB \in SL_2(\mathbf{R})$.
   b. Prove that if $A \in SL_2(\mathbf{R})$, then A is invertible and $A^{-1} \in SL_2(\mathbf{R})$. Compute A^{-1}.

   The set $SL_2(\mathbf{R})$ is called the *special linear group*.

5. The *integer special linear group* $SL_2(\mathbf{Z})$ is the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a,b,c,d \in \mathbf{Z}$ and $ad-bc=1$.

   a. Prove that if $A,B \in SL_2(\mathbf{Z})$, then $AB \in SL_2(\mathbf{Z})$.
   b. Prove that if $A \in SL_2(\mathbf{Z})$, then A is invertible and $A^{-1} \in SL_2(\mathbf{Z})$. Compute A^{-1}.

6. For $\theta \in \mathbf{R}$, let
$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \in SL_2(\mathbf{R}).$$
   Prove that, for all $\theta_1, \theta_2, \theta \in \mathbf{R}$,
$$R(\theta_1)R(\theta_2) = R(\theta_1+\theta_2)$$
   and
$$R(\theta)^{-1} = R(-\theta).$$
   The *rotation group* $SO(2)$ is the set of matrices $\{R(\theta) : \theta \in \mathbf{R}\}$.

7. The *affine group* $\mathscr{A}(\mathbf{R})$ is the set of all matrices of the form $\begin{pmatrix} r & x \\ 0 & 1 \end{pmatrix}$ with $r \in \mathbf{R}\setminus\{0\}$ and $x \in \mathbf{R}$.

   a. Prove that if $A,B \in \mathscr{A}(\mathbf{R})$, then $AB \in \mathscr{A}$.
   b. Prove that if $A \in \mathscr{A}(\mathbf{R})$, then A is invertible and $A^{-1} \in \mathscr{A}(\mathbf{R})$. Compute A^{-1}.

8. The *Heisenberg group* $H_3(\mathbf{R})$ is the set of all 3×3 matrices $\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ such that $a,b,c \in \mathbf{R}$.

   a. Prove that if $A,B \in H_3(\mathbf{R})$, then $AB \in H_3(\mathbf{R})$.
   b. Prove that if $A \in H_3(\mathbf{R})$, then A is invertible and $A^{-1} \in H_3(\mathbf{R})$. Compute A^{-1}.

   Solution: Let $A,B \in H_3(\mathbf{R})$. If
$$A = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 1 & d & f \\ 0 & 1 & e \\ 0 & 0 & 1 \end{pmatrix}$$

then

$$AB = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & f \\ 0 & 1 & e \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & c+f+ae \\ 0 & 1 & b+e \\ 0 & 0 & 1 \end{pmatrix} \in H_3(\mathbf{R})$$

and

$$A^{-1} = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \in H_3(\mathbf{R}).$$

2.6 The augmented matrix of a linear system

We can use matrices to represent systems of linear equations. Here is a system of m linear equations in n variables:

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n & = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n & = b_2 \\ \vdots & \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n & = b_m. \end{cases} \tag{2.5}$$

The *matrix of coefficients* of this system is the $m \times n$ matrix

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}. \tag{2.6}$$

Consider the n-dimensional column vector $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and the m-dimensional column vector $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$. Multiplying the matrix A by the vector x, we obtain

$$\begin{aligned} Ax &= \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \\ &= \begin{pmatrix} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n \\ \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n \end{pmatrix}. \end{aligned}$$

Thus, writing in coordinate form the matrix equation

$$Ax = b$$

we obtain

$$\begin{pmatrix} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n \\ \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Equating coordinates of these two m-dimensional column vectors, we recover the system of linear equations (2.5).

Consider the system of m linear equations (2.5) with matrix of coefficients (2.6). From the right sides of the linear equations, we construct the m-dimensional column vector $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$. Combining this column vector with the matrix of coefficients, we obtain the following $m \times (n+1)$ matrix

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} & b_2 \\ \vdots & & & \vdots & \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} & b_m \end{pmatrix}. \tag{2.7}$$

This is called the *augmented matrix* of the linear system. Conversely, from every $m \times (n+1)$ matrix of the form (2.7) , we can construct a system (2.5) of m linear equations in n variables.

For example, the system of linear equations

$$\begin{aligned} x + 2y &= 3 \\ 4x + 5y &= 6 \end{aligned}$$

has the 2×2 matrix of coefficients

$$\begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix},$$

the column vector $\binom{3}{6}$, and the 2×3 augmented matrix

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

From the augmented matrix, we easily recover the original system of linear equations.

In this section, we shall show how to solve a system of linear equations by performing elementary operations on the rows of the augmented matrix. Recall that two systems of linear equations are *equivalent* if they have the same solutions

In Gaussian elimination, there are three elementary operations on a system of linear equations that produce an equivalent system of equations.

1. Interchange: We can interchange two equations in the system.
2. Multiplication: We can multiply an equation by a nonzero scalar.
3. Replacement: We can choose one equation in the system and add to it a multiple of a different equation in the system.

How do these elementary operations on a linear system affect the augmented matrix of the system?

1. Interchanging the kth and ℓth equations corresponds to interchanging the kth and ℓth rows of the augmented matrix.
2. Multiplying the kth equation by a nonzero number c corresponds to multiplying the kth row of the augmented matrix by c.
3. Adding c times the kth equation to the ℓth equation corresponds to adding c times the kth row to the ℓth row of the augmented matrix.

Thus, corresponding to the three elementary operations on the equations in a linear system, we define three *elementary row operations* on the rows of a matrix:

1. Interchange: We can interchange two rows in the matrix.
2. Multiplication: We can a multiply the coordinates in a row by a nonzero scalar.
3. Replacement: We can choose one row in the matrix and add to it a multiple of a different row in the matrix.

The inverse of each elementary row operation is another elementary row operation.

1. Interchange: The inverse of interchanging rows k and ℓ of a matrix is another interchange of rows k and ℓ.
2. Multiplication: The inverse of multiplying row k by the nonzero scalar c is multiplying row k by the nonzero scalar c^{-1}.
3. Replacement: The inverse of adding c times row k to row ℓ is adding $-c$ times row k to row ℓ.

We summarize this important discussion as follows. Given a system of m linear equations in n variables, we construct the $m \times (n+1)$ augmented matrix A. Applying any finite sequence of elementary row operations to this matrix, we obtain another $m \times (n+1)$ augmented matrix A'. The system of m linear equations in n variables obtained from the matrix A' is equivalent to the original m linear equations in n variables.

The matrices A and B are *row-equivalent* if B can be obtained from A by a finite sequence of elementary row operations. For example, consider the matrices $A = \begin{pmatrix} 2 & 5 \\ 9 & 3 \end{pmatrix}$ and $B = \begin{pmatrix} -8 & 7 \\ 1 & 6 \end{pmatrix}$.

1. Start with the matrix A. Add -4 times row 1 to row 2 and obtain

$$A_1 = \begin{pmatrix} 2 & 5 \\ 1 & -17 \end{pmatrix}.$$

2. Add -2 times row 2 to row 1 and obtain
$$A_2 = \begin{pmatrix} 0 & 39 \\ 1 & -17 \end{pmatrix}.$$
3. Add 23/39 times row 1 to row 2 and obtain
$$A_3 = \begin{pmatrix} 0 & 39 \\ 1 & 6 \end{pmatrix}.$$
4. Multiply row 1 by 55/39 and obtain
$$A_4 = \begin{pmatrix} 0 & 55 \\ 1 & 6 \end{pmatrix}.$$
5. Add -8 times row 2 to row 1 and obtain
$$B = \begin{pmatrix} -8 & 7 \\ 1 & 6 \end{pmatrix}.$$

Thus, matrix A is row-equivalent to matrix B. We may write this sequence of elementary row operations in the form
$$\begin{pmatrix} 2 & 5 \\ 9 & 3 \end{pmatrix} \to \begin{pmatrix} 2 & 5 \\ 1 & -17 \end{pmatrix} \to \begin{pmatrix} 0 & 39 \\ 1 & -17 \end{pmatrix} \to \begin{pmatrix} 0 & 39 \\ 1 & 6 \end{pmatrix} \to \begin{pmatrix} 0 & 55 \\ 1 & 6 \end{pmatrix} \to \begin{pmatrix} -8 & 7 \\ 1 & 6 \end{pmatrix}.$$
Because each elementary row operation is invertible, it follows that matrix B is also row-equivalent to matrix A. Here is a sequence of elementary row operations that produces A from B:
$$\begin{pmatrix} -8 & 7 \\ 1 & 6 \end{pmatrix} \to \begin{pmatrix} 0 & 55 \\ 1 & 6 \end{pmatrix} \to \begin{pmatrix} 0 & 39 \\ 1 & 6 \end{pmatrix} \to \begin{pmatrix} 0 & 39 \\ 1 & -17 \end{pmatrix} \to \begin{pmatrix} 2 & 5 \\ 1 & -17 \end{pmatrix} \to \begin{pmatrix} 2 & 5 \\ 9 & 3 \end{pmatrix}.$$

Write $A \sim B$ if A and B are $m \times n$ matrices and A is row-equivalent to B. Because the identity operation on a matrix is an elementary row operation, every matrix is row-equivalent to itself, that is, the relation of row-equivalence is *reflexive* in the sense that $A \sim A$ for every matrix A. Because every elementary row operation is invertible, it follows that if the matrix A is row-equivalent to B, then the matrix B is row-equivalent to A. Thus, row-equivalence is *symmetric* in the sense that, if A and B are $m \times n$ matrices and $A \sim B$, then $B \sim A$. If A, B, and C are $m \times n$ matrices such that $A \sim B$ and $B \sim C$, then there is a finite sequence of elementary row operations that produces the matrix B from A, and a finite sequence of elementary row operations that produces the matrix C from B. The concatenation of these two sequences is a finite sequence of elementary row operations that produces the matrix C from A. Thus, row-equivalence is *transitive* in the sense that if $A \sim B$ and $B \sim C$, then $A \sim C$. A relation that is reflexive, symmetric, and transitive is called an *equivalence relation* (Appendix A.4), and so, for every pair (m,n) of positive integers, row-equivalence is an equivalence relation on the set $\mathrm{Mat}_{m,n}(\mathbf{R})$.

Recall the sequence of elementary operations on equations that we used to solve the system (1.26) of two linear equations in two variables in Example 1 in Section 1.4. Here are the equations and the corresponding augmented matrix:

$$\begin{aligned} 9x + 11y &= -1 \\ 5x + 6y &= 3 \end{aligned} \qquad \begin{pmatrix} 9 & 11 & -1 \\ 5 & 6 & 3 \end{pmatrix}$$

Multiplying the first equation by 1/9 gives a new system of equations and a new augmented matrix. The new augmented matrix also arises from the original augmented matrix by performing the elementary row operation of multiplying the first row by 1/9:

$$\begin{aligned} x + \tfrac{11}{9}y &= -\tfrac{1}{9} \\ 5x + 6y &= 3 \end{aligned} \qquad \begin{pmatrix} 1 & \frac{11}{9} & -\frac{1}{9} \\ 5 & 6 & 3 \end{pmatrix}$$

Adding (-5) times the first equation to the second equation gives another system of equations and another augmented matrix. Again, the new augmented matrix is also obtained from the previous augmented matrix by adding (-5) times the first row to the second row:

$$\begin{aligned} x + \tfrac{11}{9}y &= -\tfrac{1}{9} \\ -\tfrac{1}{9}y &= \tfrac{32}{9} \end{aligned} \qquad \begin{pmatrix} 1 & \frac{11}{9} & -\frac{1}{9} \\ 0 & -\frac{1}{9} & \frac{32}{9} \end{pmatrix}$$

We continue to perform elementary operations on the equations and to compute the corresponding augmented matrices. Multiply the second equation by -9:

$$\begin{aligned} x + \tfrac{11}{9}y &= -\tfrac{1}{9} \\ y &= -32 \end{aligned} \qquad \begin{pmatrix} 1 & \frac{11}{9} & -\frac{1}{9} \\ 0 & 1 & -32 \end{pmatrix}$$

Adding (-11/9) times the second equation to the first equation gives the solution of the system of equations:

$$\begin{aligned} x &= 39 \\ y &= -32 \end{aligned} \qquad \begin{pmatrix} 1 & 0 & 39 \\ 0 & 1 & -32 \end{pmatrix}.$$

Here is another example of the equivalence of solving a system of linear equations by elementary equation operations and by elementary row operations. Consider the following system of three equations in three variables:

$$\left\{ \begin{aligned} 2x_1 - x_2 + x_3 &= 6 \\ x_1 - 7x_2 - 4x_3 &= 0 \\ -3x_1 + 2x_2 - x_3 &= -1. \end{aligned} \right. \tag{2.8}$$

Interchange equations 1 and 2:

$$\begin{aligned} x_1 - 7x_2 - 4x_3 &= 0 \\ 2x_1 - x_2 + x_3 &= 6 \\ -3x_1 + 2x_2 - x_3 &= -1 \end{aligned}$$

Add (-2) times equation 1 to equation 2:

$$\begin{aligned} x_1 - \ \ 7x_2 - 4x_3 &= \ \ 0 \\ 13x_2 + 9x_3 &= \ \ 6 \\ -3x_1 + \ \ 2x_2 - \ \ x_3 &= -1 \end{aligned}$$

Add 3 times equation 1 to equation 3:

$$\begin{aligned} x_1 - \ \ 7x_2 - \ \ 4x_3 &= \ \ 0 \\ 13x_2 + \ \ 9x_3 &= \ \ 6 \\ -\ 19x_2 - 13x_3 &= -1 \end{aligned}$$

Multiply equation 2 by 1/13:

$$\begin{aligned} x_1 - \ \ 7x_2 - \quad 4x_3 &= \quad 0 \\ x_2 + 9/13x_3 &= 6/13 \\ -\ 19x_2 - \quad 13x_3 &= \ \ -1 \end{aligned}$$

Add 7 times equation 2 to equation 1:

$$\begin{aligned} x_1 \qquad\quad + 11/13x_3 &= 42/13 \\ x_2 + \ \ 9/13x_3 &= \ \ 6/13 \\ -\ 19x_2 - \quad 13x_3 &= \quad -1 \end{aligned}$$

Add 19 times equation 2 to equation 3:

$$\begin{aligned} x_1 \quad + 11/13x_3 &= \ \ 42/13 \\ x_2 + \ \ 9/13x_3 &= \quad 6/13 \\ 2/13x_3 &= 101/13 \end{aligned}$$

Multiply equation 3 by 13/2:

$$\begin{aligned} x_1 \quad + 11/13x_3 &= 42/13 \\ x_2 + \ \ 9/13x_3 &= \ \ 6/13 \\ x_3 &= 101/2 \end{aligned}$$

Add (-11/13) times equation 3 to equation 1:

$$\begin{aligned} x_1 \qquad\qquad\quad &= -79/2 \\ x_2 + 9/13x_3 &= \quad 6/13 \\ x_3 &= \ \ 101/2 \end{aligned}$$

Add (-9/13) times equation 3 to equation 2 and obtain the solution:

$$\begin{aligned} x_1 \qquad\quad &= -79/2 \\ x_2 \quad &= -69/2 \\ x_3 &= 101/2. \end{aligned}$$

The augmented matrix for the system (2.8) is

$$\begin{pmatrix} 2 & -1 & 1 & 6 \\ 1 & -7 & -4 & 0 \\ -3 & 2 & -1 & -1 \end{pmatrix}.$$

The corresponding sequence of elementary row operations on the augmented matrix produces the following matrices:

$$\begin{pmatrix} 2 & -1 & 1 & 6 \\ 1 & -7 & -4 & 0 \\ -3 & 2 & -1 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & -7 & -4 & 0 \\ 2 & -1 & 1 & 6 \\ -3 & 2 & -1 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & -7 & -4 & 0 \\ 0 & 13 & 9 & 6 \\ -3 & 2 & -1 & -1 \end{pmatrix}$$
$$\to \begin{pmatrix} 1 & -7 & -4 & 0 \\ 0 & 13 & 9 & 6 \\ 0 & -19 & -13 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & -7 & -4 & 0 \\ 0 & 1 & 9/13 & 6/13 \\ 0 & -19 & -13 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 11/13 & 42/13 \\ 0 & 1 & 9/13 & 6/13 \\ 0 & -19 & -13 & -1 \end{pmatrix}$$
$$\to \begin{pmatrix} 1 & 0 & 11/13 & 42/13 \\ 0 & 1 & 9/13 & 6/13 \\ 0 & 0 & 2/13 & 101/13 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 11/13 & 42/13 \\ 0 & 1 & 9/13 & 6/13 \\ 0 & 0 & 1 & 101/2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & -79/2 \\ 0 & 1 & 9/13 & 6/13 \\ 0 & 0 & 1 & 101/2 \end{pmatrix}$$
$$\to \begin{pmatrix} 1 & 0 & 0 & -79/2 \\ 0 & 1 & 0 & -69/2 \\ 0 & 0 & 1 & 101/2 \end{pmatrix}.$$

Translating this into equations yields the solution $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -79/2 \\ -69/2 \\ 101/2 \end{pmatrix}$.

In the case of a homogeneous system of linear equations, the right hand column of the augmented matrix is the zero column vector, and remains the zero vector after any elementary row operation on the matrix. Therefore, to solve a system of homogeneous equations, we can simply apply elementary row operations to the matrix of coefficients of the system of equations.

Here are two more examples. Consider the following homogeneous system of three equations in three variables:

$$\begin{aligned} x_1 + 4x_2 - 5x_3 &= 0 \\ 3x_1 + 8x_2 - 7x_3 &= 0 \\ 2x_1 + 5x_2 + 5x_3 &= 0 \end{aligned}$$

The matrix of coefficients of this system is

$$\begin{pmatrix} 1 & 4 & -5 \\ 3 & 8 & -7 \\ 2 & 5 & 5 \end{pmatrix}$$

Applying elementary row operations, we obtain the following sequence of matrices:

$$\begin{pmatrix} 1 & 4 & -5 \\ 3 & 8 & -7 \\ 2 & 5 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 4 & -5 \\ 0 & -4 & 8 \\ 2 & 5 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 4 & -5 \\ 0 & -4 & 8 \\ 0 & -3 & 15 \end{pmatrix} \to \begin{pmatrix} 1 & 4 & -5 \\ 0 & 1 & -2 \\ 0 & -3 & 15 \end{pmatrix}$$
$$\to \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -2 \\ 0 & -3 & 15 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -2 \\ 0 & 0 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and so the homogeneous system has only the zero solution $x_1 = x_2 = x_3 = 0$.

Consider the following homogeneous system of three equations in three variables:

$$\begin{cases} x_1 + 2x_2 + x_3 = 0 \\ 4x_1 + 5x_2 + 6x_3 = 0 \\ 7x_1 + 8x_2 + 9x_3 = 0 \end{cases} \tag{2.9}$$

The matrix of coefficients of this system is

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

Applying elementary row operations, we obtain the following sequence of matrices:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 7 & 8 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & -6 & -12 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

and so the homogeneous system (2.9) is equivalent to the system of equations

$$\begin{aligned} x_1 - x_3 &= 0 \\ x_2 + 2x_3 &= 0 \end{aligned}$$

It follows that the general solution of (2.9) is

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} t \\ -2t \\ t \end{pmatrix} = t \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

for any number t in the field $\mathbf{R}$.

Observe that the final matrix in the preceding problem has the following properties: Every zero row is below every nonzero row. The first nonzero coordinate in each nonzero row is 1, and, if this 1 occurs in column k, then every other coordinate in column k is 0. If i and $i+1$ are successive nonzero rows, and if the first nonzero coordinate in row i occurs in column k_1 and the first nonzero coordinate in row $i+1$

occurs in column k_2, then $k_1 < k_2$. We memorialize these properties of a matrix in the definition of reduced row echelon form.

Every zero matrix is in reduced row echelon form.

A nonzero $m \times n$ matrix $A = (a_{i,j})$ is in *row echelon form* if it satisfies the following properties: There is a positive integer r and a strictly increasing sequence of positive integers

$$k_1 < k_2 < \cdots < k_r$$

such that

$$\begin{aligned} a_{i,k_i} &= 1 \quad \text{for } i = 1, \ldots, r \\ a_{i,j} &= 0 \quad \text{for } i = 1, \ldots, r \text{ and } j = 1, \ldots, k_i - 1 \\ a_{\ell,k_i} &= 0 \quad \text{for } i = 1, \ldots, r \text{ and } \ell = i+1, \ldots, m \\ a_{i,j} &= 0 \quad \text{for } i = r+1, \ldots, m \text{ and } j = 1, \ldots, n. \end{aligned}$$

The matrix A is in *reduced row echelon form* if it also satisfies:

$$a_{\ell,k_i} = 0 \quad \text{for } i = 1, \ldots, r \text{ and } \ell = 1, \ldots, i-1.$$

A complete list of 2×2 matrices in reduced row echelon form is:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & a_{1,2} \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

For $a_{1,2} \neq 0$, the matrix

$$\begin{pmatrix} 1 & a_{1,2} \\ 0 & 1 \end{pmatrix}$$

is in row echelon form but not reduced row echelon form.

A complete list of 2×3 matrices in reduced row echelon form is:

$$\begin{pmatrix} 1 & 0 & a_{1,3} \\ 0 & 1 & a_{2,3} \end{pmatrix}, \quad \begin{pmatrix} 1 & a_{1,2} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & a_{1,2} & a_{1,3} \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & a_{1,3} \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Theorem 2.12. *Every matrix is row-equivalent to a reduced row echelon matrix.*

Proof. The proof is by induction on the number of rows.

Let $A = (a_{i,j})$ be a nonzero $m \times n$ matrix. If $m = 1$, then $A = (a_{1,j})$ is a nonzero row vector. Let k_1 be the least integer such that $a_{1,k_1} \neq 0$. Multiplying A by a_{1,k_1}^{-1} gives a matrix in reduced row echelon form.

Let $m \geq 1$, and assume that the Theorem is true for $m \times n$ matrices. Let A be an $(m+1) \times n$ matrix. Let k_1 be the least integer such that $a_{i,k_1} \neq 0$ for some i. If $i \neq 1$, then interchange rows 1 and i,. We obtain a matrix $A^{(1)} = (a_{i,j}^{(1)})$ such that $a_{i,j}^{(1)} = 0$ if $j < k_1$ and $a_{1,k_1}^{(1)} \neq 0$. If $a_{1,k_1}^{(1)} \neq 1$, then multiply row 1 by a_{1,k_1}^{-1} and obtain a matrix

$A^{(2)} = (a^{(2)}_{i,j})$ with $a^{(2)}_{i,j} = 0$ if $j < k_1$ and $a^{(2)}_{1,k_1} = 1$. For $i = 2,\ldots,m$, if $a^{(2)}_{i,k_1} \neq 0$, then add $-a^{(2)}_{i,k_1}$ times row 1 to row i. We obtain the $m \times n$ matrix $A^{(3)} = (a^{(3)}_{i,j})$ with $a^{(3)}_{i,j} = 0$ if $j < k_1$, $a^{(3)}_{1,k_1} = 1$, and $a^{(3)}_{i,k_1} = 0$ for $i = 2,\ldots,m$.

Let $B = (b_{i,j})$ be the $m \times n$ matrix obtained by deleting the first row of the $(m+1) \times n$ matrix $A^{(3)}$. We have $b_{i,j} = a^{(3)}_{i+1,j}$ for $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,n\}$, and so $b_{i,j} = 0$ for all $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,k_1\}$. By the induction hypothesis, elementary row operations applied to B, that is, to rows $2,3,\ldots,m+1$ of A, put these m rows in reduced row echelon form with integers $k_1 < k_2 < \cdots < k_r$ that satisfy $a_{i,k_i} = 1$ for $i = 2,\ldots,r$ and the other requirements for reduced row echelon form. If $a_{1,k_i} \neq 0$ for some $i \in \{2,\ldots,r\}$, then we subtract a_{1,k_i} times row i from row 1, and obtain an $(m+1) \times n$ matrix in reduced row echelon form. This completes the proof.

Here is an example. Consider the 3×3 matrix

$$A = \begin{pmatrix} 3 & 13 & 37 \\ 1 & 4 & 13 \\ 2 & 14 & 14 \end{pmatrix}.$$

We shall put the matrix A into reduced row echelon form by a sequence of elementary row operations.

1. Interchange rows 1 and 2, and obtain

$$A_1 = \begin{pmatrix} 1 & 4 & 13 \\ 3 & 13 & 37 \\ 2 & 14 & 14 \end{pmatrix}.$$

2. Add -3 times row 1 to row 2 and obtain

$$A_2 = \begin{pmatrix} 1 & 4 & 13 \\ 0 & 1 & -2 \\ 2 & 14 & 14 \end{pmatrix}.$$

3. Add -2 times row 1 to row 3 and obtain

$$A_3 = \begin{pmatrix} 1 & 4 & 13 \\ 0 & 1 & -2 \\ 0 & 6 & -12 \end{pmatrix}.$$

4. Add -4 times row 2 to row 1 and obtain

$$A_4 = \begin{pmatrix} 1 & 0 & 21 \\ 0 & 1 & -2 \\ 0 & 6 & -12 \end{pmatrix}.$$

5. Add -6 times row 2 to row 3 and obtain

$$A_5 = \begin{pmatrix} 1 & 0 & 21 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{pmatrix}.$$

This is the reduced row echelon matrix equivalent to A. Equivalently, the system of equations

$$\begin{cases} 3x + 13y = 37 \\ x + 4y \ = 13 \\ 2x + 14y = 14 \end{cases} \tag{2.10}$$

is equivalent to the system

$$x = 21$$
$$y = -2$$

and so the system of linear equations (2.10) has the unique solution $(x, y) = (21, -2)$.

Consider the matrix $A = \begin{pmatrix} 6 & 5 \\ 7 & 3 \end{pmatrix}$. Here is a sequence of elementary row operations that produces a row-equivalent matrix that is in reduced row echelon form:

$$\begin{pmatrix} 6 & 5 \\ 7 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & \frac{5}{6} \\ 7 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & \frac{5}{6} \\ 0 & \frac{1}{6} \end{pmatrix} \to \begin{pmatrix} 1 & \frac{5}{6} \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Here is a different sequence of elementary row operations that produces a reduced row echelon form matrix that is row-equivalent to A:

$$\begin{pmatrix} 6 & 5 \\ 7 & 3 \end{pmatrix} \to \begin{pmatrix} 6 & 5 \\ 1 & -2 \end{pmatrix} \to \begin{pmatrix} 0 & 17 \\ 1 & -2 \end{pmatrix} \to \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Notice that these different sequences of elementary row operations produce the same reduced row echelon form matrix. This always happens: If A is an $m \times n$ matrix and if A' and A'' are reduced row echelon form matrices obtained from A by different sequences of elementary row operations, that is, if A' and A'' are reduced row echelon form matrices that are row-equivalent to A, then $A' = A''$. This is Theorem 2.15 in Section 2.10 .

Exercises

Solve the following systems of linear equations by using elementary row operations to put the augmented matrix into reduced row echelon form.

1.

$$\begin{aligned} 9x \ - 4y &= 1 \\ -11x + 5y &= 3 \end{aligned}$$

2.
$$\begin{aligned} 8x + 3y &= 0 \\ 5x + 2y &= 1 \end{aligned}$$

3.
$$\begin{aligned} 6x - y &= -3 \\ 7x - 2y &= 6 \\ 8x - 3y &= 15 \end{aligned}$$

4.
$$\begin{aligned} x + 4y + 3z &= 2 \\ 2x + y + z &= 3 \\ 3x - 2y - z &= 4 \end{aligned}$$

5.
$$\begin{aligned} x + 4y + 3z &= 1 \\ 2x + y + z &= 3 \\ 3x - 2y - z &= 4 \end{aligned}$$

6.
$$\begin{aligned} x + 2y + 3z &= -8 \\ 4x + 5y + 6z &= -8 \\ 7x + 8y + 9z &= -8 \end{aligned}$$

7.
$$\begin{aligned} x + 2y + 3z &= 10 \\ 2x - 3y + 7z &= -9 \end{aligned}$$

8.
$$\begin{aligned} -4x + 6y - 9z &= 20 \\ 2x + 5y + 11z &= -15 \end{aligned}$$

9.
$$\begin{aligned} 2x + 3y \qquad &= 25 \\ x + y - z &= 9 \\ 4x - 5y - 22z &= -27 \\ 7x + 8y - 5z &= 70 \end{aligned}$$

10. a. Compute the reduced row echelon form of the matrix

$$A = \begin{pmatrix} 2 & 0 & 5 & -1 \\ 1 & -1 & 10 & 5 \\ 3 & 1 & 0 & -7 \end{pmatrix}$$

b. Compute the reduced row echelon form of the matrix

$$B = \begin{pmatrix} 2 & 1 & 3 \\ 0 & -1 & 1 \\ 5 & 10 & 0 \\ -1 & 5 & -7 \end{pmatrix}$$

c. Observe that B is the transpose of A, and that the row rank of A equals the row rank of B equals the column rank of A.

11. Compute the reduced row echelon form and the reduced column echelon form of the following matrices:

a.
$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & \\ 12 & & & \end{pmatrix}.$$

Solution: Reduced row echelon form:
$$\begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Reduced column echelon form:
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 2 & 0 & 0 \end{pmatrix}$$

b.
$$B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & \\ 12 & & & & & \end{pmatrix}.$$

Solution: Reduced row echelon form:
$$\begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Reduced column echelon form:
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2.7 A second proof of Theorem 1.6

We can use the reduced row echelon form of a matrix to give a second proof of Theorem 1.6. Let $m < n$. Consider the homogeneous system of m linear equations with n variables

$$a_{1,1}x_1 + \cdots a_{1,n}x_n = 0$$
$$\vdots$$
$$a_{m,1}x_1 + \cdots a_{m,n}x_n = 0$$

Associated to this system is its $m \times n$ matrix of coefficients $A = (a_{i,j})$. Applying a sequence of elementary row operations, we obtain a row-equivalent matrix $A' = (a'_{i,j})$ that is in reduced row echelon form. Let r denote the number of nonzero rows. Then $r \leq m < n$. For $i = 1, \ldots, r$, let k_i denote the column in which the first nonzero coordinate in row i appears. Let

$$J = \{1, \ldots, n\} \setminus \{k_1, \ldots, k_r\} = \{j_1, \ldots, j_{n-r}\} \neq \emptyset.$$

The homogeneous system is equivalent to the following homogeneous system of r linear equations in n variables:

$$\begin{cases} x_{1,k_1} + \sum_{j \in J} a'_{1,j} x_j &= 0 \\ \quad\vdots & \\ x_{i,k_i} + \sum_{j \in J} a'_{i,j} x_j &= 0 \\ \quad\vdots & \\ x_{r,k_i} + \sum_{j \in J} a'_{r,j} x_j &= 0 \end{cases}$$

Choosing $x_j = 1$ for $j \in J$ and $x_{k_i} = -\sum_{j \in J} a'_{i,j}$ for $i \in \{1, \ldots, r\}$, we obtain a nontrivial solution of the homogeneous system. This completes the second proof.

Theorem 2.13. *A homogeneous system of n linear equations in n variables has only the trivial solution if and only if the reduced row echelon form of the coefficient matrix of the system is the identity matrix I_n.*

Proof. An $n \times n$ matrix in reduced row echelon form has no nonzero rows if and only if the matrix is the identity matrix I_n. The only solution of the homogeneous system of linear equations derived from I_n is the trivial solution $x_1 = \cdots = x_n = 0$. If the reduced row matrix has a zero row, then the corresponding homogeneous system of equations is a system of m equations in n variables with $m < n$, and, by Theorem 1.6, has a nontrivial solution. This completes the proof.

Here is an example. Consider the following homogeneous system of two linear equations in three variables:

$$x + y + z + w = 0$$
$$x + 2y + 4z + 8w = 0.$$

Using elementary row operations, we row-reduce the coefficient matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 3 & 7 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -2 & -6 \\ 0 & 1 & 3 & 7 \end{pmatrix}$$

and obtain the equivalent homogeneous system

$$\begin{aligned} x - 2z - 6w &= 0 \\ y + 3z + 7w &= 0. \end{aligned}$$

It follows that $(x,y,z,w) = (2s+6t, -3s-7t, s, t)$ is a two-parameter solution of the linear system. Fox example, choosing $s = 2$ and $t = -1$, we obtain the solution $(x,y,z,w) = (-2,1,2,-1)$.

Recall that a *linear combination* of the column vectors $v_1, \ldots, v_n \in \mathbf{R}^n$ is a column vector of the form

$$c_1 v_1 + \cdots + c_n v_n$$

where $c_1, \ldots, c_n$ are scalars, that is, $c_1, \ldots, c_n \in \mathbf{R}$.

Consider the following system of m linear equations in n variables:

$$\left\{ \begin{array}{lllllllll} a_{1,1}x_1 & + & \cdots & + & a_{1,j}x_j & + \cdots + & a_{1,n}x_n & = & b_1 \\ \quad\vdots & & & & & & & & \\ a_{i,1}x_1 & + & \cdots & + & a_{i,j}x_j & + \cdots + & a_{i,n}x_n & = & b_i \\ \quad\vdots & & & & & & & & \\ a_{m,1}x_1 & + & \cdots & + & a_{m,j}x_j & + \cdots + & a_{m,n}x_n & = & b_m. \end{array} \right. \tag{2.11}$$

Define column vectors $v_1, \ldots, v_j, \ldots, v_n$, and b in $\mathbf{R}^m$ by

$$v_1 = \begin{pmatrix} a_{1,1} \\ \vdots \\ a_m, 1 \end{pmatrix}, \ldots, v_j = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_m, j \end{pmatrix}, \ldots, v_n = \begin{pmatrix} a_{1,1} \\ \vdots \\ a_m, 1 \end{pmatrix}, b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}, \tag{2.12}$$

Every sequence of scalars $x_1, \ldots, x_n$ determines a linear combination of column vectors

$$x_1 v_1 + \cdots + x_n v_n = \begin{pmatrix} a_{1,1}x_1 + \cdots + a_{1,j}x_j + \cdots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,j}x_j + \cdots + a_{m,n}x_n \end{pmatrix}.$$

The vector equation

$$x_1 v_1 + \cdots + x_n v_n = b$$

is equivalent to the vector identity

$$\begin{pmatrix} a_{1,1}x_1 + \cdots + a_{1,j}x_j + \cdots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,j}x_j + \cdots + a_{m,n}x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

Because column vectors are equal if and only if they have the same coordinates, the vector identity is equivalent to the system (2.5) of linear equations.

Conversely, every sequence of $n+1$ column vectors in $\mathbf{R}^m$ determines a system of m linear equations in n variables. If $v_1, \ldots, v_n$ and b are column vectors in $\mathbf{R}^m$ with coordinates (2.12), then the vector equation $x_1 v_1 + \cdots + x_n v_n = b$ defines the system (2.5) of linear equations.

If the system (2.5) of linear equations is homogeneous, that is, if $b_i = 0$ for $i = 1, \ldots, m$, then the column vector $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{R}^n$ is a solution of the system if and only if

$$x_1 v_1 + \cdots + x_n v_n = 0. \tag{2.13}$$

In this vector equation, 0 is the zero vector, that is, the vector each of whose coordinates is the scalar 0.

The vectors $v_1, \ldots, v_n$ in $\mathbf{R}^m$ are *linearly dependent* if there exist scalars $x_1, \ldots, x_n$ not all 0 that satisfy the vector equation (2.13). The vectors $v_1, \ldots, v_n$ in $\mathbf{R}^m$ are *linearly independent* if the only solution of the vector equation (2.13) is $x_i = 0$ for all $i = 1, \ldots, n$. It follows that the homogeneous system of linear equations

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,j}x_j + \cdots + a_{1,n}x_n = 0 \\ \quad\vdots \\ a_{m,1}x_1 + \cdots + a_{m,j}x_j + \cdots + a_{m,n}x_n = 0 \end{cases}$$

has a nonzero solution if and only if the column vectors $v_1, \ldots, v_n$ defined by (2.12) are linearly dependent in $\mathbf{R}^m$.

Exercises

Find all solutions of the following homogeneous systems of linear equations.

1.
$$\begin{cases} x + 3y + 2z = 0 \\ 2x + 7y - 3z = 0 \end{cases}$$

2.
$$\begin{cases} -4x + 6y - 9z = 0 \\ 2x + 5y + 11z = 0 \end{cases}$$

3.
$$\begin{cases} 7x - y + 3z = 0 \\ 2x + y - z = 0 \end{cases}$$

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

5.

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

6.

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

2.8 Elementary matrices and reduced row echelon form

An $n \times n$ *elementary matrix* is a matrix obtained from the identity matrix by applying one elementary row operation. There are three elementary row operations, and so there are three types of elementary matrices.

1. Interchanging two rows of the identity matrix yields an elementary matrix.
2. Multiplying one row of the identity matrix by a nonzero number yields an elementary matrix.
3. Adding a multiple of one row of the identity matrix to another row yields an elementary matrix..

Note that the identity matrix is also an elementary matrix.

Lemma 2.4. *Every elementary matrix is invertible.*

Proof. Every elementary row operation can be inverted by another elementary row operation, and so every elementary matrix is invertible.

.

Here are the 2×2 elementary matrices and their inverses (with $c \neq 0$):

E	E^{-1}	E	E^{-1}
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} c^{-1} & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & c^{-1} \end{pmatrix}$
$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix}$

The elementary row operations on a matrix can be described by multiplication on the left by an elementary matrix. This means that if A is an $m \times n$ matrix and if A' is an $m \times n$ matrix obtained from A by an elementary row operation, then there is a unique $m \times m$ elementary matrix E such that $EA = A'$.

1. If E is the $m \times m$ elementary matrix obtained by interchanging rows k and ℓ of the identity matrix I_m, then EA is the matrix obtained from A by interchanging rows k and ℓ. Moreover, $E^{-1} = E$.
2. If E is the $m \times m$ elementary matrix obtained from I_m by multiplying row k by the nonzero number c, then EA is the matrix obtained from A by multiplying row k by the nonzero number c. Moreover, E^{-1} is the $m \times m$ elementary matrix obtained from I_m by multiplying row k by the nonzero number c^{-1}.
3. Let E be the $m \times m$ elementary matrix obtained from I_m by replacing row ℓ with row ℓ plus row k multiplied by the number c. Then EA is the matrix obtained from A by replacing row ℓ with row ℓ plus row k multiplied by the number c. Moreover, E^{-1} is the $m \times m$ elementary matrix obtained from I_m by replacing row ℓ with row ℓ plus row k multiplied by the number $-c$.

For example, let $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, and consider the 2×2 elementary matrices

$$E_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 0 \\ 0 & -5 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}.$$

The elementary matrix E_1 interchanges rows 1 and 2:

$$E_1 A = \begin{pmatrix} 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix}.$$

The elementary matrix E_2 multiplies row 2 by -5:

$$E_2 A = \begin{pmatrix} 1 & 2 & 3 \\ -20 & -25 & -30 \end{pmatrix}.$$

The elementary matrix E_3 add 7 times row 2 to row 1:

$$E_3 A = \begin{pmatrix} 29 & 37 & 45 \\ 4 & 5 & 6 \end{pmatrix}.$$

An $m \times n$ matrix is in *reduced row echelon form* (also called *row canonical form*) if it satisfies the following properties:

1. If there are r nonzero rows and $n - r$ zero rows, then the zero rows are below the nonzero rows, that is, the nonzero rows are rows $1, 2, \ldots, r$, and the zero rows are rows $r+1, r+2, \ldots, m$.
2. In each nonzero row, the first (that is, the leftmost) nonzero coordinate is 1.
3. If there are r nonzero rows and if the leftmost 1 in row i is in column k_i, then $k_1 < k_2 < \cdots < k_r$.
4. If the leftmost coordinate 1 in the nonzero row i is in column k_i, then every other coordinate in column k_i is 0, that is, $a_{\ell,k_i} = 0$ for all $\ell \neq i$.

Equivalently, the $m \times n$ matrix $A = (a_{i,j})$ is in reduced row echelon form if there is a nonnegative integer $r \leq m$ and a strictly increasing sequence of integers

$$1 \leq k_1 < k_2 < \cdots < k_r \leq n$$

such that

$$\begin{aligned} a_{i,k_i} &= 1 \quad \text{for } i = 1, \ldots, r \\ a_{\ell,k_i} &= 0 \quad \text{for } i = 1, \ldots, r \text{ and } \ell \neq i \\ a_{i,j} &= 0 \quad \text{if } i = 1, \ldots, r \text{ and } j < k_i \\ a_{i,j} &= 0 \quad \text{if } i = r+1, \ldots, m \text{ and } j = 1, \ldots, n. \end{aligned}$$

The sequence of strictly increasing integers $k_1 < k_2 < \cdots < k_r$ is called the sequence of *pivot numbers* of the reduced row echelon form. The *pivot columns* of the matrix A are the r columns $\mathrm{col}_{k_j}(A)$ for $j \in \{1, \ldots, r\}$.

For example, the following 5×8 matrix is in reduced row echelon form with $r = 3$ and pivot numbers $k_1 = 2$, $k_2 = 4$, and $k_3 = 7$:

$$\begin{pmatrix} 0 & 1 & 3 & 0 & 5 & 6 & 0 & 4 \\ 0 & 0 & 0 & 1 & 9 & 2 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Recall that $m \times n$ matrices A and B are row-equivalent if a finite sequence of elementary row operations applied to the matrix A produces the matrix B. Thus, matrices A and B are row-equivalent if there exists a finite sequence $E_1, E_2, \ldots, E_\ell$ of elementary matrices such that

$$E_\ell \cdots E_2 E_1 A = B.$$

Because every elementary matrix is invertible, it follows that the matrix $E_\ell \cdots E_2 E_1$ is invertible.

Theorem 2.14. *Every matrix is row-equivalent to a reduced row echelon matrix.*

Proof. If A is the zero matrix, then A is in reduced row echelon form.

Let $A = (a_{i,j})$ be a nonzero $m \times n$ matrix. The first pivot number k_1 is the least integer such that $a_{i,k_1} \neq 0$ for some i. If $i \neq 1$, then interchange rows 1 and i, and obtain a matrix $A' = (a'_{i,j})$ such that $a'_{1,k_1} \neq 0$ and $a'_{i,j} = 0$ for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, k_1 - 1\}$

If $a'_{1,k_1} \neq 1$, then multiply row 1 by a^{-1}_{1,k_1} and obtain a matrix $A'' = (a''_{i,j})$ with $a''_{i,j} = 0$ if $j < k_1$ and $a''_{1,k_1} = 1$. For $i = 2, \ldots, m$, if $a''_{i,k_1} \neq 0$, then add $-a''_{i,k_1}$ times row 1 to row i. We obtain the $m \times n$ matrix $B = (b_{i,j})$ with $b_{i,j} = 0$ if $j < k_1$, $b_{1,k_1} = 1$, and $b_{i,k_1} = 0$ for $i = 2, \ldots, m$.

If $b_{i,j} \neq 0$ for some $i \geq 2$, then the second pivot number k_2 is the least integer such that $b_{i,k_2} \neq 0$ for some $i \geq 2$. Then $k_2 > k_1$. If $i \neq 2$, then interchange rows 2 and i, and obtain a matrix $B' = (b'_{i,j})$ such that $b'_{2,k_2} \neq 0$ and $b'_{i,j} = 0$ if $i \geq 2$ and $j < k_2$. If $b'_{2,k_2} \neq 1$, then multiply row 2 by b^{-1}_{2,k_2} and obtain a matrix $B'' = (b''_{i,j})$ with

$b''_{2,k_2} = 1$ and $b''_{i,j} = 0$ if $i \geq 2$ and $j < k_2$. For $i = 1, 3, 4, \ldots, m$, if $b''_{i,k_2} \neq 0$, then add $-b''_{i,k_2}$ times row 2 to row i. We obtain an $m \times n$ matrix $C = (c_{i,j})$ such that

$$c_{i,j} = \begin{cases} 1 & \text{if } (i,j) = (1,k_1) \text{ or } (2,k_2) \\ 0 & \text{if } (i,j) = (i,k_1) \text{ and } i \neq 1 \\ 0 & \text{if } (i,j) = (i,k_2) \text{ and } i \neq 2 \\ 0 & \text{if } i = 1,\ldots,n \text{ and } j < k_1 \\ 0 & \text{if } i = 2,\ldots,n \text{ and } k_1 < j < k_2. \end{cases}$$

Continuing inductively, by a finite sequence of elementary row operations, we obtain a matrix in reduced row echelon form with pivot numbers $k_1 < k_2 < \cdots < k_r$. This completes the proof.

Here is an example. Consider the 3×3 matrix

$$A = \begin{pmatrix} 3 & 13 & 37 \\ 1 & 4 & 13 \\ 2 & 14 & 14 \end{pmatrix}.$$

We shall put the matrix A into reduced row echelon form in two ways: First, by a sequence of elementary row operations, and, second, by multiplying by the corresponding sequence of elementary matrices.

1. Interchange rows 1 and 2, and obtain

$$A_1 = \begin{pmatrix} 1 & 4 & 13 \\ 3 & 13 & 37 \\ 2 & 14 & 14 \end{pmatrix}.$$

2. Add -3 times row 1 to row 2 and obtain

$$A_2 = \begin{pmatrix} 1 & 4 & 13 \\ 0 & 1 & -2 \\ 2 & 14 & 14 \end{pmatrix}.$$

3. Add -2 times row 1 to row 3 and obtain

$$A_3 = \begin{pmatrix} 1 & 4 & 13 \\ 0 & 1 & -2 \\ 0 & 6 & -12 \end{pmatrix}.$$

4. Add -4 times row 2 to row 1 and obtain

$$A_4 = \begin{pmatrix} 1 & 0 & 21 \\ 0 & 1 & -2 \\ 0 & 6 & -12 \end{pmatrix}.$$

5. Add -6 times row 2 to row 3 and obtain

$$A_5 = \begin{pmatrix} 1 & 0 & 21 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{pmatrix}.$$

This is the reduced row echelon matrix equivalent to A.

We repeat the reduction process using elementary matrices.

1. We interchange rows 1 and 2 by multiplying A by the elementary matrix
$$E_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$
Then $A_1 = E_1 A$.
2. We add -3 times row 1 to row 2 by multiplying A_1 by the elementary matrix
$$E_2 = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$
Then $A_2 = E_2 A_1 = E_2 E_1 A$.
3. We add -2 times row 1 to row 3 by multiplying A_2 by the elementary matrix
$$E_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix}.$$
Then $A_3 = E_3 A_2 = E_3 E_2 E_1 A$.
4. We add -4 times row 2 to row 1 by multiplying A_3 by the elementary matrix
$$E_4 = \begin{pmatrix} 1 & -4 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$
Then $A_4 = E_4 A_3 = E_4 E_3 E_2 E_1 A$.
5. We add -6 times row 2 to row 3 by multiplying A_4 by the elementary matrix
$$E_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -6 & 1 \end{pmatrix}.$$
Then $A_5 = E_5 A_4 = E_5 E_4 E_3 E_2 E_1 A$.

The product of the five elementary matrices is

$$S = E_5 E_4 E_3 E_2 E_1 = \begin{pmatrix} -4 & 13 & 0 \\ 1 & -3 & 0 \\ -6 & 16 & 1 \end{pmatrix}$$

and

$$SA = \begin{pmatrix} -4 & 13 & 0 \\ 1 & -3 & 0 \\ -6 & 16 & 1 \end{pmatrix} \begin{pmatrix} 3 & 13 & 37 \\ 1 & 4 & 13 \\ 2 & 14 & 14 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 21 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Lemma 2.5. *Let A be an $n \times n$ matrix, and let R be an $n \times n$ matrix in reduced row echelon form that is row equivalent to A. The matrix A is invertible if and only if $R = I$.*

Proof. There exist elementary matrices $E_1, \ldots, E_\ell$ such that

$$R = E_\ell \cdots E_1 A.$$

The matrix $S = E_k \cdots E_1$ is a product of elementary matrices. Because elementary matrices are invertible, the matrix S is also invertible, and $SA = R$. If $R = I$, then $SA = I$ and $A = S^{-1}$ is invertible.

Conversely, if A is invertible, then $R = SA$ is a product of invertible matrices, and so R is an invertible $n \times n$ matrix in reduced row echelon form. If $R \neq I$, then the nth row of R is the zero row. This implies that, for every matrix M, the rth row of RM is the zero row, and so R is not invertible. Therefore, $R = I$. This completes the proof.

Let us consider again a system of n linear equations in n variables:

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = b_2 \\ \quad \vdots \\ a_{n,1}x_1 + a_{n,j}x_j + \cdots + a_{n,n}x_n = b_n \end{cases} \tag{2.14}$$

The $n \times n$ matrix of coefficients of this system is

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}. \tag{2.15}$$

We introduce the column vectors

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad \text{and} \quad \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}. \tag{2.16}$$

A solution of the system of equations (2.14) is equivalent to a solution of the vector equation $A\mathbf{x} = \mathbf{b}$.

Lemma 2.6. *Let A be an $n \times n$ matrix. The following are equivalent:*

(i) For every n-dimensional column vector $\mathbf{b}$*, the equation* $A\mathbf{x} = \mathbf{b}$ *has a unique solution* $\mathbf{x}$*.*
(ii) The equation $A\mathbf{x} = 0$ *has only the zero solution* $\mathbf{x} = 0$*.*
(iii) The matrix A is invertible.

Proof. The n-dimensional column vector $\mathbf{0}$ is always a solution of the vector equation $A\mathbf{x} = \mathbf{0}$. If, for every column vector $\mathbf{b}$, the system of linear equations $A\mathbf{x} = \mathbf{b}$ has a unique solution, then, in particular, the homogeneous system of equations $A\mathbf{x} = \mathbf{0}$ has only the zero solution. Thus, (i) implies (ii).

Let R be a reduced row echelon matrix that is row equivalent to A, and let S be an invertible matrix such that $SA = R$. If $R \neq I$, then the nth row of R is nonzero. Let R' be the $(n-1) \times n$ matrix consisting of the first $n-1$ rows of R. The vector equation $R'x = \mathbf{0}$ corresponds to a homogeneous system of $n-1$ linear equations in n variables. By Theorem 1.6, this system has a nonzero solution, and so there exists a nonzero n-dimensional vector $\mathbf{x}$ such that $R'\mathbf{x} = \mathbf{0}$. Because the nth row of R is the zero row, we also have $R\mathbf{x} = \mathbf{0}$. Therefore, $A\mathbf{x} = S^{-1}R\mathbf{x} = \mathbf{0}$. Thus, if $R \neq I$, then $A\mathbf{x} = \mathbf{0}$ has a nonzero solution, which contradicts (ii). It follows that $R = I$, and so, by Lemma 2.5, the matrix A is invertible. Thus, (ii) implies (iii).

Let $A\mathbf{x} = \mathbf{b}$. If A is invertible, then

$$\mathbf{x} = A^{-1}A\mathbf{x} = A^{-1}\mathbf{b}$$

and so the vector equation $A\mathbf{x} = \mathbf{b}$ has a unique solution. Thus, (iii) implies (i). This completes the proof.

Lemma 2.6 is equivalent to the following statement about systems of linear equations.

Lemma 2.7. *Consider the system* (2.14) *of n linear equations in n variables, and define the matrix A by* (2.15) *and the vectors* $\mathbf{x}$ *and* $\mathbf{b}$ *by* (2.16)*. The following are equivalent:*

(i) For every column vector $\mathbf{b}$*, the inhomogeneous system of equations* $A\mathbf{x} = \mathbf{b}$ *has a unique solution* $\mathbf{x}$*.*
(ii) The homogeneous system of equations $A\mathbf{x} = \mathbf{0}$ *has only the zero solution* $\mathbf{x} = \mathbf{0}$*.*
(iii) The matrix A is invertible.

Lemma 2.8. *Let A be an* $n \times n$ *matrix. The following are equivalent:*

(i) A is invertible.
(ii) A has a left inverse.
(iii) A has a right inverse.

Proof. If A is invertible, then the inverse of A is both a left inverse and a right inverse of A.

Let B be a left inverse of A. Thus, $BA = I$. If $\mathbf{x}$ is a solution of the homogeneous system of linear equations $A\mathbf{x} = \mathbf{0}$, then

$$\mathbf{x} = I\mathbf{x} = BA\mathbf{x} = B\mathbf{0} = \mathbf{0}.$$

It follows from Lemma 2.6 that A is invertible, and so A has a right inverse.

Suppose that C is a right inverse of A. Then $AC = I$, and A is a left inverse of C. It follows that C is invertible, and so $A = C^{-1}$ is invertible. This completes the proof.

Lemma 2.9. *Let $A_1, \ldots, A_\ell$ be $n \times n$ matrices. If the product matrix $A_1 \cdots A_\ell$ is invertible, then A_i is invertible for all $i = 1, \ldots, \ell$.*

Proof. The proof is by induction on ℓ. If $A = A_1 \cdots A_\ell$ is invertible, then

$$I = A^{-1}A = \left(A^{-1}A_1 \cdots A_{\ell-1}\right) A_\ell$$

and so $A^{-1}A_1 \cdots A_{\ell-1}$ is a left inverse of A_ℓ. By Lemma 2.8, the matrix A_ℓ is invertible and so $A_1 \cdots A_{\ell-1} = AA_\ell^{-1}$ is invertible. Continuing inductively, it follows that A_i is invertible for all $i = 1, \ldots, \ell$. This completes the proof.

Exercises

1. Consider the elementary matrices

$$E_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad E_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$E_3 = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad E_4 = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

   a. Compute the inverse of each of these matrices.
   b. Show that $E_iE_j \neq E_jE_i$ for all $i \neq j$.

2. Write each of the following matrices as a product of elementary matrices:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 4 & 5 & 6 \end{pmatrix}$$

2.9 An algorithm to compute the inverse of a matrix

Let A be an $n \times n$ matrix, and let R be a matrix in reduced row echelon form that is row-equivalent to A. We can construct the matrix R by a sequence of elementary row operations on A, or, equivalently, by multiplying A on the left by a sequence of elementary matrices $E_1, \ldots, E_\ell$. If $S = E_\ell \cdots E_2E_1$, then

$$SA = E_\ell \cdots E_1 A = R. \tag{2.17}$$

Because

$$S = SI_n = E_\ell \cdots E_1 I_n$$

we can produce the matrix S by performing on the identity matrix I_n exactly the same sequence of elementary row operations that we perform on A to obtain R.

An algorithm to compute S is as follows: If A is an $n \times n$ matrix, then construct the $n \times 2n$ matrix $A^\sharp$ whose left half is A and whose right half is I_n. We draw a vertical line to separate the left and right halves of the matrix:

$$A^\sharp = \left(A \mid I \right)$$

For example, if

$$A = \begin{pmatrix} 5 & 7 \\ 2 & 3 \end{pmatrix}$$

then

$$A^\sharp = \left(\begin{array}{cc|cc} 5 & 7 & 1 & 0 \\ 2 & 3 & 0 & 1 \end{array} \right).$$

Applying a sequence of elementary row operations to $A^\sharp$ that reduces the left half to the reduced row echelon form $n \times n$ matrix R will produce the $n \times n$ matrix S in the right half. Equivalently, if $SA = R$, then

$$SA^\sharp = S\left(A \mid I \right) = \left(SA \mid S \right) = \left(R \mid S \right).$$

By Lemma 2.5, if the $n \times n$ matrix A is invertible, then a reduced row echelon form matrix R equivalent to A must be the identity matrix I, and so

$$SA^\sharp = \left(SA \mid S \right) = \left(I \mid S \right)$$

and $S = A^{-1}$. This gives an algorithm to compute the matrix A^{-1} if it exists.

Here are three examples.

Example 1: Let $A = \begin{pmatrix} 5 & 7 \\ 2 & 3 \end{pmatrix}$. Applying elementary row operations to $A^\sharp$, we obtain

$$\begin{aligned} A^\sharp = \left(\begin{array}{cc|cc} 5 & 7 & 1 & 0 \\ 2 & 3 & 0 & 1 \end{array} \right) &\to \left(\begin{array}{cc|cc} 1 & 7/5 & 1/5 & 0 \\ 2 & 3 & 0 & 1 \end{array} \right) \to \left(\begin{array}{cc|cc} 1 & 7/5 & 1/5 & 0 \\ 0 & 1/5 & -2/5 & 1 \end{array} \right) \\ &\to \left(\begin{array}{cc|cc} 1 & 7/5 & 1/5 & 0 \\ 0 & 1 & -2 & 5 \end{array} \right) \to \left(\begin{array}{cc|cc} 1 & 0 & 3 & -7 \\ 0 & 1 & -2 & 5 \end{array} \right). \end{aligned}$$

The left half of this 2×4 matrix is I_2, and so A is invertible. The right half of the 2×4 matrix gives $A^{-1} = \begin{pmatrix} 3 & -7 \\ -2 & 5 \end{pmatrix}$. To check that this is correct, we compute

$$A\,A^{-1} = \begin{pmatrix} 5 & 7 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 3 & -7 \\ -2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

Example 2. Let $A = \begin{pmatrix} 2 & -3 & 0 \\ 0 & -1 & 4 \\ 6 & 1 & 0 \end{pmatrix}$. Row reducing $A^\sharp$, we obtain

$$A^\sharp = \left(\begin{array}{ccc|ccc} 2 & -3 & 0 & 1 & 0 & 0 \\ 0 & -1 & 4 & 0 & 1 & 0 \\ 6 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & -3/2 & 0 & 1/2 & 0 & 0 \\ 0 & -1 & 4 & 0 & 1 & 0 \\ 6 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$
$$\to \left(\begin{array}{ccc|ccc} 1 & -3/2 & 0 & 1/2 & 0 & 0 \\ 0 & -1 & 4 & 0 & 1 & 0 \\ 0 & 10 & 0 & -3 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & -3/2 & 0 & 1/2 & 0 & 0 \\ 0 & 1 & -4 & 0 & -1 & 0 \\ 0 & 10 & 0 & -3 & 0 & 1 \end{array}\right)$$
$$\to \left(\begin{array}{ccc|ccc} 1 & 0 & -6 & 1/2 & -3/2 & 0 \\ 0 & 1 & -4 & 0 & -1 & 0 \\ 0 & 10 & 0 & -3 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & 0 & -6 & 1/2 & -3/2 & 0 \\ 0 & 1 & -4 & 0 & -1 & 0 \\ 0 & 0 & 40 & -3 & 10 & 1 \end{array}\right)$$
$$\to \left(\begin{array}{ccc|ccc} 1 & 0 & -6 & 1/2 & -3/2 & 0 \\ 0 & 1 & -4 & 0 & -1 & 0 \\ 0 & 0 & 1 & -3/40 & 1/4 & 1/40 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1/20 & 0 & 3/20 \\ 0 & 1 & -4 & 0 & -1 & 0 \\ 0 & 0 & 1 & -3/40 & 1/4 & 1/40 \end{array}\right)$$
$$\to \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1/20 & 0 & 3/20 \\ 0 & 1 & 0 & -3/10 & 0 & 1/10 \\ 0 & 0 & 1 & -3/40 & 1/4 & 1/40 \end{array}\right).$$

It follows that A is invertible and that the right half of this 3×6 matrix is

$$A^{-1} = \begin{pmatrix} 1/20 & 0 & 3/20 \\ -3/10 & 0 & 1/10 \\ -3/40 & 1/4 & 1/40 \end{pmatrix}.$$

We can check that

$$AA^{-1} = \begin{pmatrix} 2 & -3 & 0 \\ 0 & -1 & 4 \\ 6 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1/20 & 0 & 3/20 \\ -3/10 & 0 & 1/10 \\ -3/40 & 1/4 & 1/40 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Example 3. If $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$, then $A^\sharp = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 9 & 0 & 0 & 1 \end{array}\right)$. Row reducing $A^\sharp$, we obtain

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 9 & 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 7 & 8 & 9 & 0 & 0 & 1 \end{array}\right)$$
$$\to \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & -6 & -12 & -7 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 4/3 & -1/3 & 0 \\ 0 & -6 & -12 & -7 & 0 & 1 \end{array}\right)$$
$$\to \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & -5/3 & 2/3 & 0 \\ 0 & 1 & 2 & 4/3 & -1/3 & 0 \\ 0 & -6 & -12 & -7 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & -5/3 & 2/3 & 0 \\ 0 & 1 & 2 & 4/3 & -1/3 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right).$$

Because the left half of the final 3×6 matrix is not the identity, it follows that A is not invertible, that A is row-equivalent to the reduced row echelon form matrix

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

and that $SA = R$, where

$$S = \begin{pmatrix} -5/3 & 2/3 & 0 \\ 4/3 & -1/3 & 0 \\ 1 & -2 & 1 \end{pmatrix}.$$

Check:

$$SA = \begin{pmatrix} -5/3 & 2/3 & 0 \\ 4/3 & -1/3 & 0 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} = R.$$

Exercises

1. Use the algorithm in this section to compute the inverses of the following matrices:

   a.
   $$\begin{pmatrix} 3 & 2 \\ -8 & -5 \end{pmatrix}$$

   b.
   $$\begin{pmatrix} 7 & -9 \\ 3 & -4 \end{pmatrix}$$

   c.
   $$\begin{pmatrix} 7 & 9 \\ 3 & -4 \end{pmatrix}$$

2. Use the algorithm in this section to compute the inverses of the following matrices:

a.
$$\begin{pmatrix} 7 & 0 & 2 \\ 0 & 5 & 1 \\ 2 & 2 & 1 \end{pmatrix}$$

b.
$$\begin{pmatrix} 1 & 0 & 3 \\ 2 & 1 & 5 \\ -4 & 1 & 7 \end{pmatrix}.$$

c.
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}.$$

3.
$$\begin{pmatrix} 1 & 3 & 0 & 2 \\ 0 & 5 & 2 & 5 \\ -1 & 0 & 1 & 3 \\ -2 & -6 & 0 & 1 \end{pmatrix}.$$

Solutions

1. a.
$$\begin{pmatrix} 3 & 2 \\ -8 & -5 \end{pmatrix}^{-1} = \begin{pmatrix} -5 & -2 \\ 8 & 3 \end{pmatrix}.$$

b.
$$\begin{pmatrix} 7 & -9 \\ 3 & -4 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & -9 \\ 3 & -7 \end{pmatrix}.$$

c.
$$\begin{pmatrix} 7 & 9 \\ 3 & -4 \end{pmatrix}^{-1} = \frac{1}{55}\begin{pmatrix} 4 & 9 \\ 3 & -7 \end{pmatrix}.$$

2. a.
$$\begin{pmatrix} 7 & 0 & 2 \\ 0 & 5 & 1 \\ 2 & 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 4 & -10 \\ 2 & 3 & -7 \\ -10 & -14 & 35 \end{pmatrix}.$$

b.
$$\begin{pmatrix} 1 & 0 & 3 \\ 2 & 1 & 5 \\ -4 & 1 & 7 \end{pmatrix}^{-1} = \frac{1}{20}\begin{pmatrix} 2 & 3 & -3 \\ -34 & 19 & 1 \\ 6 & -1 & 1 \end{pmatrix}.$$

c.
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \frac{1}{18}\begin{pmatrix} -5 & 7 & 1 \\ 1 & -5 & 7 \\ 7 & 1 & -5 \end{pmatrix}.$$

3.
$$\begin{pmatrix} 1 & 3 & 0 & 2 \\ 0 & 5 & 2 & 5 \\ -1 & 0 & 1 & 3 \\ -2 & -6 & 0 & 1 \end{pmatrix}^{-1} = -\frac{1}{5}\begin{pmatrix} -1 & -15 & 30 & -13 \\ 0 & 5 & -10 & 5 \\ 5 & -15 & 25 & -10 \\ -2 & 0 & 0 & -1 \end{pmatrix}$$

2.10 Uniqueness of the reduced row echelon form of a matrix

In this section we shall prove that every matrix is row-equivalent to a unique matrix that is in reduced row echelon form.

Theorem 2.15. *Let A be an $m \times n$ matrix. If R and R' are $m \times n$ matrices in reduced row echelon form that are row-equivalent to A, then $R = R'$.*

Proof. Let A be an $m \times n$ matrix, and let R and R' be matrices in reduced row echelon form that are row equivalent to A. Because the matrix A is row-equivalent to both R and R', the transitivity of row-equivalence implies that the matrices R and R' are row-equivalent. It follows that there is an invertible $m \times m$ matrix $T = (t_{i,j})$ such that $R' = TR$ and $R = T^{-1}R'$. In particular, R is the zero matrix if and only if R' is the zero matrix. Thus, we can assume that R and R' are nonzero matrices, and so $r \geq 1$ and $r' \geq 1$.

Let $k_1 < \cdots < k_r$ be the pivot numbers of R, and let $k'_1 < \cdots < k'_{r'}$ be the pivot numbers of R'. It follows that $\mathrm{row}_i(R)$ is the zero row for $i \in \{r+1, r+2, \ldots, m\}$ and $\mathrm{row}_i(R')$ is the zero row for $i \in \{r'+1, r'+2, \ldots, m\}$. Let

$$\mathbf{x} = \sum_{i=1}^{m} c_i \,\mathrm{row}_i(R) = \sum_{i=1}^{r} c_i \,\mathrm{row}_i(R) = (x_1, \ldots, x_n)$$

be a linear combination of the rows of R. In the n-dimensional row vector $\mathbf{x}$, The definition of pivot number implies that $x_{k_i} = c_i$ for all $i \in \{1, \ldots, r\}$.

We begin by proving that $r = r'$ and $k_i = k'_i$ for $i = 1, \ldots, r$.

Let $r \leq r'$. By definition of the pivot number k_1, the first $k_1 - 1$ columns of R are zero columns, and so the first $k_1 - 1$ coordinates of every linear combination of the rows of R are 0. Because the first row of matrix R' is a linear combination of the rows of R, it follows that the first $k_1 - 1$ coordinates of $\mathrm{row}_1(R')$ are 0. Because coordinate k'_1 of $\mathrm{row}_1(R')$ is 1, we have $k'_1 \geq k_1$. Similarly, $k_1 \leq k'_1$, and so $k_1 = k'_1$.

Let $2 \leq \ell \leq r$, and suppose that $k_i = k'_i$ for $i = 1, \ldots, \ell - 1$. Because $R' = TR$, every row of R' is a linear combination of the rows of R. In particular,

$$\mathrm{row}_\ell(R') = \sum_{i=1}^{m} t_{\ell,i} \,\mathrm{row}_i(R) = \sum_{i=1}^{r} t_{\ell,i} \,\mathrm{row}_i(R)$$

and coordinate k_i in $\mathrm{row}_\ell(R')$ is $t_{\ell,i}$ for $i \in \{1, \ldots, r\}$.

The induction hypothesis implies that coordinates $k_1, \ldots, k_{\ell-1}$ in $\mathrm{row}_\ell(R')$ are 0, and so $t_{\ell,i} = 0$ for $i \in \{1, \ldots, \ell - 1\}$. Therefore,

$$\text{row}_\ell(R') = \sum_{i=\ell}^{r} t_{\ell,i}\,\text{row}_i(R). \tag{2.18}$$

In $\text{row}_\ell(R')$, the first nonzero coordinate is the 1 in position k'_ℓ. In $\text{row}_i(R)$, the first nonzero coordinate is the 1 in position k_i. In $\sum_{i=\ell}^{r} t_{\ell,i}\,\text{row}_i(R)$, the first nonzero coordinate is in position j for some $j \geq k_\ell$, and so $k'_\ell \geq k_\ell$. Similarly, $k_\ell \geq k'_\ell$ and so $k_\ell = k'_\ell$. It follows by induction that $k_i = k'_i$ for all $i \in \{1,\ldots,r\}$.

We have

$$\text{row}_{r+1}(R') = \sum_{i=1}^{r} t_{r+1,i}\,\text{row}_i(R).$$

The k_ith coordinate of $\text{row}_{r+1}(R')$ is 0 for $i \in \{1,\ldots,r\}$, and so $t_{r+1,i} = 0$ for $i \in \{1,\ldots,r\}$. Therefore, $\text{row}_{r+1}(R)$ is the zero row, and $r = r'$.

Next we prove that $\text{row}_\ell(R) = \text{row}_\ell(R')$ for all $\ell \in \{1,\ldots,r\}$. For $i \in \{1,\ldots,r\}$, the k_ith coordinate in the row vector $\sum_{i=\ell}^{r} t_{\ell,i}\,\text{row}_i(R)$ is $t_{\ell,i}$. For $i \neq \ell$, the k_ith coordinate in the row vector $\text{row}_\ell(R')$ is 0. It follows from (2.18) that $t_{\ell,i} = 0$ for $i \neq \ell$. The k_ℓth coordinate of $\text{row}(R)_\ell$ is 1, and so $t_{\ell,\ell} = 1$. Therefore, $\text{row}_\ell(R) = \text{row}(R')_\ell$. This completes the proof.

The *row rank* of an $m \times n$ matrix A is the number of nonzero rows in the reduced row echelon matrix that is row-equivalent to A. By Theorem 2.15, the row rank of a matrix is well-defined.

For every ordered pair (m,n) of positive integers, there are only finitely many shapes of reduced row echelon form $m \times n$ matrices. For example, there are exactly two 1×1 reduced row echelon form matrices:

$$\begin{pmatrix} 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 \end{pmatrix}.$$

There are exactly three shapes of 1×2 reduced row echelon form matrices:

$$\begin{pmatrix} 1 & c \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 \end{pmatrix}.$$

There are exactly four shapes of 2×2 reduced row echelon form matrices:

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

There are exactly seven shapes of 2×3 reduced row echelon form matrices:

$$\begin{pmatrix} 1 & 0 & c_1 \\ 0 & 1 & c_2 \end{pmatrix} \qquad \begin{pmatrix} 1 & c_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & c_1 & c_2 \\ 0 & 0 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 & c_1 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Exercises

1. Compute the number of pairwise distinct shapes of $1 \times n$ reduced row echelon form matrices for every positive integer n.
2. Compute the number of pairwise distinct shapes of $2 \times n$ reduced row echelon form matrices for $n = 1, 2, 3, 4$.
3. Prove that there are $1 + (n^2 + n)/2$ pairwise distinct shapes of $2 \times n$ reduced row echelon form matrices is for every positive integer n.
4. Compute the number of pairwise distinct shapes of $m \times 2$ reduced row echelon form matrices for $m = 3, 4, 5, 6$.
5. Compute the number of pairwise distinct shapes of $m \times 3$ reduced row echelon form matrices for $m = 2, 3, 4, 5$.
6. Let $f(m,n)$ denote the number pairwise distinct shapes of $m \times n$ reduced row echelon form matrices. Prove that $f(m,n) = f(n,n)$ for all $m \geq n$.

2.11 Additional topics

2.11.1 Block multiplication

For 2×2 matrices, we have the multiplication rule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \tag{2.19}$$

and the transpose

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix}. \tag{2.20}$$

Let m and n be positive integers. Let A be an $m \times m$ matrix, let B be an $m \times n$ matrix, let C be an $n \times m$ matrix, and let D be an $n \times n$ matrix. We define the $(m+n) \times (m+n)$ *block matrix*

$$R = (r_{i,j}) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

as follows: For $1 \leq i \leq m$ and $1 \leq j \leq m$,

$$r_{i,j} = a_{i,j}$$

For $1 \leq i \leq m$ and $m+1 \leq j \leq m+n$,

$$r_{i,j} = b_{i,j-m}$$

For $m+1 \leq i \leq m+n$ and $1 \leq j \leq m$,

$$r_{i,j} = c_{i-m,j}$$

For $m+1 \leq i \leq m+n$ and $m+1 \leq j \leq m+n$,

$$r_{i,j} = d_{i-m,j-m}.$$

For example, from the matrices

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 6 & 7 \\ 8 & 9 & 10 \end{pmatrix}, \quad C = \begin{pmatrix} 11 & 12 \\ 13 & 14 \\ 15 & 16 \end{pmatrix}, \quad D = \begin{pmatrix} 17 & 18 & 19 \\ 20 & 21 & 22 \\ 23 & 24 & 25 \end{pmatrix}$$

we construct the block matrix

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 1 & 2 & 5 & 6 & 7 \\ 3 & 4 & 8 & 9 & 10 \\ 11 & 12 & 17 & 18 & 19 \\ 13 & 14 & 20 & 21 & 22 \\ 15 & 16 & 23 & 24 & 25 \end{pmatrix}.$$

Computing the transposes of the matrices, we obtain

$$A^t = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}, \quad B^t = \begin{pmatrix} 5 & 8 \\ 6 & 9 \\ 7 & 10 \end{pmatrix}, \quad C^t = \begin{pmatrix} 11 & 13 & 15 \\ 12 & 14 & 16 \end{pmatrix}, \quad D^t = \begin{pmatrix} 17 & 20 & 23 \\ 18 & 21 & 24 \\ 19 & 22 & 25 \end{pmatrix}$$

and

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^t = \begin{pmatrix} 1 & 3 & 11 & 13 & 15 \\ 2 & 4 & 12 & 14 & 16 \\ 5 & 8 & 17 & 20 & 23 \\ 6 & 9 & 18 & 21 & 24 \\ 7 & 10 & 19 & 22 & 25 \end{pmatrix} = \begin{pmatrix} A^t & C^t \\ B^t & D^t \end{pmatrix}.$$

Analogous to the multiplication and transpose rules for 2×2 matrices, we have the following multiplication and transpose rules for 2×2 block matrices.

Theorem 2.16. *Let m and n be positive integers. Let A be an $m \times m$ matrix, let B be an $m \times n$ matrix, let C be an $n \times m$ matrix, and let D be an $n \times n$ matrix. The transpose of the $(m+n) \times (m+n)$ block matrix R is the block matrix*

$$R^t = \begin{pmatrix} A & B \\ C & D \end{pmatrix}^t = \begin{pmatrix} A^t & C^t \\ B^t & D^t \end{pmatrix}.$$

Proof. Let $R = (r_{i,j})$ and $R^t = \left(r^t_{i,j}\right)$, where $r^t_{i,j} = r_{j,i}$ for all $i, j \in \{1, \ldots, m+n\}$. For $i, j \in \{1, \ldots, m\}$, we have

$$r^t_{i,j} = r_{j,i} = a_{j,i} = a^t_{i,j}.$$

For $i \in \{1, \ldots, m\}$ and $j \in \{m+1, \ldots, m+n\}$, we have

$$r^t_{i,j} = r_{j,i} = c_{j-m,i} = c^t_{i,j-m}.$$

For $i \in \{m+1, \ldots, m+n\}$ and $j \in \{1, \ldots, m\}$, we have

$$r^t_{i,j} = r_{j,i} = b_{j,i-m} = b^t_{i-m,j}.$$

For $i \in \{m+1, \ldots, m+n\}$ and $j \in \{m+1, \ldots, m+n\}$, we have

$$r^t_{i,j} = r_{j,i} = d_{j-m,i-m} = d^t_{i-m,j-m}.$$

This completes the proof.

Theorem 2.17. *Let m and n be positive integers. Let A and E be $m \times m$ matrices, let B and F be $m \times n$ matrices, let C and G be $n \times m$ matrices, and let D and H be $n \times n$ matrices. Matrix multiplication gives the $m \times m$ matrices AE and BG, the $m \times n$ matrices AF and BH, the $n \times m$ matrices CF and DG, and the $n \times n$ matrices CG and DH.*

The product of the $(m+n) \times (m+n)$ block matrices

$$R = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \qquad \text{and} \qquad S = \begin{pmatrix} E & F \\ G & H \end{pmatrix}$$

is the block matrix

$$RS = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} E & F \\ G & H \end{pmatrix} = \begin{pmatrix} AE+BG & AF+BH \\ CE+DG & CF+DH \end{pmatrix}. \tag{2.21}$$

Proof. For $1 \leq i \leq m$ and $1 \leq j \leq m$, we have

$$\begin{aligned}
(RS)_{i,j} &= \sum_{k=1}^{m+n} r_{i,k} s_{k,j} = \sum_{k=1}^{m} r_{i,k} s_{k,j} + \sum_{k=1}^{n} r_{i,m+k} s_{m+k,j} \\
&= \sum_{k=1}^{m} a_{i,k} e_{k,j} + \sum_{k=m+1}^{m+n} b_{i,k} g_{k,j} \\
&= (AE)_{i,j} + (BG)_{i,j} = (AE+BG)_{i,j}.
\end{aligned}$$

For $1 \leq i \leq m$ and $1 \leq j \leq n$, we have

$$\begin{aligned}
(RS)_{i,m+j} &= \sum_{k=1}^{m+n} r_{i,k} s_{k,m+j} = \sum_{k=1}^{m} r_{i,k} s_{k,m+j} + \sum_{k=1}^{n} r_{i,m+k} s_{m+k,m+j} \\
&= \sum_{k=1}^{m} a_{i,k} f_{k,j} + \sum_{k=1}^{n} b_{i,k} h_{k,j} \\
&= (AF)_{i,j} + (BH)_{i,j} = (AF+BH)_{i,j}.
\end{aligned}$$

For $1 \leq i \leq n$ and $1 \leq j \leq m$, we have

$$\begin{aligned}(RS)_{m+i,j} &= \sum_{k=1}^{m+n} r_{m+i,k}s_{k,j} = \sum_{k=1}^{m} r_{m+i,k}s_{k,j} + \sum_{k=1}^{n} r_{m+i,m+k}s_{m+k,j} \\ &= \sum_{k=1}^{m} c_{m+i,k}e_{k,j} + \sum_{k=1}^{n} d_{i,k}g_{k,j} \\ &= (CE)_{i,j} + (DG)_{i,j} = (CE+DG)_{i,j}.\end{aligned}$$

For $1 \leq i \leq n$ and $1 \leq j \leq n$, we have

$$\begin{aligned}(RS)_{m+i,m+j} &= \sum_{k=1}^{m+n} r_{m+i,k}s_{k,m+j} = \sum_{k=1}^{m} r_{m+i,k}s_{k,m+j} + \sum_{k=1}^{n} r_{m+i,m+k}s_{m+k,m+j} \\ &= \sum_{k=1}^{m} c_{i,k}f_{k,j} + \sum_{k=1}^{n} d_{i,k}h_{k,j} \\ &= (CF)_{i,j} + (DH)_{i,j} = (CF+DH)_{i,j}.\end{aligned}$$

This completes the proof.

Let $k_1, k_2, \ell_1, \ell_2, m_1, m_2$ be positive integers. Let A be a $k_1 \times \ell_1$ matrix, let B be a $k_1 \times \ell_2$ matrix, let C be a $k_2 \times \ell_1$ matrix, and let D be a $k_2 \times \ell_2$ matrix. We define the $(k_1+k_2) \times (\ell_1+\ell_2)$ block matrix

$$R = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

where

$$\begin{aligned} r_{i,j} &= a_{i,j} && \text{for } 1 \leq i \leq k_1 \text{ and } 1 \leq j \leq \ell_1, \\ r_{i,\ell_1+j} &= b_{i,j} && \text{for } 1 \leq i \leq k_1 \text{ and } 1 \leq j \leq \ell_2, \\ r_{k_1+i,j} &= c_{i,j} && \text{for } 1 \leq i \leq k_2 \text{ and } 1 \leq j \leq \ell_1, \\ r_{k_1+i,\ell_1+j} &= d_{i,j} && \text{for } 1 \leq i \leq k_2 \text{ and } 1 \leq j \leq \ell_2. \end{aligned}$$

Let E be a $\ell_1 \times m_1$ matrix, let F be a $\ell_1 \times m_2$ matrix, let G be a $\ell_2 \times m_1$ matrix, and let H be a $\ell_2 \times m_2$ matrix. We define the $(\ell_1+\ell_2) \times (m_1+m_2)$ block matrix

$$S = \begin{pmatrix} E & F \\ G & H \end{pmatrix}$$

where

$$\begin{aligned} s_{i,j} &= e_{i,j} && \text{for } 1 \leq i \leq \ell_1 \text{ and } 1 \leq j \leq m_1, \\ s_{i,m_1+j} &= f_{i,j} && \text{for } 1 \leq i \leq \ell_1 \text{ and } 1 \leq j \leq m_2, \\ s_{\ell_1+i,j} &= g_{i,j} && \text{for } 1 \leq i \leq \ell_2 \text{ and } 1 \leq j \leq m_1, \\ s_{\ell_1+i,m_1+j} &= h_{i,j} && \text{for } 1 \leq i \leq \ell_2 \text{ and } 1 \leq j \leq m_2. \end{aligned}$$

The matrices AE and BG are $k_1 \times m_1$ matrices. The matrices AF and BH are $k_1 \times m_2$ matrices. The matrices CE and DG are $k_2 \times m_1$ matrices. The matrices CF and DH are $k_2 \times m_2$ matrices.

Theorem 2.18. *The product of the $(k_1+k_2)\times(\ell_1+\ell_2)$ block matrix R and the $(\ell_1+\ell_2)\times(m_1+m_2)$ block matrix S is the $(k_1+k_2)\times(m_1+m_2)$ block matrix*

$$RS = \begin{pmatrix} AE+BG & AF+BH \\ CE+DG & CF+DH \end{pmatrix}.$$

Proof. The proof is similar to the proof of Theorem 2.17.

Exercises

1. Use block matrix multiplication to prove that

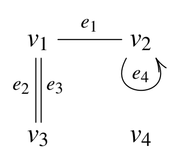
$$\begin{pmatrix} 1 & 2 & 1 & 2 \\ 3 & 4 & 3 & 4 \\ 1 & 2 & 1 & 2 \\ 3 & 4 & 3 & 4 \end{pmatrix}^2 = \begin{pmatrix} 14 & 20 & 14 & 20 \\ 30 & 44 & 30 & 44 \\ 14 & 20 & 14 & 20 \\ 30 & 44 & 30 & 44 \end{pmatrix}.$$

2.11.2 An application of matrices to graphs

An *undirected graph* $\Gamma = \Gamma(V,E)$ consists of a set V whose elements are called the *vertices* of the graph, and a set E whose elements are called the *edges* of the graph. Each edge $e \in E$ is a set consisting of one or two vertices. An edge $\{v\}$ consisting of one vertex v is called a *loop*. If $e = \{v,v'\} \in E$, then we say that e is an edge connecting the vertices v and v'. We say that vertices v and v' in the graph Γ are *adjacent* if $\{v,v'\} \in E$. The graph Γ is *finite* if it has only finitely many vertices and finitely many edges.

An undirected graph is *simple* if it has no loop and if it has at most one edge connecting any pair of vertices.

For example, let $\Gamma = \Gamma(V,E)$ be the graph with vertex set $V = \{v_1,v_2,v_3,v_4\}$ and edge set $E = \{e_1,e_2,e_3,e_4\}$, where $e_1 = \{v_1,v_2\}$, $e_2 = e_3 = \{v_1,v_3\}$, and $e_4 = \{v_2\}$. Then e_1 and e_2 are multiple edges between vertices v_1 and v_2, e_3 is a single edge between vertices v_2 and v_3, and e_4 is a loop at vertex v_3. Vertex v_4 is isolated; it is not adjacent to any other vertex. We can draw this graph as follows:



(2.22)

Let $\Gamma(V,E)$ be a graph. A path of length k between the vertices v and v' is a $(k+1)$-tuple of vertices $(v_0, v_1, \ldots, v_k)$ such that $v_0 = v$, $v_k = v'$, and $\{v_{i-1}, v_i\}$ is an edge in Γ for all $i = 1, \ldots, k$. The *neighboorhood* of a vertex v in Γ is the set $N(v)$ of vertices connected to v by an edge, that is,

$$N(v) = \{v' \in V : \{v, v'\} \in E\}.$$

If Γ is a simple graph, then the number of paths of length 2 connecting vertices v and v' is exactly $|N(v) \cap N(v')|$.

Let $\Gamma = \Gamma(V,E)$ be a finite graph. The *degree* of a vertex v in the graph $\Gamma(V,E)$, denoted $\deg(v)$, is the number of edges that contain the vertex, that is,

$$\deg(v) = \sum_{\substack{e \in E \\ v \in E}} 1.$$

A set of vertices in Γ is *independent* if the set does not contain two adjacent vertices. Every subset of an independent set is independent. The *independence number* of a finite graph is the cardinality of the largest independent subset of V. If the graph contains a loop at v, then v is adjacent to itself and no set containing v is independent. We denote the independence number by $i(\Gamma)$.

Let $\Gamma = \Gamma(V,E)$ be a finite graph with n vertices, and let

$$V = \{v_1, \ldots, v_n\}.$$

The *adjacency matrix* of Γ is the $n \times n$ matrix $A = A(\Gamma) = (a_{i,j})$, where $a_{i,j}$ is the number of edges connecting vertex $v_i i$ and vertex v_j. In an undirected graph, an edge e connects vertex i and vertex j if and only if e connects vertex j and vertex i, and so $a_{i,j} = a_{j,i}$ for all $i, j \in \{1, \ldots, n\}$, that is, the adjacency matrix is symmetric. Note that $a_{i,i} > 0$ if and only if there is at least one loop at vertex i.

For example, the adjacency matrix of the graph (2.22) is

$$\begin{pmatrix} 0 & 1 & 2 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The ith row sum $\mathrm{row}_i(A)$ is the degree of vertex i. Because A is symmetric, the ith row sum equals the ith column sum.

A *directed graph* $\Gamma = \Gamma(V,E)$ consists of a set V whose elements are called the *vertices* of the graph, and a set E whose elements are called the *directed edges* of the graph. Each edge $e \in E$ is an ordered pair of the form (v, v'), where v and v' are vertices that are not necessarily distinct. We can draw the directed edge (v, v') as an arrow from v to v'. A directed edge of the form (v, v) is called a *loop*. If $e = (v, v') \in E$, then we say that e is an edge from vertex v to vertex v'. The directed graph Γ is *finite* if it has only finitely many vertices and finitely many edges.

The *outdegree* of a vertex $v \in V$ is the number of edges $e \in E$ of the form (v, v'), that is, the number of arrows that start at v. The *indegree* of a vertex $v \in V$ is the number of edges $e \in E$ of the form (v', v), that is, the number of arrows that end at v.

Let $\Gamma = \Gamma(V, E)$ be a finite directed graph with n vertices, and let

$$V = \{v_1, \ldots, v_n\}.$$

The *adjacency matrix* of Γ is the $n \times n$ matrix $A = A(\Gamma) = (a_{i,j})$, where $a_{i,j}$ is the number of edges from vertex $v_i i$ to vertex v_j. The ith row sum $\mathrm{row}_i(A)$ is the outdegree of vertex i. The jth column sum $\mathrm{col}_j(A)$ is the indegree of vertex j.

Consider the directed graph $\Gamma = (V, E)$, where $V = \{v_1, v_2, v_3, v_4\}$ and $E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$, where

$$\begin{aligned}
e_1 &= (v_1, v_2) \\
e_2 &= (v_1, v_3) \\
e_3 &= (v_3, v_1) \\
e_4 &= (v_2, v_4) \\
e_5 &= e_6 = (v_4, v_3).
\end{aligned}$$

We can draw this graph as follows:

$$\begin{tikzcd}
v_1 \arrow[r, "e_1"] \arrow[d, bend right, "e_2"'] & v_2 \arrow[d, "e_4"] \\
v_3 \arrow[u, bend right, "e_3"'] & v_4 \arrow[l, bend right, "e_5"'] \arrow[l, bend left, "e_6"]
\end{tikzcd} \tag{2.23}$$

The adjacency matrix of the directed graph (2.23) is

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

The ith row sum is the out-degree of vertex i. The jth column sum is the in-degree of t vertex j.

We have

$$A^2 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 0 \end{pmatrix}.$$

A *bipartite graph* is a simple undirected graph $\Gamma = \Gamma(V, E)$ whose vertex set is the union of disjoint sets V_1 and V_2, and whose edges are of the form $\{v_1, v_2\}$, where $v_1 \in V_1$ and $v_2 \in V_2$. We denote this bipartite graph by $\Gamma = \Gamma(V_1, V_2, E)$.

Equivalently, the graph $\Gamma = \Gamma(V,E)$ is bipartite if there is a partition $V = V_1 \cup V_2$ such that $V_1 \cap V_2 = \emptyset$ and

$$E \subseteq \{\{v_1, v_2\} : v_1 \in V_1 \text{ and } v_2 \in V_2\}.$$

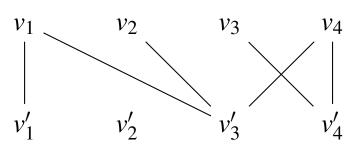
A bipartite graph is finite if it has only finitely many vertices.

Let $\Gamma = \Gamma(V,E)$ be a bipartite graph with vertex partition $V = V_1 \cup V_2$, where $|V_1| = m$ and $|V_2| = n$. Let $V_1 = \{v_1, \ldots, v_m\}$ and $V_2 = \{v_1', \ldots, v'_{\}}$. The usual adjacency matrix of Γ is an $(m+n) \times (m+n)$ matrix. We can associate a second adjacency matrix to Γ as follows:

This is the $m \times n$ matrix $A = (a_{i,j})$, where

$$a_{i,j} = \begin{cases} 1 & \text{if } v_i \text{ and } v_j' \text{ are adjacent vertices} \\ 0 & \text{if } v_i \text{ and } v_j' \text{ are not adjacent vertices.} \end{cases}$$

For example, the adjacency matrix of the bipartite graph



is

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

Theorem 2.19. *Let $\Gamma = (V,E)$ be a finite undirected graph. Let $V = \{v_1, \ldots, v_n\}$, and let A be the adjacency matrix of Γ. The matrix A is symmetric. Let $A^\ell = \left(a_{i,j}^{(\ell)}\right)$. The coordinate $a_{i,j}^{(\ell)}$ denotes the number of paths of length ℓ between vertices v_i and v_j.*

Theorem 2.20. *Let $\Gamma = (V,E)$ be a finite directed graph. Let $V = \{v_1, \ldots, v_n\}$, and let A be the adjacency matrix of Γ. Let $A^\ell = \left(a_{i,j}^{(\ell)}\right)$. The coordinate $a_{i,j}^{(\ell)}$ denotes the number of directed paths of length ℓ from vertex v_i to vertex v_j.*

2.11.3 Hadamard matrices

A *Hadamard matrix* of order n is an $n \times n$ matrix $H = (h_{i,j})$ with coordinates $h_{i,j} = \pm 1$ for all i and j, and with row vectors that are orthogonal in the sense that

$$\sum_{k=1}^{n} h_{i,k}h_{j,k} = 0$$

for all $i \neq j$. For example, the matrices

$$\begin{pmatrix}1\end{pmatrix}, \qquad \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \qquad \begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}$$

are Hadamard matrices of orders 1, 2, and 4, respectively.

Theorem 2.21. *An $n \times n$ matrix H with coordinates $h_{i,j} = \pm 1$ is a Hadamard matrix if and only if*

$$HH^t = nI_n.$$

Proof. Every $n \times n$ matrix H with coordinates $h_{i,j} = \pm 1$ satisfies

$$\left(HH^t\right)_{i,i} = \sum_{k=1}^{n} h_{i,k}h^t_{k,i} = \sum_{k=1}^{n} h_{i,k}h_{i,k} = \sum_{k=1}^{n} h^2_{i,k} = \sum_{k=1}^{n} 1 = n.$$

The matrix H is Hadamard if and only if

$$\left(HH^t\right)_{i,j} = \sum_{k=1}^{n} h_{i,k}h^t_{k,j} = \sum_{k=1}^{n} h_{i,k}h_{j,k} = 0$$

for all $i \neq j$. It follows that, for all $i, j \in \{1, \ldots, n\}$,

$$\left(HH^t\right)_{i,j} = n\delta_{i,j}$$

where $\delta_{i,j}$ is the Kronecker delta, and so $HH^t = nI_n$. This completes the proof.

Corollary 2.1. *If $H = (h_{i,j})$ is a Hadamard matrix of order n, then the column vectors of H are orthogonal in the sense that*

$$\sum_{k=1}^{n} h_{k,i}h_{k,j} = 0$$

for all $i \neq j$.

Proof. It follows from Theorem 2.21 that H is invertible and that

$$H^{-1} = \frac{1}{n}H^t.$$

By Theorem **??**, if $HH^{-1} = I_n$, then $H^{-1}H = I_n$, and so

$$\frac{1}{n}H^tH = H^{-1}H = I_n.$$

This matrix identity implies the orthogonality of the columns of H.

Lemma 2.10. *Let $H = (h_{i,j})$ be a Hadamard matrix of order n. The matrix obtained by multiplying any column or row of H by -1 is a Hadamard matrix. The matrix obtained by interchanging any two columns or any two rows of H is also a Hadamard matrix.*

Proof. Let $\ell \in \{1,\ldots,n\}$. Multiplying the ℓth column of H by -1, we obtain the matrix $H' = \left(h'_{i,j}\right)$, where

$$h'_{i,k} = h_{i,k} \qquad \text{if } k \neq \ell$$

and

$$h'_{i,\ell} = -h_{i,\ell}.$$

For $i \neq j$, we have

$$\begin{aligned}
\sum_{k=1}^{n} h'_{i,k}h'_{j,k} &= \sum_{\substack{k=1\\k\neq\ell}}^{n} h'_{i,k}h'_{j,k} + h'_{i,\ell}h'_{j,\ell} \\
&= \sum_{\substack{k=1\\k\neq\ell}}^{n} h_{i,k}h_{j,k} + \left(-h_{i,\ell}\right)\left(-h_{j,\ell}\right) \\
&= \sum_{\substack{k=1\\k\neq\ell}}^{n} h_{i,k}h_{j,k} + h_{i,\ell}h_{j,\ell} \\
&= \sum_{k=1}^{n} h_{i,k}h_{j,k} \\
&= 0
\end{aligned}$$

and so H' is Hadamard.

Let $p,q \in \{1,\ldots,n\}$ with $p \neq q$. Let $H'' = \left(h''_{i,j}\right)$ be the matrix obtained by interchanging columns p and q of H. We have

$$\begin{aligned}
h''_{i,j} &= h_{i,j} \qquad \text{if } j \neq p,q, \\
h''_{i,p} &= h_{i,q} \\
h''_{i,q} &= h_{i,p}.
\end{aligned}$$

For $i \neq j$, we have

$$\begin{aligned}
\sum_{k=1}^{n} h''_{i,k}h''_{j,k} &= \sum_{\substack{k=1\\k\neq p,q}}^{n} h''_{i,k}h''_{j,k} + h''_{i,p}h''_{j,p} + h''_{i,q}h''_{j,q} \\
&= \sum_{\substack{k=1\\k\neq p,q}}^{n} h_{i,k}h_{j,k} + h_{i,q}h_{j,q} + h_{i,p}h_{j,p} \\
&= \sum_{k=1}^{n} h_{i,k}h_{j,k} \\
&= 0
\end{aligned}$$

and so H'' is Hadamard.

The proof for rows is the same as the proof for columns.

Theorem 2.22. *If H is a Hadamard matrix of order n, then $n = 1$, $n = 2$, or n is a multiple of 4.*

Proof. Let $H = (h_{i,j})$ be a Hadamard matrix of order $n \geq 3$. Multiplying the kth column by -1 for every k such that $h_{1,k} = -1$, we obtain a Hadamard matrix $H' = \left(h'_{i,j}\right)$ such that every coordinate in the first row is 1, that is, $h'_{1,j} = 1$ for all $j \in \{1,\ldots,n\}$. Let r be the number of coordinates in the second row that are equal to 1, and let s be the number of coordinates in the second row that are equal to -1. We have

$$r + s = n.$$

Multiplying the first and second rows, we obtain

$$0 = \sum_{j=1}^{n} h'_{1,j}h'_{2,j} = \sum_{j=1}^{n} h'_{2,j} = r - s$$

and so $r = s$ and $n = 2r$ is even.

Interchanging columns, we can construct a Hadamard matrix $H'' = \left(h''_{i,j}\right)$ of order n such that

$$\begin{aligned}
h''_{1,j} &= 1 \qquad \text{for all } j \in \{1,\ldots,n\} \\
h''_{2,j} &= 1 \qquad \text{for all } j \in \{1,\ldots,r\} \\
h''_{2,j} &= -1 \qquad \text{for all } j \in \{r+1,\ldots,n\}.
\end{aligned}$$

Thus, the first row of H'' consists of $n = 2r$ consecutive 1's, and the second row of H'' consists of r consecutive 1's followed by r consecutive (-1)'s.

Consider the third row of H''.

Let t_1 be the number of $k \in \{1,\ldots,r\}$ such that $h''_{3,k} = 1$.

Let t_2 be the number of $k \in \{1,\ldots,r\}$ such that $h''_{3,k} = -1$.

Let u_1 be the number of $k \in \{r+1,\ldots,n\}$ such that $h''_{3,k} = 1$.

Let u_2 be the number of $k \in \{r+1,\ldots,n\}$ such that $h''_{3,k} = -1$.

Because H'' is a Hadamard matrix, we have

$$0 = \sum_{k=1}^{n} h''_{1,k} h_{3,k} = t_1 - t_2 + u_1 - u_2$$

and

$$0 = \sum_{k=1}^{n} h''_{2,k} h_{3,k} = t_1 - t_2 - u_1 + u_2.$$

Adding and subtracting these equations, we obtain $t_1 = t_2$ and $u_1 = u_2$, and so $r = 2t_1 = 2u_1$ and $n = 2r = 4t_1$. Thus, if $n \geq 3$, then n is a multiple of 4. This completes the proof.

Theorem 2.23 (Sylvester). *Let H_n be a Hadamard matrix of order n. The $2n \times 2n$ block matrix*

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

is a Hadamard matrix.

Proof. The coordinates of H_n are ± 1, and so the coordinates of H_{2n} are also ± 1, By Lemma **??**, the transpose of H_{2n} is

$$H_{2n}^t = \begin{pmatrix} H_n^t & H_n^t \\ H_n^t & -H_n^t \end{pmatrix}.$$

By Theorem 2.21, $H_n H_n^t = nI_n$, and the matrix H_{2n} is Hadamard if and only if $H_{2n} H_{2n}^t = 2nI_{2n}$. Using the multiplication rule for block matrices (Theorem 2.17), we obtain

$$\begin{aligned} H_{2n} H_{2n}^t &= \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix} \begin{pmatrix} H_n^t & H_n^t \\ H_n^t & -H_n^t \end{pmatrix} \\ &= \begin{pmatrix} H_n H_n^t + H_n H_n^t & H_n H_n^t - H_n H_n^t \\ H_n H_n^t - H_n H_n^t & H_n H_n^t + H_n H_n^t \end{pmatrix} \\ &= \begin{pmatrix} 2H_n H_n^t & 0 \\ 0 & 2H_n H_n^t \end{pmatrix} \\ &= \begin{pmatrix} 2nI_n & 0 \\ 0 & 2nI_n \end{pmatrix} = 2nI_{2n}. \end{aligned}$$

This completes the proof.

Corollary 2.2. *There exist Hadamard matrices of order 2^k for all nonnegative integers k.*

Exercises

1. Prove that if H is a Hadamard matrix, then the matrix $\frac{1}{\sqrt{n}}H$ is orthogonal in the sense that
$$\left(\frac{1}{\sqrt{n}}H\right)\left(\frac{1}{\sqrt{n}}H\right)^t = I_n.$$
2.
$$\det(H) = \pm n^{n/2}$$
3. Sylvester's construction: If H is Hadamard, then $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ is Hadamard.
4. Hadamard determinant inequality: If $A = (a_{i,j}) \in \mathrm{Mat}_n$ and $|a_{i,j}| \leq 1$, then
$$|\det(A)| \leq n^{n/2}$$
with equality if and only if H is Hadamard.

It is a famous unsolved problem in matrix theory to prove that there exists a Hadamard matrix of order $4k$ for every positive integer k.

2.11.4 Rank one matrices

Let $A = (a_{i,j})$ be a rank one matrix. This means that the set of column vectors of A spans a subspace of dimension 1. It follows that at least one column of A is nonzero, and that every other column is a scalar multiple of it. Suppose that the kth column is nonzero. Let
$$\begin{pmatrix} u_1 \\ \vdots \\ u_m \end{pmatrix} = \begin{pmatrix} a_{1,k} \\ \vdots \\ a_{m,k} \end{pmatrix} \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$
For every $j \neq k$ there exists a scalar v_j such that
$$\begin{pmatrix} a_{1,j} \\ \vdots \\ a_{m,j} \end{pmatrix} = v_j \begin{pmatrix} a_{1,k} \\ \vdots \\ a_{m,k} \end{pmatrix} = \begin{pmatrix} u_1 v_j \\ \vdots \\ u_m v_j \end{pmatrix}.$$
Let $v_k = 1$. We obtain

$$\begin{aligned}
A &= \begin{pmatrix} u_1v_1 & u_1v_2 & \cdots & u_1v_n \\ u_2v_1 & u_2v_2 & \cdots & u_2v_n \\ \vdots & & \vdots & \\ u_mv_1 & u_mv_2 & \cdots & u_mv_n \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} \begin{pmatrix} v_1 & v_2 & \cdots & v_n \end{pmatrix} \\
&= \mathbf{u}\mathbf{v}^t
\end{aligned}$$

where

$$\mathbf{u} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} \in \mathbf{R}^m \qquad \text{and} \qquad \mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \in \mathbf{R}^n.$$

Thus, every rank one matrix is the product of an m-dimensional column vector and an n-dimensional row vector.

For example, we have the following decomposition of the rank one matrix

$$\begin{pmatrix} 2 & 7 & 0 & -5 \\ 4 & 14 & 0 & -10 \\ 6 & 21 & 0 & -15 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \begin{pmatrix} 2 & 7 & 0 & -5 \end{pmatrix}.$$

Consider the rank two matrix

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

Columns 1 and 2 are linearly independent, and

$$\begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix} = -3 \begin{pmatrix} 0 \\ -1 \\ -2 \end{pmatrix} + 2 \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 6 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \\ -6 \end{pmatrix}.$$

It follows that

$$\begin{aligned}
A = \begin{pmatrix} 0 & 1 & 2 \\ -1 & 0 & 3 \\ -2 & -3 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 3 \\ -2 & 0 & 6 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & -3 & -6 \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ -1 \\ -2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 2 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \end{pmatrix}.
\end{aligned}$$

Thus, the rank 2 matrix A is the sum of two rank one matrices. Because the rank of a matrix is well defined, the matrix A is not also a rank one matrix.

Lemma 2.11. *Let A be an $m \times n$ matrix. If A is the sum of r rank one matrices, then the rank of A is at most r.*

Proof. Let $A_1, \ldots, A_r$ be rank one matrices, and let $A = A_1 + \cdots + A_r$. For $i = 1, \ldots, r$, the columns of the matrix A_i are scalar multiples of a nonzero vector $\mathbf{v}_i \in \mathbf{R}^m$. Thus, every column vector in A is a linear combination of the r vectors $\mathbf{v}_1, \ldots, \mathbf{v}_r$, and so the columns of A are vectors in the subspace of $\mathbf{R}^m$ generated by the set of r vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$. The dimension of a vector space generated by a set of r vectors is at most r, and so A has rank at most r. This completes the proof.

Theorem 2.24. *The rank of a matrix A is the smallest number r such that A is the sum of r matrices of rank one.*

Proof. Let $A = (a_{i,j})$ be an $m \times n$ matrix, and let $\mathbf{c}_j = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{m,j} \end{pmatrix} \in \mathbf{R}^m$ denote the jth column vector of A. We write the matrix A as an n-tuple of column vectors:

$$A = (\mathbf{c}_1, \ldots, \mathbf{c}_n).$$

If A has rank r, then there exist distinct integers $j_1, \ldots, j_r \in \{1, \ldots, n\}$ such that the r column vectors $\mathbf{c}_{j_1}, \ldots, \mathbf{c}_{j_r}$ are linearly independent, and every other column vector of A is a linear combination of these r column vectors. Thus, for all $j \in \{1, \ldots, n\} \setminus \{j_1, \ldots, j_r\}$, there exist scalars $b_{j,1}, \ldots, b_{j,r}$ such that

$$\mathbf{c}_j = \sum_{k=1}^{r} b_{j,j_k} \mathbf{c}_{j_k}. \tag{2.24}$$

For $j \in \{j_1, \ldots, j_r\}$, let $b_{j,k}$ be the Kronecker delta δ_{j,j_k}, and so (2.24) holds for all $j \in \{1, \ldots, n\}$. We obtain

$$\begin{aligned}
A &= (\mathbf{c}_1, \ldots, \mathbf{c}_n) \\
&= \left(\sum_{k=1}^{r} b_{1,j_k} \mathbf{c}_{j_k}, \ldots, \sum_{k=1}^{r} b_{n,j_k} \mathbf{c}_{j_k} \right) \\
&= \sum_{k=1}^{r} \left(b_{1,j_k} \mathbf{c}_{j_k}, \ldots, b_{n,j_k} \mathbf{c}_{j_k} \right) \\
&= \sum_{k=1}^{r} \mathbf{c}_{j_k} \left(b_{1,j_k}, \ldots, b_{n,j_k} \right) \\
&= \sum_{k=1}^{r} \begin{pmatrix} a_{1,j_k} \\ \vdots \\ a_{m,j_k} \end{pmatrix} \left(b_{1,j_k}, \ldots, b_{n,j_k} \right)
\end{aligned}$$

Thus, A is the sum of r rank one matrices. It follows from Lemma 2.11 that A is not the sum of less than r rank one matrices. This completes the proof.

Exercises

Compute the rank of the matrix A and write the matrix as a sum of $r = \operatorname{rank}(A)$ matrices of rank one.

1.
$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

Solution: $\operatorname{rank}(A) = 2$.
$$\begin{pmatrix} 1 \\ 3 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix} \begin{pmatrix} 0 & 2 \end{pmatrix}$$

2.
$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

Solution: $\operatorname{rank}(A) = 2$.
$$\begin{pmatrix} 1 \\ 4 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \end{pmatrix} + \begin{pmatrix} 2 \\ 5 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \end{pmatrix}$$

3.
$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Solution: $\operatorname{rank}(A) = 2$.
$$\begin{pmatrix} 1 \\ 4 \\ 7 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \end{pmatrix} + \begin{pmatrix} 2 \\ 5 \\ 8 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \end{pmatrix}$$

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

Solution: $\operatorname{rank}(A) = 3$.
$$\begin{pmatrix} 1 \\ 0 \\ -3 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & -8/3 \end{pmatrix} + \begin{pmatrix} 2 \\ 0 \\ 0 \\ -3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 4/3 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ -4 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 2 \end{pmatrix}$$

2.12 Stuff to add

1. Define scalar product of vectors before matrix multiplication, and use scalar product to define matrix multiplication.
2. Let A and B be $n \times n$ matrices. Prove that if $AB = I_n$, then $BA = I_n$.
3. Permutation matrices: Multiplying on the left permute rows and on the right permute columns.
4. Example of $n \times n$ matrix: Jacobian of a change of variables, e.g polar to rectangular.
5. Wronskian in ODE
6. Lie algebra of matrices
7. An $m \times n$ matrix $A = (a_{i,j})$ is *nonnegative* if $a_{i,j} \geq 0$ for all $i = 1, \ldots, m$ and $j = 1, \ldots, n$. An $m \times n$ matrix $A = (a_{i,j})$ is *positive* if $a_{i,j} > 0$ for all $i = 1, \ldots, m$ and $j = 1, \ldots, n$.

   a. Prove that if A and B are nonnegative matrices, then $A + B$ is nonnegative.
   b. Prove that if A is a nonnegative matrix and B is a positive matrix, then $A + B$ is positive.
   c. Let A be a nonnegative $n \times n$ matrix. Prove that A^k is nonnegative and that $(I + A)^k$ is nonnegative for all $k \in \mathbf{N}$.
   d. Let A be a positive $n \times n$ matrix. Prove that A^k is positive and that $(I + A)^k$ is positive for all $k \in \mathbf{N}$.

8. A nonnegative $n \times n$ matrix A is *irreducible* if, for all (i, j) there exists $k(i, j) \in \mathbf{N}$ such that the (i, j)th coordinate of the matrix $A^{k(i,j)}$ is positive, that is, $\left(A^{k(i,j)}\right)_{i,j} > 0$.

   a. Prove that the nonnegative matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is irreducible, but that A^k is not positive for all $k \in \mathbf{N}$.
   b. Prove that the nonnegative matrix $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ is irreducible, but that A^k is not positive for all $k \in \mathbf{N}$.
   c. Prove that the nonnegative matrix $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is not irreducible.
   d. Let A be an $n \times n$ matrix. Prove the binomial theorem

$$
\begin{aligned}
(I + A)^k &= \sum_{r=0}^{k} \binom{k}{r} A^r \\
&= I + kA + \frac{k(k-1)}{2} A^2 + \frac{k(k-1)(k-2)}{3!} A^3 + \cdots .
\end{aligned}
$$

e. Let A be an irreducible $n \times n$ matrix. Prove that the matrices $\sum_{r=0}^{k} A^r$ and $(I+A)^k$ are positive for all sufficiently large integers k.

2.13 Solution space of a system of linear equations

Recall that $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ is an n-dimensional *column vector*, and that $\mathbf{R}^n$ is the set of all n-dimensional column vectors. The real numbers $x_1, \ldots, x_n$ are called the *coordinates* of the column vector. If $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and $\mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ are column vectors, then $\mathbf{x} = \mathbf{y}$ if and only if $\mathbf{x}$ and $\mathbf{y}$ have the same coordinates, that is, if and only if $x_i = y_i$ for all $i = 1, \ldots, n$.

We define addition and subtraction of column vectors as follows:
If $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and $\mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, then

$$\mathbf{x} + \mathbf{y} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

and

$$\mathbf{x} - \mathbf{y} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} - \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 - y_1 \\ \vdots \\ x_n - y_n \end{pmatrix}$$

For every scalar $c \in \mathbf{R}$ and vector $\mathbf{x} \in \mathbf{R}^n$, we define *scalar multiplication* as follows:

$$c\mathbf{x} = c \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} cx_1 \\ \vdots \\ cx_n \end{pmatrix}.$$

If $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbf{R}^n$ and $c_1, \ldots, c_k \in \mathbf{R}$, the column vector

$$c_1\mathbf{x}_1 + \cdots + c_k\mathbf{x}_k = c_1 \begin{pmatrix} x_{1,1} \\ \vdots \\ x_{n,1} \end{pmatrix} + \cdots + c_k \begin{pmatrix} x_{1,k} \\ \vdots \\ x_{n,k} \end{pmatrix} = \begin{pmatrix} c_1 x_{1,1} + \cdots + c_k x_{1,k} \\ \vdots \\ c_1 x_{n,1} + \cdots + c_k x_{n,k} \end{pmatrix}$$

is called a *linear combination* of the column vectors $\mathbf{x}$ and $\mathbf{y}$.

For example,

$$2\begin{pmatrix}7\\-5\\1\end{pmatrix}+5\begin{pmatrix}0\\3\\11\end{pmatrix}=\begin{pmatrix}14\\-10\\2\end{pmatrix}+\begin{pmatrix}0\\15\\55\end{pmatrix}=\begin{pmatrix}14\\5\\57\end{pmatrix}.$$

Similarly, we call $\left(x_1,\ldots,x_n\right)$ an n-dimensional *row vector*, and we denote by $(\mathbf{R}^n)^*$ the set of all n-dimensional row vectors. The real numbers $x_1,\ldots,x_n$ are called the *coordinates* of the row vector. If $x=\left(x_1,\ldots,x_n\right)$ and $y=\left(y_1,\ldots,y_n\right)$ are row vectors, then $x=y$ if and only if x and y have the same coordinates, that is, if and only if $x_i=y_i$ for all $i=1,\ldots,n$.

We define addition and subtraction of row vectors as follows: If $x=\left(x_1,\ldots,x_n\right)$ and $y=\left(y_1,\ldots,y_n\right)$, then

$$x+y=\left(x_1,\ldots,x_n\right)+\left(y_1,\ldots,y_n\right)=\left(x_1+y_1,\ldots,x_n+y_n\right)$$

and

$$x-y=\left(x_1,\ldots,x_n\right)-\left(y_1,\ldots,y_n\right)=\left(x_1-y_1,\ldots,x_n-y_n\right).$$

For every scalar $c\in\mathbf{R}$ and row vector $x\in(\mathbf{R}^n)^*$, we define *scalar multiplication* as follows:

$$cx=c\left(x_1,\ldots,x_n\right)=\left(cx_1,\ldots,cx_n\right).$$

If $x,y\in(\mathbf{R}^n)^*$ and $c,c'\in\mathbf{R}$, the row vector

$$cx+c'y=c\left(x_1,\ldots,x_n\right)+c'\left(y_1,\ldots,y_n\right)=\left(cx_1+c'y_1,\ldots,cx_n+c'y_n\right)$$

is called a *linear combination* of the row vectors x and y.

Let (**??**) be an inhomogeneous system of linear equations. The *associated homogeneous system* is the system of linear equations

$$\left\{\begin{array}{ccccccccc} a_{1,1}x_1 & + & \cdots & + & a_{1,j}x_j & + & \cdots & + & a_{1,n}x_n = 0\\ \vdots & & & & & & & & \\ a_{i,1}x_1 & + & \cdots & + & a_{i,j}x_j & + & \cdots & + & a_{i,n}x_n = 0\\ \vdots & & & & & & & & \\ a_{m,1}x_1 & + & \cdots & + & a_{m,j}x_j & + & \cdots & + & a_{m,n}x_n = 0. \end{array}\right. \tag{2.25}$$

Let

$$x=\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix},\quad x'=\begin{pmatrix}x_1'\\\vdots\\x_n'\end{pmatrix},\quad y=\begin{pmatrix}y_1\\\vdots\\y_n\end{pmatrix},\quad y=\begin{pmatrix}y_1'\\\vdots\\y_n'\end{pmatrix}$$

be column vectors in $\mathbf{R}^n$ such that x and x' are solutions of the inhomogeneous system (**??**), and y and y' are solutions of the homogeneous system (2.5). For $i=1,\ldots,m$ we have

$$\sum_{j=1}^{n} a_{i,j}x_j = \sum_{j=1}^{n} a_{i,j}x'_j = b_i$$

and

$$\sum_{j=1}^{n} a_{i,j}y_j = \sum_{j=1}^{n} a_{i,j}y'_j = 0.$$

It follows that

$$\sum_{j=1}^{n} a_{i,j}(x_j + y_j) = \sum_{j=1}^{n} a_{i,j}x_j + \sum_{j=1}^{n} a_{i,j}y_j = b_j + 0 = b_j$$

and so $x+y$ is also a solution of the inhomogeneous system. Similarly,

$$\sum_{j=1}^{n} a_{i,j}(x'_j - x_j) = \sum_{j=1}^{n} a_{i,j}x'_j - \sum_{j=1}^{n} a_{i,j}x_j = b_j - b_j = 0.$$

and so $x' - x$ is also a solution of the homogeneous system. Therefore, $x \in \mathbf{R}^n$ is one solution of the inhomogeneous system, then $x' \in \mathbf{R}^n$ is also a solution if and only if $x' = x + (x' - x) = x + y$, where $y \in \mathbf{R}^n$ is a solution of the associated homogeneous system.

If y and y' in $\mathbf{R}^n$ are solutions of the homogeneous system (2.5), then for all scalars $c, c' \in \mathbf{R}$, we have

$$\sum_{j=1}^{n} a_{i,j}(cy_j + c'y'_j) = c\sum_{j=1}^{n} a_{i,j}y_j + c'\sum_{j=1}^{n} a_{i,j}y'_j = 0$$

and so the column vector

$$\begin{pmatrix} cy_1 + c'y'_1 \\ \vdots \\ cy_n + c'y'_n \end{pmatrix} = c\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} + c'\begin{pmatrix} y'_1 \\ \vdots \\ y'_n \end{pmatrix} = cy + c'y'$$

is also a solution of the homogeneous system (2.5). If $x \in \mathbf{R}^n$ is a solution of the inhomogeneous system (**??**), then $x' \in \mathbf{R}^n$ is also solution of (**??**) if and only if $x' = x + y$, where $y \in \mathbf{R}^n$ is a solution of the associated homogeneous system (2.5).

Let x and x' be solutions of the inhomogeneous system, let t be any real number, and consider the vector

$$tx + (1-t)x' = \begin{pmatrix} tx_1 + (1-t)x'_1 \\ \vdots \\ tx_n + (1-t)x'_n \end{pmatrix}.$$

Computing the ith equation of the system at the coordinates of this vector, we obtain

$$\begin{aligned}\sum_{j=1}^{n} a_{i,j}(tx_j+(1-t)x'_j) &= t\sum_{j=1}^{n} a_{i,j}x_j+(1-t)\sum_{j=1}^{n} a_{i,j}x'_j \\ &= tb_i+(1-t)b_i=b_i\end{aligned}$$

and so $tx+(1-t)x'$ is also a solution of the inhomogeneous system (**??**). The vector $tx+(1-t)x'$ is called an *affine combination* of the vectors x and x'.

A *vector subspace* of $\mathbf{R}^n$ is a nonempty subset W of $\mathbf{R}^n$ such that, if $y,y' \in \mathbf{R}^n$ and $c,c' \in \mathbf{R}$, then $cy+c'y' \in W$. Equivalently, a subset W of $\mathbf{R}^n$ is a vector subspace if $0 \in W$ and if W contains all linear combinations of vectors in W.

Let $x \in \mathbf{R}^n$ and let W be a subset of $\mathbf{R}^n$. The *translate* of W by the vector x is the set

$$x+W=\{x+w : w \in W\}.$$

An *affine subspace* of $\mathbf{R}^n$ is a translate of a subspace, that is, a subset of $\mathbf{R}^n$ of the form $L=x+W$, where $x \in \mathbf{R}^n$ and W is a vector subspace of $\mathbf{R}^n$. Thus, $x' \in L$ if and only if $x'=x+w$ for some $w \in W$. We call W the vector subspace associated with the affine subspace L. Because $0 \in W$, we have $x=x+0 \in L$.

Theorem 2.25. *Let L be the set of solutions of an inhomogeneous system of linear equations in n variables with coefficients in the field $\mathbf{R}$, and let W be the set of solutions of the associated homogeneous system. The set W is a vector subspace of $\mathbf{R}^n$, and the set L is an affine subspace with associated vector subspace W.*

For example, consider the inhomogeneous system

$$\begin{aligned} x+2y&=-1 \\ 2x+y&=4 \end{aligned}$$

and the associated homogeneous system

$$\begin{aligned} x+2y&=0 \\ 2x+y&=0. \end{aligned}$$

The homogeneous system has the unique solution $\begin{pmatrix}0\\0\end{pmatrix}$ and the inhomogeneous system has the unique solution $\begin{pmatrix}3\\-2\end{pmatrix}$. Thus, $W=\left\{\begin{pmatrix}0\\0\end{pmatrix}\right\}$ and $L=\left\{\begin{pmatrix}3\\-2\end{pmatrix}\right\}$.

Consider the inhomogeneous system

$$\begin{aligned} 2x+y+z&=2 \\ x-y-2z&=7 \end{aligned}$$

and the associated homogeneous system

$$\begin{aligned} 2x+y+z&=0 \\ x-y-2z&=0. \end{aligned}$$

The set of solutions of the homogeneous system is the vector subspace

$$W = \left\{ c \begin{pmatrix} 1 \\ -5 \\ 3 \end{pmatrix} : c \in \mathbf{R} \right\}.$$

One solution of the homogeneous system is $x = \begin{pmatrix} 3 \\ -4 \\ 0 \end{pmatrix}$, and so the affine subspace of solutions of the inhomogeneous system is

$$L = x + W = \left\{ \begin{pmatrix} 3 \\ -4 \\ 0 \end{pmatrix} + c \begin{pmatrix} 1 \\ -5 \\ 3 \end{pmatrix} : c \in \mathbf{R} \right\} = \left\{ \begin{pmatrix} 3+c \\ -4-5c \\ 3c \end{pmatrix} : c \in \mathbf{R} \right\}.$$

Exercises

1. a. Find all solutions of the homogenous equation

$$7x - 2y = 0.$$

Draw the graph of the vector subspace of solutions.

b. Find all solutions of the inhomogenous equation

$$7x - 2y = 3.$$

Draw the graph of the affine subspace of solutions.

2. a. Find all solutions of the system of homogenous equations

$$\begin{aligned} x + y + z &= 0 \\ 2x + y - z &= 0 \end{aligned}$$

Solution: $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2z \\ -3z \\ z \end{pmatrix}$

b. Find all solutions of the system of inhomogenous equations

$$\begin{aligned} x + y + z &= 6 \\ 2x + y - z &= 1 \end{aligned}$$

Solution: $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2z-5 \\ -3z+11 \\ z \end{pmatrix}$

3. Let W be a subspace of $\mathbf{R}^n$, let $v_0 \in \mathbf{R}^n$, and consider the affine subspace $L = v_0 + W$.

   a. Prove that if $v_1, v_2 \in L$, then $tv_1 + (1-t)v_2 \in L$ for all $t \in \mathbf{R}$.
   b. Let $v_1, \ldots, v_k \in L$, and let $t_1, \ldots, t_k \in \mathbf{R}$ satisfy $t_1 + \cdots + t_k = 1$. Prove that $t_1 v_1 + \cdots t_k v_k \in L$.

4. Let L be an affine subspace of $\mathbf{R}^n$, and let $u \in L$. Prove that $\{v - u : u \in L\}$ is a subspace of $\mathbf{R}^n$.

Chapter 3
Determinants and Permanents

In this chapter, R is a commutative ring and $M_n(R)$ is the noncommutative ring of $n \times n$ matrices with coordinates in R. We denote by $\mathbf{0}$ both the zero vector in R^n and the zero matrix in $M_n(R)$. The identity matrix in $M_n(R)$ is denoted by I or I_n.

3.1 Determinants of 2×2 matrices

Let R be a field or, more generally, a commutative ring. For every positive integer n, let

$$R^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in R \text{ for } i = 1, \ldots, n \right\}.$$

An element of R^n is called an *n-dimensional vector* with coordinates in R. We define the *vector addition* in R^n by

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

and *scalar multiplication* of a vector by an element $r \in R$ by

$$r \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} rx_1 \\ \vdots \\ rx_n \end{pmatrix}.$$

In this section we study 2-dimensional vectors and determinants. The *determinant* of a 2×2 matrix

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

with coordinates $a,b,c,d \in R$ is a function

$$\det : \mathrm{Mat}_2(R) \to R$$

defined by

$$\det(A) = ad - bc. \tag{3.1}$$

The determinant satisfies the following properties:

$$\begin{aligned}\det\begin{pmatrix} a+a' & c \\ b+b' & d\end{pmatrix} &= (a+a')d - (b+b')c = (ad-bc) + (a'd - b'c) \\ &= \det\begin{pmatrix} a & c \\ b & d\end{pmatrix} + \det\begin{pmatrix} a' & c \\ b' & d\end{pmatrix} \end{aligned} \tag{3.2}$$

and

$$\begin{aligned}\det\begin{pmatrix} ra & b \\ tc & d\end{pmatrix} &= (ra)d - b(rc) = r(ad-bc) \\ &= r\det\begin{pmatrix} a & b \\ c & d\end{pmatrix}. \end{aligned} \tag{3.3}$$

Similarly,

$$\det\begin{pmatrix} a & c+c' \\ b & d+d'\end{pmatrix} = \det\begin{pmatrix} a & c \\ b & d\end{pmatrix} + \det\begin{pmatrix} a & c' \\ b & d'\end{pmatrix} \tag{3.4}$$

and

$$\det\begin{pmatrix} a & rc \\ b & rd\end{pmatrix} = r\det\begin{pmatrix} a & c \\ b & d\end{pmatrix}. \tag{3.5}$$

We also have

$$\det\begin{pmatrix} c & a \\ d & b\end{pmatrix} = bc - ad = -(ad-bc) = -det\begin{pmatrix} a & c \\ b & d\end{pmatrix} \tag{3.6}$$

and

$$\det\begin{pmatrix} a & a \\ b & b\end{pmatrix} = ab - ab = 0. \tag{3.7}$$

The 2×2 matrix $A = \begin{pmatrix} a & c \\ b & d\end{pmatrix}$ is determined by its column vectors

$$\mathbf{v}_1 = \begin{pmatrix} a \\ b\end{pmatrix} \qquad \text{and} \qquad \mathbf{v}_2 = \begin{pmatrix} c \\ d\end{pmatrix}$$

and we often write

$$A = (\mathbf{v}_1, \mathbf{v}_2).$$

This defines a one-to-one correspondence between the set $\mathrm{Mat}_2(R)$ of 2×2 matrices and the set $R^2 \times R^2$ of ordered pairs of vectors in R^2. We can write

$$\det(A) = \det(\mathbf{v}_1, \mathbf{v}_2).$$

Thus, the determinant of a 2×2 matrix is also a function of the columns of the matrix, that is,

$$\det : R^2 \times R^2 \to R.$$

Let

$$\mathbf{v}'_1 = \begin{pmatrix} a' \\ b' \end{pmatrix}, \quad \text{and} \quad \mathbf{v}'_2 = \begin{pmatrix} c' \\ d' \end{pmatrix}.$$

We have

$$\begin{pmatrix} a+a' & c \\ b+b' & d \end{pmatrix} = (\mathbf{v}_1 + \mathbf{v}'_1, \mathbf{v}_2) \qquad \text{and} \qquad \begin{pmatrix} ra & c \\ rb & d \end{pmatrix} = (r\mathbf{v}_1, \mathbf{v}_2).$$

Similarly,

$$\begin{pmatrix} a & c+c'' \\ b & d+d' \end{pmatrix} = (\mathbf{v}_1, \mathbf{v}_2 + \mathbf{v}'_2) \qquad \text{and} \qquad \begin{pmatrix} a & rb \\ c & rd \end{pmatrix} = (\mathbf{v}_1, r\mathbf{v}_2).$$

Properties (3.2), (3.3), (3.4), and (3.5) can be expressed as follows: For all vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}'_1, \mathbf{v}'_2 \in R^2$ and scalars $r \in R$,

$$\begin{aligned} \det(\mathbf{v}_1 + \mathbf{v}'_1, \mathbf{v}_2) &= \det(\mathbf{v}_1, \mathbf{v}_2) + \det(\mathbf{v}'_1, \mathbf{v}_2) \\ \det(r\mathbf{v}_1, \mathbf{v}_2) &= r\det(\mathbf{v}_1, \mathbf{v}_2) \\ \det(\mathbf{v}_1, \mathbf{v}_2 + \mathbf{v}'_2) &= \det(\mathbf{v}_1, \mathbf{v}_2) + \det(\mathbf{v}_1, \mathbf{v}'_2) \\ \det(\mathbf{v}_1, r\mathbf{v}_2) &= r\det(\mathbf{v}_1, \mathbf{v}_2). \end{aligned}$$

A function from $R^2 \times R^2$ into R with these properties is called *bilinear*.

Property (3.6) can be expressed as follows:

$$\det(\mathbf{v}_2, \mathbf{v}_1) = -\det(\mathbf{v}_1, \mathbf{v}_2).$$

A function with this property is called *alternating*. Note also that

$$\det(I) = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1.$$

The transpose of the matrix $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is $A^t = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We have

$$\det(A^t) = ad - cb = ad - bc = \det(A).$$

We can use determinants to solve systems of linear equations.

Theorem 3.1 (Cramer's rule). *Consider the system of equations*

$$\begin{aligned} ax+by &= r \\ cx+dy &= s. \end{aligned}$$

If $ad-bc$ is a unit, then

$$x = \frac{rd-bs}{ad-bc} = \frac{\det\begin{pmatrix} r & b \\ s & d \end{pmatrix}}{\det\begin{pmatrix} a & b \\ c & d \end{pmatrix}}$$

and

$$y = \frac{as-cr}{ad-bc} = \frac{\det\begin{pmatrix} a & r \\ c & s \end{pmatrix}}{\det\begin{pmatrix} a & b \\ c & d \end{pmatrix}}.$$

Proof. Multiply the first equation by d and the second equation by b. Subtraction gives

$$x \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ad-bc)x = rd-bs = \det\begin{pmatrix} r & b \\ s & d \end{pmatrix}.$$

Multiply the first equation by c and the second equation by a. Subtraction gives

$$y \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ad-bc)y = as-cr = \det\begin{pmatrix} a & r \\ c & s \end{pmatrix}.$$

We can divide by $ad-bc$ if it is a unit.

The determinant contains important geometrical information.

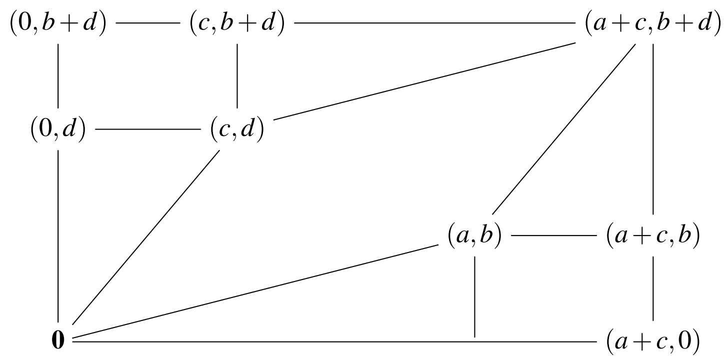
Theorem 3.2. *The area of the parallelogram in $\mathbf{R}^2$ with vertices*

$$\mathbf{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad \mathbf{v}_1 = \begin{pmatrix} a \\ b \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} c \\ d \end{pmatrix}, \quad \mathbf{v}_1 + \mathbf{v}_2 = \begin{pmatrix} a+c \\ b+d \end{pmatrix}$$

is

$$\left| \det\begin{pmatrix} a & c \\ b & d \end{pmatrix} \right| = |ad-bc|.$$

Proof. There are several cases. Consider the case where a,b,c,d are positive real numbers with $c < a$ and $b < d$. Consider the diagram



The area of the large rectangle is $(a+c)(b+d)$. Beginning at $\mathbf{0}$ and moving counterclockwise around the rectangle, we have a triangle of area $ab/2$, a small rectangle of area bc, a triangle of area $cd/2$, a triangle of area $ab/2$, a small rectangle of area bc, and a triangle of area $cd/2$. Deleting the areas of the four triangles and two small rectangles from the area of the large rectangle, we obtain the area of the parallelogram:

$$\begin{aligned}
\text{Area} &= (a+c)(b+d) - (ab/2 + bc + cd/2 + ab/2 + bc + cd/2) \\
&= (ab + ad + bc + cd) - (ab + 2bc + cd) \\
&= ad - bc = \det \begin{pmatrix} a & c \\ b & d \end{pmatrix}.
\end{aligned}$$

There are corresponding diagrams for other configurations of the vectors $\mathbf{v}_1$ and $\mathbf{v}_2$.

Exercises

1. Let
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$
   a. Compute AB and BA.
   b. Prove that
   $$\det(A)\det(B) = \det(AB) = \det(BA).$$
   c. The *trace* of A is
   $$\text{trace}(A) = a + d.$$
   Prove that
   $$\text{trace}(AB) = \text{trace}(BA).$$
   d. Prove that

$$A^2 - (a+d)A + (ad-bc)I = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Equivalently, the matrix A is a root of the polynomial

$$x^2 - \text{trace}(A)x + \det(A)I = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

2. Prove Theorem 3.1.
3. Prove Theorem 3.2.
   Hint: If a,b,c,d are positive, then imbed the parallelogram into the rectangle with vertices $(0,0)$, $(a+b,0)$, $(0,c+d)$, and $(a+b,c+d)$, and decompose complement of the parallelogram into triangles and rectangles.
4. Let
   $$SL_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbf{Z} \text{ and } ad-bc = 1 \right\}.$$
   Prove that $SL_2(\mathbf{Z})$ is a multiplicative group.
5. Let N be a positive integer, and let
   $$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) : c = Nq \text{ for some integer q.} \right\}.$$
   Prove that $\Gamma_0(N)$ is a multiplicative group.
6. Let $SL_2(\mathbf{F})$ be the set of 2×2 matrices of determinant 1, that is,
   $$SL_2(\mathbf{F}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbf{F} \text{ and } ad-bc = 1 \right\}.$$
   Prove that $SL_2(\mathbf{F})$ is a multiplicative group.
7. Let
   $$GL_2(\mathbf{F}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbf{F} \text{ and } ad-bc \neq 0 \right\}.$$
   Prove that $GL_2(\mathbf{F})$ is a multiplicative group.

3.2 Alternating multilinear forms

Let R be a commutative ring, let n be a positive integer, and let

$$A = \begin{pmatrix} a_{1,1} & \dots & a_{1,j} & \dots & a_{1,n} \\ a_{2,1} & \dots & a_{2,j} & \dots & a_{2,n} \\ \vdots & & \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,j} & \dots & a_{n,n} \end{pmatrix} \tag{3.8}$$

be an $n \times n$ matrix with coordinates $a_{i,j} \in R$ for $i, j = 1, \ldots, n$. For $j = 1, \ldots, n$, the jth column of A is the n-dimensional column vector

$$\mathbf{v}_j = \mathrm{col}_j(A) = \begin{pmatrix} a_{1,j} \\ a_{2,j} \\ \vdots \\ a_{n,j} \end{pmatrix} \in R^n.$$

Let $M_n(R)$ be the set of all $n \times n$ matrices with coordinates in R. Every function of an $n \times n$ matrix can be considered as a function of the ordered sequence of n-dimensional column vectors of the matrix. Conversely, to every ordered sequence of n n-dimensional column vectors there is an associated $n \times n$ matrix, and every function of an ordered sequence of n n-dimensional column vectors can be considered as a function of the associated matrix.

A function D of n column vectors in R^n is *multilinear* or *n-linear* if it satisfies the following properties: For all $j \in \{1, \ldots, n\}$ and $c \in R$, and for all vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in R^n$ and $\mathbf{v}'_j \in R^n$, we have

$$\begin{aligned} &D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_j + \mathbf{v}'_j, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_n) \\ &\quad = D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_j, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_n) + D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}'_j, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_n) \end{aligned} \tag{3.9}$$

and

$$D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, c\mathbf{v}_j, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_n) = cD(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_j, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_n). \tag{3.10}$$

A *multilinear form* is a multilinear function $D : M_n(R) \to R$. For example, the 2×2 determinant is a multilinear form.

A multilinear form D is *alternating* if $D(\mathbf{v}_1, \ldots, \mathbf{v}_n) = 0$ whenever $\mathbf{v}_i = \mathbf{v}_{i+1}$ for some $i \in \{1, 2, \ldots, n-1\}$, that is, if two adjacent vectors are equal. For example, the 2×2 determinant is alternating.

In Section 3.4, we construct alternating multilinear forms on $M_n(R)$ for every positive integer n and every commutative ring R. In this section we deduce properties of such forms.

Theorem 3.3. *Let R be a commutative ring, and let $D : M_n(R) \to R$ be an alternating multilinear form. Let $A \in M_n(R)$, and let $\mathbf{v}_j = col_j(A)$ for $j = 1, \ldots, n$.*

(i) If the matrix A has a zero column, that is, if $\mathbf{v}_j = \mathbf{0}$ for some $j \in \{1, \ldots, n\}$, then $D(A) = 0$.
(ii) Interchanging two adjacent columns of a matrix changes the sign of D:

$$\begin{aligned} &D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_j, \mathbf{v}_{j+1}, \mathbf{v}_{j+2}, \ldots, \mathbf{v}_n) \\ &\quad = -D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \mathbf{v}_j, \mathbf{v}_{j+2}, \ldots, \mathbf{v}_n) \end{aligned}$$

(iii) Interchanging any two columns of a matrix changes the sign of D.

(iv) If the matrix A has two equal columns, that is, if $\mathbf{v}_j = \mathbf{v}_k$ for some $j \neq k$, then $D(A) = 0$.

Proof. Let A be a matrix whose jth column vector is $\mathbf{0}$. Because $0\mathbf{0} = \mathbf{0}$, the multilinearity condition (3.10) implies

$$\begin{aligned} D(A) &= D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{0}, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_n) \\ &= D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, 0\mathbf{0}, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_n) \\ &= 0D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{0}, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_n) \\ &= 0. \end{aligned}$$

Thus, the determinant of a matrix with a zero column is 0.

Let $j \in \{1, 2, \ldots, n-1\}$, and consider the $n \times n$ matrix

$$A = (\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_j, \mathbf{v}_{j+1}, \mathbf{v}_{j+2}, \ldots, \mathbf{v}_n).$$

Interchanging columns $\mathbf{v}_j$ and $\mathbf{v}_{j+1}$, we obtain the matrix

$$A' = (\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \mathbf{v}_j, \mathbf{v}_{j+2}, \ldots, \mathbf{v}_n).$$

Consider the matrix whose jth and $(j+1)$st columns are equal to $\mathbf{v}_j + \mathbf{v}_{j+1}$ and whose ith column if $\mathbf{v}_i$ for $i \neq j, j+1$. Applying multilinearity properties (3.9) and (3.10), we obtain

$$\begin{aligned} 0 &= D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_j + \mathbf{v}_{j+1}, \mathbf{v}_j + \mathbf{v}_{j+1}, \mathbf{v}_{j+2}, \ldots, \mathbf{v}_n) \\ &= D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_j, \mathbf{v}_j, \mathbf{v}_{j+2}, \mathbf{v}_n) + D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_j, \mathbf{v}_{j+1}, \mathbf{v}_{j+2}, \ldots, \mathbf{v}_n) \\ &\quad + D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \mathbf{v}_j, \mathbf{v}_{j+2}, \mathbf{v}_n) + D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \mathbf{v}_{j+1}, \mathbf{v}_{j+2}, \mathbf{v}_n) \\ &= D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_j, \mathbf{v}_{j+1}, \mathbf{v}_{j+2}, \mathbf{v}_n) + D(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \mathbf{v}_j, \mathbf{v}_{j+2}, \mathbf{v}_n) \\ &= D(A) + D(A') \end{aligned}$$

and so

$$D(A') = -D(A).$$

Let $j, k \in \{1, 2, \ldots, n\}$ with $j < k$. Consider the $n \times n$ matrix

$$A = (\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_j, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_{k-1}, \mathbf{v}_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n)$$

Successively interchanging column $\mathbf{v}_j$ with columns $\mathbf{v}_{j+1}, \mathbf{v}_{j+2}, \ldots, \mathbf{v}_k$, we obtain the matrix

$$A'' = (\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_{k-1}, \mathbf{v}_k, \mathbf{v}_j, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n).$$

Having performed $k - j$ interchanges of adjacent columns, we have

$$D(A'') = (-1)^{k-j} D(A).$$

Next, we successively interchange column $\mathbf{v}_k$ with columns $\mathbf{v}_{k-1}, \mathbf{v}_{k-2}, \ldots, \mathbf{v}_{j+1}$, and obtain the matrix

$$A''' = (\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{v}_k, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_{k-1}, \mathbf{v}_j, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n).$$

Having performed $k-j-1$ interchanges of adjacent columns, we have

$$D(A''') = (-1)^{k-j-1} D(A'') = (-1)^{k-j-1}(-1)^{k-j} D(A) = -D(A).$$

Thus, the interchange of any two different columns of a matrix changes the sign of the determinant.

It follows that if two columns of a matrix A are equal, then their interchange changes the sign of the $D(A)$, but does not change the matrix, and so does not change $D(A)$. Therefore, $-D(A) = D(A) = 0$. This completes the proof.

Exercises

1. Let A be an $n \times n$ matrix.

   a. Prove that
   $$D(P^{-1}AP) = D(A)$$
   for every $n \times n$ invertible matrix P.

   b. Prove that if A is invertible, then
   $$D\left(A^{-1}\right) = D(A)^{-1}.$$

2. Let $A = (a_{i,j}) \in M_n(R)$.

   a. Prove that the function $f : M_n(R) \to R$ defined by
   $$f(A) = a_{1,1}a_{2,1} \cdots a_{n,1}$$
   is multilinear.

   b. For every function $\lambda : \{1, \ldots, n\} \to \{1, \ldots, n\}$, prove that the function $f^{(\lambda)} : M_n(R) \to R$ defined by
   $$F^{(\lambda)}(A) = a_{\lambda(1),1}a_{\lambda(2),2} \cdots a_{\lambda(n),n}$$
   is multilinear.

3.3 Permutations acting on matrices

Let G be a multiplicative group with identity element e, and let X be a set. An *action* of the group G on the set X is a function from $G \times X$ into X (denoted $(\sigma, x) \mapsto \sigma x$) such that

$$ex = x$$

and

$$(\sigma\tau)x = \sigma(\tau x)$$

for all $x \in X$ and $\sigma, \tau \in G$.

Let n be a positive integer, and let S_n be the group of permutations of the set $\{1, 2, \ldots, n\}$. We construct an action of S_n on the set $M_n(R)$ as follows. Let $A \in M_n(R)$, and let

$$\mathbf{v}_j = \mathrm{col}_j(A)$$

for $j = 1, \ldots, n$. The matrix σA has column vectors

$$\mathrm{col}_j(\sigma A) = \mathrm{col}_{\sigma^{-1}(j)}(A) = \mathbf{v}_{\sigma^{-1}(j)}$$

for $j = 1, \ldots, n$. Thus, the jth column of the matrix σA is the $\sigma^{-1}(j)$th column of A, and so

$$\sigma A = \left(\mathbf{v}_{\sigma^{-1}(1)}, \ldots, \mathbf{v}_{\sigma^{-1}(n)}\right). \tag{3.11}$$

Because $\left(\sigma^{-1}\right)^{-1} = \sigma$, we have

$$\sigma^{-1} A = \left(\mathbf{v}_{\sigma(1)}, \ldots, \mathbf{v}_{\sigma(n)}\right) \tag{3.12}$$

for all $\sigma \in S_n$.

For example, let $n = 3$, and consider the permutations $\sigma = (1, 2, 3) \in S_3$ and $\tau = (1, 2) \in S_3$ with inverses $\sigma^{-1} = (1, 3, 2)$ and $\tau^{-1} = \tau$. Let

$$A = \begin{pmatrix} 5 & 2 & 8 \\ 1 & 7 & 9 \\ 0 & 4 & 3 \end{pmatrix} \in M_3(R).$$

We have

$$\mathrm{col}_1(A) = \begin{pmatrix} 5 \\ 1 \\ 0 \end{pmatrix}, \quad \mathrm{col}_2(A) = \begin{pmatrix} 2 \\ 7 \\ 4 \end{pmatrix}, \quad \mathrm{col}_3(A) = \begin{pmatrix} 8 \\ 9 \\ 3 \end{pmatrix}$$

and so

$$\mathrm{col}_1(\sigma A) = \mathrm{col}_{\sigma^{-1}(1)}(A) = \mathrm{col}_3(A) = \begin{pmatrix} 8 \\ 9 \\ 3 \end{pmatrix}$$

$$\mathrm{col}_2(\sigma A) = \mathrm{col}_{\sigma^{-1}(2)}(A) = \mathrm{col}_1(A) = \begin{pmatrix} 5 \\ 1 \\ 0 \end{pmatrix}$$

and

$$\mathrm{col}_3(\sigma A) = \mathrm{col}_{\sigma^{-1}(3)}(A) = \mathrm{col}_2(A) = \begin{pmatrix} 2 \\ 7 \\ 4 \end{pmatrix}.$$

Therefore,

$$\sigma A = \begin{pmatrix} 8 & 5 & 2 \\ 9 & 1 & 7 \\ 3 & 0 & 4 \end{pmatrix}.$$

Similarly,

$$\tau A = \begin{pmatrix} 2 & 5 & 8 \\ 7 & 1 & 9 \\ 4 & 0 & 3 \end{pmatrix} \qquad \text{and} \qquad \sigma(\tau(A)) = \begin{pmatrix} 8 & 2 & 5 \\ 9 & 7 & 1 \\ 3 & 4 & 0 \end{pmatrix}.$$

Because $\sigma\tau = (1,3)$, we have

$$(\sigma\tau)A = \begin{pmatrix} 8 & 2 & 5 \\ 9 & 7 & 1 \\ 3 & 4 & 0 \end{pmatrix}.$$

It is important to observe that $(\sigma\tau)A = \sigma(\tau(A))$.

Theorem 3.4. *Equation* (3.11) *defines an action of the permutation group S_n on the set $M_n(R)$.*

Let D be an alternating multilinear form on $M_n(R)$. For every permutation σ in S_n,

$$D(\sigma A) = sgn(\sigma)D(A) \tag{3.13}$$

where $sgn(\sigma) \in \{\pm 1\}$ is the sign of σ.

Proof. We must show that, for all matrices $A \in M_n(R)$ and permutations $\sigma, \tau \in S_n$,

$$(\sigma\tau)A = \sigma(\tau(A)). \tag{3.14}$$

Recall that

$$(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}.$$

Let $B = \tau A$. For $j,k = 1,\ldots,n$, let

$$\mathbf{v}_j = \mathrm{col}_j(A) \quad \text{and} \quad \mathbf{w}_k = \mathrm{col}_k(B).$$

We have

$$\mathbf{w}_k = \mathrm{col}_k(\tau A) = \mathrm{col}_{\tau^{-1}(k)}(A) = \mathbf{v}_{\tau^{-1}(k)}$$

and so

$$\begin{aligned}\mathrm{col}_k(\sigma(\tau A)) &= \mathrm{col}_k(\sigma B) = \mathrm{col}_{\sigma^{-1}(k)}(B) \\ &= \mathbf{w}_{\sigma^{-1}(k)} = \mathbf{v}_{\tau^{-1}(\sigma^{-1}(k))} \\ &= \mathbf{v}_{(\tau^{-1}\sigma^{-1})(k)} = \mathbf{v}_{(\sigma\tau)^{-1}(k)} \\ &= \mathrm{col}_k((\sigma\tau)A).\end{aligned}$$

This proves (3.14).

Let $\sigma \in S_n$. If $\tau_1, \tau_2, \ldots, \tau_\ell$ are transpositions in S_n such that $\sigma = \tau_\ell \cdots \tau_2\tau_1$, then $\mathrm{sgn}(\sigma) = (-1)^\ell$ by Theorem 3.13. Let $A_0 = A$. For $k = 1, \ldots, \ell$, define the matrix $A_k \in M_n(R)$ by

$$A_k = (\tau_k \cdots \tau_2\tau_1)A = \tau_k(\tau_{k-1} \cdots \tau_2\tau_1)A = \tau_k A_{k-1}.$$

The transposition τ_k interchanges two columns of A. If $D(A_{k-1}) = (-1)^{k-1}D(A)$, then, by Theorem 3.3 (iii),

$$D(A_k) = -D(A_{k-1}) = -(-1)^{k-1}D(A) = (-1)^k D(A).$$

It follows by induction that

$$D(\sigma A) = D(A_\ell) = (-1)^\ell D(A) = \mathrm{sgn}(\sigma)D(A).$$

This proves (3.13).

Theorem 3.5. *If $D : M_n(R) \to R$ is a multilinear form such that* $\det(A) = 0$ *if A has two equal adjacent columns, then*

$$D(A) = D(I)\det(A).$$

Corollary 3.1. *The determinant* det *is the unique multilinear form such that* $\det(A) = 0$ *if A has two equal adjacent columns and* $\det(I) = 1$.

Theorem 3.6. *For all matrices A and B in $M_n(R)$,*

$$\det(AB) = \det(A)\det(B).$$

Proof. Fix the matrix A, and define $D : M_n(R) \to R$ by

$$D(B) = \det(AB)$$

for all $B \in M_n(R)$. Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be the sequence of ordered column vectors of B. We have $\det(B) = \det(\mathbf{v}_1, \ldots, \mathbf{v}_n)$. The sequence of ordered column vectors of the $n \times n$ matrix AB is $A\mathbf{v}_1, \ldots, A\mathbf{v}_n$, and so

$$D(B) = \det(A\mathbf{v}_1, \ldots, A\mathbf{v}_n).$$

This is an alternating multilinear form with

$$D(I) = \det(A)$$

and so, by Theorem 3.5,

$$\det(AB) = D(B) = D(I)\det(B) = \det(A)\det(B).$$

This completes the proof.

Theorem 3.7. *Let D be an alternating multilinear form on $M_n(R)$, and let I be the $n \times n$ identity matrix. For all matrices $A, B \in M_n(R)$,*

$$D(B) = D(I) \sum_{\sigma \in S_n} sgn(\sigma) b_{\sigma(1),1} \cdots b_{\sigma(n),n} \tag{3.15}$$

and

$$D(I)D(AB) = D(A)D(B). \tag{3.16}$$

Equation (3.15) implies that an alternating multilinear form on $M_n(R)$ is uniquely determined by the scalar $D(I)$.

Proof. Let $A = (a_{i,j})$ and $B = (b_{i,j})$ be matrices in $M_n(R)$ with column vectors

$$\mathbf{v}_j = \operatorname{col}_j(A) = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{n,j} \end{pmatrix} \quad \text{and} \quad \mathbf{w}_j = \operatorname{col}_j(B) = \begin{pmatrix} b_{1,j} \\ \vdots \\ b_{n,j} \end{pmatrix}$$

for $j = 1, \ldots, n$. By Chapter **??**, Theorem 2.10, the product matrix $AB = C$ has column vectors

$$\mathbf{x}_j = \operatorname{col}_j(C) = A\mathbf{w}_j = \sum_{i=1}^{n} b_{i,j}\mathbf{v}_i.$$

Let D be an alternating multilinear form on $M_n(R)$. Because D is multilinear, we have

$$\begin{aligned} D(AB) = D(C) &= D(\mathbf{x}_1, \ldots, \mathbf{x}_j, \ldots, \mathbf{x}_n) \\ &= D\left(\sum_{i_1=1}^{n} b_{i_1,1}\mathbf{v}_{i_1}, \ldots, \sum_{i_j=1}^{n} b_{i_j,j}\mathbf{v}_{i_j}, \ldots, \sum_{i_n=1}^{n} b_{i_n,n}\mathbf{v}_{i_n} \right) \\ &= \sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} b_{i_1,1} \cdots b_{i_n,n} D(\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_n}). \end{aligned}$$

Because D is alternating, by Theorem 3.3 (iv), we have

$$D(\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_n}) = 0$$

if $i_j = i_k$ for some $j \neq k$, and so

$$D(AB) = \underbrace{\sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n}}_{\{1_1,\ldots,i_n\}=\{1,\ldots,n\}} b_{i_1,1} \cdots b_{i_n,n} D(\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_n}).$$

The identity

$$\{\sigma(1),\ldots,\sigma(n)\} = \{1,\ldots,n\}$$

establishes a one-to-one correspondence between permutations $\sigma \in S_n$ and n-tuples $(i_1,\ldots,i_n)$ such that

$$\{i_1,\ldots,i_n\} = \{1,\ldots,n\}.$$

Applying identity (3.12) and Lemma 3.1, we obtain

$$\begin{aligned}
D(AB) &= \underbrace{\sum_{i_1=1}^{n}\cdots\sum_{i_n=1}^{n}}_{\{1_1,\ldots,i_n\}=\{1,\ldots,n\}} b_{i_1,1}\cdots b_{i_n,n} D\left(\mathbf{v}_{i_1},\ldots,\mathbf{v}_{i_n}\right) \\
&= \sum_{\sigma\in S_n} b_{\sigma(1),1}\cdots b_{\sigma(n),n} D\left(\mathbf{v}_{\sigma(1)},\ldots,\mathbf{v}_{\sigma(n)}\right) \\
&= \sum_{\sigma\in S_n} b_{\sigma(1),1}\cdots b_{\sigma(n),n} D\left(\sigma^{-1}A\right) \\
&= D(A)\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma^{-1}) b_{\sigma(1),1}\cdots b_{\sigma(n),n}
\end{aligned}$$

and so

$$D(AB) = D(A)\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{\sigma(1),1}\cdots b_{\sigma(n),n} \tag{3.17}$$

Choosing $A = I$, we obtain (3.15). Multiplying formula (3.17) by $D(I)$ and applying (3.15) yields the product formula (3.16). This completes the proof.

Let $k \in \{1,\ldots,n-1\}$, and let $A = (a_{i,j})$ be the $n\times n$ matrix such

$$a_{i,j} = \begin{cases} \delta_{i,j} & \text{if } j \neq k, k+1 \\ \delta_{i,k} & \text{if } j = k \text{ and } i \neq k+1 \\ 1 & \text{if } j = k \text{ and } i = k+1 \\ 0 & \text{if } j = k+1. \end{cases}$$

For example, if $n = 3$ and $k = 1$, then

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

and

$$AB = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & b & c \\ g & h & i \end{pmatrix}.$$

If $n = 3$ and $k = 2$, then

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

and

$$AB = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ d & e & f \end{pmatrix}.$$

Then $\det(A) = 0$ because the $(k+1)$st column of A is the n-dimensional zero vector, and so

$$\det(AB) = \det(A)\det(B) = 0.$$

If B is any $n \times n$ matrix, then AB is the $n \times n$ matrix whose ith row is the ith row of B for all $i \neq k+1$, and whose $(k+1)$st row is the same as the kth row of B. In particular, if B is any matrix whose kth and $(k+1)$st rows are equal, then $AB = B$ and $\det(B) = 0$. Thus, the determinant of a matrix in which two adjacent rows are equal is 0.

Let $k \in \{1, \ldots, n\}$. By formula (**??**), the determinant of a $n \times n$ matrix is a sum of $n!$ terms, each of which contains exactly one element from the kth row of A. It follows that the determinant of an $n \times n$ matrix is a multilinear function of the rows of the matrix.

Thus, the determinant function also satisfies

DetRow1: $\det(A)$ is a multilinear function of the rows of A,
DetRow2: $\det(A) = 0$ if two adjacent rows of A are equal,
DetIden: $\det(I_n) = 1$ if I_n is the $n \times n$ identity matrix.

For example, if $n = 4$ and $k = 2$, then

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

If B is any 4×4 matrix, then AB is the matrix whose first, second, and fourth rows are the first, second, and fourth rows of B, respectively, and whose third row is the second row of B.

3.4 Construction of the determinant

Let R be a commutative associative ring. For every positive integer n, we shall construct an alternating multilinear form D_n on $M_n(R)$ such that $D_n(I) = 1$. We use induction on n.

Every 1×1 matrix A is of the form $A = (a)$. We define

$$D_1(A) = a.$$

For $A' = (a')$ and $c \in R$, we have

$$\det_1(A + cA') = a + ca' = \det_1(A) + c\det_1(A')$$

and so $\det_1$ is multilinear. Also, $I_1 = (1)$, and $\det(I_1) = 1$. Thus, $\det_1$ satisfies properties (i), (ii), and (iii).

Let $n \geq 2$, and suppose that we have defined the determinant function $\det_{n-1}$ on the set of $(n-1) \times (n-1)$ matrices. Consider the $n \times n$ matrix $A = (a_{i,j})$. For each ordered pair of integers (i, j) with $i, j \in \{1, \ldots, n\}$, the *matrix minor* $\tilde{A}_{i,j}$ is the $(n-1) \times (n-1)$ matrix obtained from A by deleting the ith row and the jth column. The (i, j)th *cofactor* of A, denoted $\operatorname{cof}(\tilde{A}_{i,j})$, is the determinant of the $(n-1) \times (n-1)$ matrix $\tilde{A}_{i,j}$ multiplied by $(-1)^{i+j}$.

Here are three examples. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

For $i = 1$ and $j = 1, 2$, the matrix A has minors

$$\tilde{A}_{1,1} = \left(d\right), \quad \tilde{A}_{1,2} = \left(c\right)$$

and cofactors

$$\operatorname{cof}(\tilde{A}_{1,1}) = d, \quad \operatorname{cof}(\tilde{A}_{1,2}) = -c.$$

We have

$$\sum_{j=1}^{2} a_{1,j} \operatorname{cof}\left(\tilde{A}_{1,j}\right) = a(d) + b(-c) = ad - bc.$$

For $i = 2$ and $j = 1, 2$, the matrix A has minors

$$\tilde{A}_{2,1} = \left(b\right), \quad \tilde{A}_{2,2} = \left(a\right)$$

and cofactors

$$\operatorname{cof}(\tilde{A}_{2,1}) = -b, \quad \operatorname{cof}(\tilde{A}_{2,2}) = a.$$

We have

$$\sum_{j=1}^{2} a_{2,j} \operatorname{cof}\left(\tilde{A}_{1,j}\right) = c(-b) + d(a) = ad - bc.$$

Consider the 3×3 matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

For $i = 1$ and $j = 1, 2, 3$, the matrix A has minors

$$\tilde{A}_{1,1} = \begin{pmatrix} 5 & 6 \\ 8 & 9 \end{pmatrix}, \quad \tilde{A}_{1,2} = \begin{pmatrix} 4 & 6 \\ 7 & 9 \end{pmatrix}, \quad \tilde{A}_{1,3} = \begin{pmatrix} 4 & 5 \\ 7 & 8 \end{pmatrix}$$

and cofactors

$$\operatorname{cof}(\tilde{A}_{1,1}) = -3, \quad \operatorname{cof}(\tilde{A}_{1,2}) = 6, \quad \operatorname{cof}(\tilde{A}_{1,3}) = -3.$$

We have

$$\sum_{j=1}^{3} a_{1,j} \operatorname{cof}\left(\tilde{A}_{1,j}\right) = 1(-3) + 2(6) + 3(-3) = 0.$$

For $i = 2$ and $j = 1, 2, 3$, the matrix A has minors

$$\tilde{A}_{2,1} = \begin{pmatrix} 2 & 3 \\ 8 & 9 \end{pmatrix}, \quad \tilde{A}_{2,2} = \begin{pmatrix} 1 & 3 \\ 7 & 9 \end{pmatrix}, \quad \tilde{A}_{2,3} = \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix}$$

and cofactors

$$\operatorname{cof}(\tilde{A}_{2,1}) = 6 \quad \operatorname{cof}(\tilde{A}_{2,2}) = -12, \quad \operatorname{cof}(\tilde{A}_{2,3}) = 6.$$

We have

$$\sum_{j=1}^{3} a_{2,j} \operatorname{cof}\left(\tilde{A}_{2,j}\right) = 4(6) + 5(-12) + 6(6) = 0.$$

For $i = 3$ and $j = 1, 2, 3$, the matrix A has minors

$$\tilde{A}_{3,1} = \begin{pmatrix} 2 & 3 \\ 5 & 6 \end{pmatrix}, \quad \tilde{A}_{3,2} = \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}, \quad \tilde{A}_{3,3} = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}$$

and cofactors

$$\operatorname{cof}(\tilde{A}_{3,1}) = -3 \quad \operatorname{cof}(\tilde{A}_{3,2}) = 6, \quad \operatorname{cof}(\tilde{A}_{3,3}) = -3.$$

We have

$$\sum_{j=1}^{3} a_{3,j} \operatorname{cof}\left(\tilde{A}_{3,j}\right) = 7(-3) + 8(6) + 9(-3) = 0.$$

For the $n \times n$ identity matrix $I = (\delta_{i,j})$, the matrix minor $\tilde{I}_{i,i}$ is the $(n-1) \times (n-1)$ identity matrix, and, for $i \neq j$, the ith column of the matrix minor $\tilde{I}_{i,j}$ is the zero column. It follows that, for all $i = 1, \ldots, n$,

$$\operatorname{cof}(\tilde{I}_{i,j}) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

and

$$\sum_{j=1}^{n} \delta_{i,j} \operatorname{cof}\left(\tilde{A}_{i,j}\right) = \operatorname{cof}\left(\tilde{A}_{i,i}\right) = 1. \tag{3.18}$$

Theorem 3.8. . *Let $A = (a_{i,j})$ be an $n \times n$ matrix with coordinates in a commutative ring R. For $i = 1, \ldots, n$, define*

$$D_i(A) = \sum_{j=1}^{n} a_{i,j} \, cof\left(\tilde{A}_{i,j}\right). \tag{3.19}$$

For all $i = 1, \ldots, n$,

(i) $D_i : M_n(R) \to R$ is a multilinear form,
(ii) $D_i : M_n(R) \to R$ is an alternating form,
(iii) $D_i(I) = 1$.

Proof. (i) Let $k \in \{1, \ldots, n\}$. Consider the $n \times n$ matrix

$$A = (\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}, \mathbf{v}_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n)$$

with column vectors

$$\mathbf{v}_j = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{n,j} \end{pmatrix} \in R^n$$

for $j = 1, \ldots, n$. Suppose that, for $i = 1, \ldots, n$,

$$a_{i,k} = c a'_{i,k} + a''_{i,k}$$

and so

$$\mathbf{v}_k = c\mathbf{v}'_k + \mathbf{v}''_k$$

where

$$\mathbf{v}'_k = \begin{pmatrix} a'_{1,k} \\ \vdots \\ a'_{n,k} \end{pmatrix} \in R^n \qquad \text{and} \qquad \mathbf{v}''_k = \begin{pmatrix} a''_{1,k} \\ \vdots \\ a''_{n,k} \end{pmatrix} \in R^n.$$

We have

$$A = (\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}, c\mathbf{v}'_k + \mathbf{v}''_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n)$$

Define the $n \times n$ matrices

$$B = (\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}, \mathbf{v}'_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n)$$

and

$$C = (\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}, \mathbf{v}''_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n).$$

Let $i \in \{1, \ldots, n\}$. The function D_i is multilinear if

$$D_i(A) = cD_i(B) + D_i(C).$$

The matrices A, B, and C differ only in the kth column, and so there are equal matrix minors

$$\tilde{A}_{i,k} = \tilde{B}_{i,k} = \tilde{C}_{i,k}$$

and equal cofactors

$$\operatorname{cof}\left(\tilde{A}_{i,k}\right) = \operatorname{cof}\left(\tilde{B}_{i,k}\right) = \operatorname{cof}\left(\tilde{C}_{i,k}\right) = (-1)^{i+k} \det\left(\tilde{A}_{i,k}\right).$$

Therefore,

$$\begin{aligned} a_{i,k} \operatorname{cof}\left(\tilde{A}_{i,k}\right) &= (ca'_{i,k} + a''_{i,k}) \operatorname{cof}\left(\tilde{A}_{i,k}\right) \\ &= ca'_{i,k} \operatorname{cof}\left(\tilde{A}_{i,k}\right) + a''_{i,k} \operatorname{cof}\left(\tilde{A}_{i,k}\right) \\ &= ca'_{i,k} \operatorname{cof}\left(\tilde{B}_{i,k}\right) + a''_{i,k} \operatorname{cof}\left(\tilde{C}_{i,k}\right). \end{aligned}$$

For $j \neq k$, the matrix minors $\tilde{A}_{i,j}, \tilde{B}_{i,j}, \tilde{C}_{i,j}$ are $(n-1) \times (n-1)$ matrices of the form

$$\begin{aligned} \tilde{A}_{i,j} &= (\mathbf{w}_1, \ldots, \mathbf{w}_k, \ldots, \mathbf{w}_n) \\ \tilde{B}_{i,j} &= (\mathbf{w}_1, \ldots, \mathbf{w}'_k, \ldots, \mathbf{w}_n) \\ \tilde{C}_{i,j} &= (\mathbf{w}_1, \ldots, \mathbf{w}''_k, \ldots, \mathbf{w}_n) \end{aligned}$$

where the column vectors arising from $\mathbf{v}_j$ are omitted, and

$$\mathbf{w}_k = c\mathbf{w}'_k + \mathbf{w}''_k.$$

The multilinearity of the $(n-1)$-dimensional determinant implies that

$$\begin{aligned} \operatorname{cof}\left(\tilde{A}_{i,j}\right) &= (-1)^{i+j} \det\left(\tilde{A}_{i,j}\right) \\ &= (-1)^{i+j} \det(\mathbf{w}_1, \ldots, \mathbf{w}_k, \ldots, \mathbf{w}_n) \\ &= (-1)^{i+j} \det(\mathbf{w}_1, \ldots, c\mathbf{w}'_k + \mathbf{w}''_k, \ldots, \mathbf{w}_n) \\ &= c(-1)^{i+j} \det(\mathbf{w}_1, \ldots, \mathbf{w}'_k, \ldots, \mathbf{w}_n) + (-1)^{i+j} \det(\mathbf{w}_1, \ldots, \mathbf{w}''_k, \ldots, \mathbf{w}_n) \\ &= c \operatorname{cof}\left(\tilde{B}_{i,j}\right) + \operatorname{cof}\left(\tilde{C}_{i,j}\right). \end{aligned}$$

We have

$$D_i(B) = \sum_{\substack{j=1 \\ j \neq k}}^{n} a_{i,j} \operatorname{cof}\left(\tilde{B}_{i,j}\right) + a'_{i,k} \operatorname{cof}\left(\tilde{B}_{i,k}\right)$$

$$D_i(C) = \sum_{\substack{j=1 \\ j \neq k}}^{n} a_{i,j} \operatorname{cof}\left(\tilde{C}_{i,j}\right) + a''_{i,k} \operatorname{cof}\left(\tilde{C}_{i,k}\right)$$

and so

$$\begin{aligned}
D_i(A) &= \sum_{\substack{j=1\\ j\neq k}}^{n} a_{i,j}\operatorname{cof}\left(\tilde{A}_{i,j}\right) + a_{i,k}\operatorname{cof}\left(\tilde{A}_{i,k}\right)\\
&= \sum_{\substack{j=1\\ j\neq k}}^{n} a_{i,j}\left(c\operatorname{cof}\left(\tilde{B}_{i,j}\right) + \operatorname{cof}\left(\tilde{C}_{i,j}\right)\right) + ca'_{i,k}\operatorname{cof}\left(\tilde{B}_{i,k}\right) + a''_{i,k}\operatorname{cof}\left(\tilde{C}_{i,k}\right)\\
&= c\left(\sum_{\substack{j=1\\ j\neq k}}^{n} a_{i,j}\operatorname{cof}\left(\tilde{B}_{i,j}\right) + a'_{i,k}\operatorname{cof}\left(\tilde{B}_{i,k}\right)\right)\\
&\qquad\qquad + \sum_{\substack{j=1\\ j\neq k}}^{n} a_{i,j}\operatorname{cof}\left(\tilde{C}_{i,j}\right) + a''_{i,k}\operatorname{cof}\left(\tilde{C}_{i,k}\right)\\
&= cD_i(B) + D_i(C).
\end{aligned}$$

This proves that D_i is a multilinear form.

(ii) If the matrix A has two equal and adjacent columns, then there exists $k \in \{1,\ldots,n-1\}$.such that $\operatorname{col}_k(A) = \operatorname{col}_{k+1}(A)$, and the matrix minors $\tilde{A}_{i,k}$ and $\tilde{A}_{i,k+1}$ are equal. Therefore,

$$\begin{aligned}
\operatorname{cof}\left(\tilde{A}_{i,k}\right) + \operatorname{cof}\left(\tilde{A}_{i,k+1}\right) &= (-1)^{i+k}\det\left(\tilde{A}_{i,k}\right) + (-1)^{i+k+1}\det\left(\tilde{A}_{i,k+1}\right)\\
&= (-1)^{i+k}\left(\det\left(\tilde{A}_{i,k}\right) - \det\left(\tilde{A}_{i,k}\right)\right)\\
&= 0.
\end{aligned}$$

For all $i,j \in \{1,\ldots,n\}$ with $j \neq k, k+1$, the matrix minor $\tilde{A}_{i,j}$ has two adjacent equal columns, and so $\operatorname{cof}(\tilde{A}_{i,j}) = 0$. Because $a_{i,k} = a_{i,k+1}$, we have

$$\begin{aligned}
D_i(A) &= \sum_{j=1}^{n} a_{i,j}\operatorname{cof}\left(\tilde{A}_{i,j}\right)\\
&= a_{i,k}\operatorname{cof}\left(\tilde{A}_{i,k}\right) + a_{i,k+1}\operatorname{cof}\left(\tilde{A}_{i,k+1}\right)\\
&= a_{i,k}\left(\operatorname{cof}\left(\tilde{A}_{i,k}\right) + \operatorname{cof}\left(\tilde{A}_{i,k+1}\right)\right)\\
&= 0.
\end{aligned}$$

Thus, D_i is an alternating form for all $i \in \{1,\ldots,n\}$.

(iii) Equation (3.18) is equivalent to (ii).

Corollary 3.2. *For $A \in M_n(R)$, define the linear form $D_i(A)$ by* (3.19). *Then*

$$D_1(A) = D_2(A) = \cdots = D_n(A) = \det(A).$$

Here is the definition of the determinant: For any $i \in \{1,\ldots,n\}$,

$$\det(A) = D_i(A) = \sum_{j=1}^{n} a_{i,j}\operatorname{cof}\left(\tilde{A}_{i,j}\right).$$

For example, the 3×3 matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

has the matrix minors

$$\tilde{A}_{1,1} = \begin{pmatrix} 5 & 6 \\ 8 & 9 \end{pmatrix}, \qquad \tilde{A}_{1,2} = \begin{pmatrix} 4 & 6 \\ 7 & 9 \end{pmatrix}, \qquad \tilde{A}_{1,3} = \begin{pmatrix} 4 & 5 \\ 7 & 8 \end{pmatrix}$$

and the corresponding cofactors

$$\begin{aligned}
\operatorname{cof}(\tilde{A}_{1,1}) &= (-1)^{1+1} \det \begin{pmatrix} 5 & 6 \\ 8 & 9 \end{pmatrix} = -3 \\
\operatorname{cof}(\tilde{A}_{1,2}) &= (-1)^{1+2} \det \begin{pmatrix} 4 & 6 \\ 7 & 9 \end{pmatrix} = (-1)(-6) = 6 \\
\operatorname{cof}(\tilde{A}_{1,3}) &= (-1)^{1+3} \det \begin{pmatrix} 4 & 5 \\ 7 & 8 \end{pmatrix} = -3.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\det(A) &= a_{1,1} \operatorname{cof}(\tilde{A}_{1,1}) + a_{1,2} \operatorname{cof}(\tilde{A}_{1,2}) + a_{1,3} \operatorname{cof}(\tilde{A}_{1,3}) \\
&= (1)(-3) + (2)(6) + 3(-3) \\
&= 0.
\end{aligned}$$

This implies that the columns of A are linearly dependent, and, indeed,

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \\ 7 \end{pmatrix} - 2 \begin{pmatrix} 2 \\ 5 \\ 8 \end{pmatrix} + \begin{pmatrix} 3 \\ 6 \\ 9 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

We shall also compute $\det(A)$ by expanding across the second row. We have the matrix minors

$$\tilde{A}_{2,1} = \begin{pmatrix} 2 & 3 \\ 8 & 9 \end{pmatrix}, \qquad \tilde{A}_{2,2} = \begin{pmatrix} 1 & 3 \\ 7 & 9 \end{pmatrix}, \qquad \tilde{A}_{2,3} = \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix}.$$

The corresponding cofactors are

$$\begin{aligned}
\operatorname{cof}(\tilde{A}_{2,1}) &= (-1)^{2+1} \det \begin{pmatrix} 2 & 3 \\ 8 & 9 \end{pmatrix} = (-1)(-6) = 6 \\
\operatorname{cof}(\tilde{A}_{2,2}) &= (-1)^{2+2} \det \begin{pmatrix} 1 & 3 \\ 7 & 9 \end{pmatrix} = -12 \\
\operatorname{cof}(\tilde{A}_{2,3}) &= (-1)^{2+3} \det \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix} = (-1)(-6) = 6
\end{aligned}$$

and so

$$\begin{aligned}\det(A) &= a_{2,1}\operatorname{cof}(\tilde{A}_{2,1}) + a_{2,2}\operatorname{cof}(\tilde{A}_{2,2}) + a_{2,3}\operatorname{cof}(\tilde{A}_{2,3})\\ &= (4)(6) + (5)(-12) + 6(6)\\ &= 0.\end{aligned}$$

Consider the 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Expanding across the first row, we obtain

$$\det(A) = a\operatorname{cof}\left(\tilde{A}_{1,1}\right) + b\operatorname{cof}\left(\tilde{A}_{1,2}\right) = ad + b(-1)c = ad - bc.$$

Expanding across the second row, we obtain

$$\det(A) = c\operatorname{cof}\left(\tilde{A}_{2,1}\right) + d\operatorname{cof}\left(\tilde{A}_{2,2}\right) = c(-1)b + da = ad - bc.$$

This is consistent with (3.1).

Exercises

1. Compute the determinant of the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ by expanding across the third row.
2. Compute the determinant of the following matrices:

   a.
   $$A_1 = \begin{pmatrix} 2 \end{pmatrix}$$

   b.
   $$A_2 = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

   c.
   $$A_3 = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$$

   d.
   $$A_4 = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$$

   e. Let $A_n = (a_{i,j})_{i,j=1}^{n} \in M_n(\mathbf{R})$ be the $n \times n$ matrix defined by

$$a_{i.j} = \begin{cases} 2 & \text{if } i = j \\ -1 & \text{if } |i-j| = 1 \\ 0 & \text{if } |i-j| \geq 2. \end{cases}$$

Prove that

$$\det(A_n) = 2\det(A_{n-1}) - \det(A_{n-2}) = n+1$$

for all $n \geq 1$.

3. Let $a, b \in R$ and $A_n = (a_{i,j})_{i,j=1}^n \in M_n(R)$ be the $n \times n$ matrix defined by

$$a_{i.j} = \begin{cases} a & \text{if } i = j \\ b & \text{if } |i-j| = 1 \\ 0 & \text{if } |i-j| \geq 2. \end{cases}$$

Prove that

$$\det(A_1) = a, \qquad \det(A_2) = a^2 - b^2$$

and

$$\det(A_n) = a\det(A_{n-1}) - b^2\det(A_{n-2}).$$

for all $n \geq 3$.

4. An $n \times n$ *tridiagonal matrix* is a matrix $(a_{i,j})_{i,j=1}^n \in M_n(R)$ such that $a_{i,j} = 0$ if $|i-j| \geq 2$. Let $(u_i)_{i=1}^\infty$, $(\mathbf{v}_i)_{i=1}^\infty$, and $(w_i)_{i=1}^\infty$ be sequences of elements of R, and let $A_n = (a_{i,j})_{i,j=1}^n$ be the $n \times n$ tridiagonal matrix defined by

$$a_{i.j} = \begin{cases} u_i & \text{if } i = j \\ \mathbf{v}_i & \text{if } j = i-1 \\ w_j & \text{if } i = j-1 \\ 0 & \text{if } |i-j| \geq 2. \end{cases}$$

For example,

$$A_1 = \begin{pmatrix} u_1 \end{pmatrix} \qquad \text{and} \qquad A_2 = \begin{pmatrix} u_1 & w_2 \\ \mathbf{v}_2 & u_2 \end{pmatrix}$$

a. Write the matrices A_3, A_4, and A_5.
b. Prove that

$$\det(A_1) = u_1, \qquad \det(A_2) = u_1u_2 - \mathbf{v}_2w_2$$

and

$$\det(A_n) = u_n\det(A_{n-1}) - \mathbf{v}_nw_n\det(A_{n-2}).$$

for all $n \geq 3$.

3.5 Determinant of the transpose

We recall some simple facts about permutations. For every permutation $\sigma \in S_n$,

$$\sigma(j) = i \quad \text{if and only if} \quad i = \sigma^{-1}(j)$$

$$\{\sigma(j) : j = 1, \ldots, n\} = \{1, \ldots, n\}$$

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$$

$$S_n = \{\sigma^{-1} : \sigma \in S_n\}.$$

The transpose of the $n \times n$ matrix $A = (a_{i,j})$ is the matrix $A^t = (a^t_{i,j})$, where

$$a^t_{i,j} = a_{j,i}.$$

Theorem 3.9. *Let A be an $n \times n$ matrix and let A^t be the transpose of A. Then*

$$\det(A) = \det(A^t).$$

Proof. The determinant of matrix $A = (a_{i,j})$ is

$$\begin{aligned}
\det(A) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{\sigma(j),\sigma^{-1}(\sigma(j))} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) \prod_{i=1}^{n} a_{i,\sigma^{-1}(i)} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a^t_{\sigma(i),i} \\
&= \det(A^t).
\end{aligned}$$

This completes the proof.

Corollary 3.3. *If two rows of a matrix A are equal, then $det(A) = 0$. If A' is a matrix obtained from A by interchanging two rows of A, then* $\det(A') = \det(A)$. *The determinant is an alternating bilinear form on the rows of a matrix.*

Proof. Let A be a matrix with transpose A^t. If A has two equal rows, then A^t has two equal columns. By Theorem 3.14,

$$\det(A) = \det(A^t) = 0.$$

The other statements are proved similarly.

3.6 The classical adjoint

For all $i \in \{1,\ldots,n\}$, the determinant of the $n \times n$ matrix $A = (a_{i,j})$ is

$$\det(A) = \sum_{j=1}^{n} a_{i,j} \operatorname{cof}(A)_{i,j} \tag{3.20}$$

where

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

is the (i,j)th cofactor of A.

Choose $k \in \{1,\ldots,n\}$ with $k \neq i$, and let $B = (b_{i,j})$ be the matrix A, but with row i replaced with row k. Thus,

$$b_{i,j} = \begin{cases} a_{i.j} & \text{if } i \neq k \\ a_{k,j} & \text{if } i = k. \end{cases}$$

We have $\det(B) = 0$ because every matrix with two equal rows has determinant 0. However, for every $j \in \{1,\ldots,n\}$ we have $\tilde{B}_{i,j} = \tilde{A}_{i,j}$, and so $\operatorname{cof}(B)_{i,j} = \operatorname{cof}(A)_{i,j}$. Therefore,

$$0 = \det(B) = \sum_{j=1}^{n} b_{i,j} \operatorname{cof}(B)_{i,j} = \sum_{j=1}^{n} a_{k,j} \operatorname{cof}(A)_{i,j}. \tag{3.21}$$

Combining (3.20) and (3.21), we obtain

$$\sum_{j=1}^{n} a_{k,j} \operatorname{cof}(A)_{i,j} = \det(A)\delta_{k,i}.$$

Consider the matrix whose (i,j)th coordinate is the cofactor $\operatorname{cof}(A)_{i,j}$. The *classical adjoint* of A, denoted $\operatorname{adj}(A)$, is the transpose of the matrix of cofactors, that is, the matrix whose (j,i)th coordinate is the cofactor $\operatorname{cof}(A)^t_{j,i} = \operatorname{cof}(A)_{i,j}$. Thus,

$$\sum_{j=1}^{n} a_{k,j} \operatorname{cof}(A)^t_{j,i} = \det(A)\delta_{k,i}$$

Other names for the classical adjoint of a matrix A are the *adjunct* and the *adjugate* of A.

Theorem 3.10. *For every $n \times n$ matrix A with coordinates in the commutative ring R,*

$$A \operatorname{adj}(A) = \det(A)I. \tag{3.22}$$

Theorem 3.11. *Let R be a commutative ring. The matrix $A \in M_n(R)$ is invertible if and only if* $\det(A)$ *is a unit in the ring R. If A is invertible, then*

$$A^{-1} = \det(A)^{-1} \operatorname{adj}(A). \tag{3.23}$$

Proof. If A is invertible, then there exists $B \in M_n(R)$ such that $AB = I$. The multiplicativity of the determinant implies that

$$\det(A)\det(B) = \det(AB) = \det(I) = 1$$

and so $\det(A)$ is a unit in R.

Conversely, if $\det(A)$ is a unit in R, then

$$A\left(\det(A)^{-1}\operatorname{adj}(A)\right) = I$$

and so A is an invertible matrix whose inverse is the matrix $\det(A)^{-1}\operatorname{adj}(A)$. This completes the proof.

3.7 Properties of determinants

(vii) Let V be an n-dimensional vector space over R, and let $\mathscr{B}$ be an ordered basis for V. For $j = 1, \dots, n$, let $\mathbf{v}_j \in V$ and let

$$[\mathbf{v}_j]_{\mathscr{B}} = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{n,j} \end{pmatrix}$$

be the coordinate vector of $\mathbf{v}_j$ with respect to the basis $\mathscr{B}$. Let A be the $n \times n$ matrix whose jth column is the coordinate vector $[\mathbf{v}_j]_{\mathscr{B}}$. Then $\det(A) = 0$ if and only if the set of vectors $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is linearly dependent.

(viii) The homogeneous system of n linear equations in n variables:

$$\begin{aligned} a_{1,1}x_1 + \cdots + a_{1,j}x_j + \cdots + a_{1,n}x_n &= 0 \\ &\vdots \\ a_{i,1}x_1 + \cdots + a_{i,j}x_j + \cdots + a_{i,n}x_n &= 0 \\ &\vdots \\ a_{n,1}x_1 + \cdots + a_{n,j}x_j + \cdots + a_{n,n}x_n &= 0 \end{aligned}$$

with coefficient matrix A defined by (3.8) has the unique solution $x_j = 0$ for all $j = 1, \dots, n$ if and only if $\det(A) = 0$.

(ix) The inhomogeneous system of n linear equations in n variables:

$$\begin{aligned} a_{1,1}x_1 + \cdots + a_{1,j}x_j + \cdots + a_{1,n}x_n &= b_1 \\ &\vdots \\ a_{i,1}x_1 + \cdots + a_{i,j}x_j + \cdots + a_{i,n}x_n &= b_i \\ &\vdots \\ a_{n,1}x_1 + \cdots + a_{n,j}x_j + \cdots + a_{n,n}x_n &= b_n \end{aligned}$$

with coefficient matrix A defined by (3.8) has a unique solution for every column vector $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ if and only if $\det(A) = 0$.

Exercises

All vector spaces in these exercises are vector spaces over the field R.

1. Let $V_1, \ldots, V_n$, and W be vector spaces over the field R, and let F and G be multilinear functions functions from $V_1 \times \cdots \times V_n$ into W. Let $c \in R$. Prove that $F+G$ and cF are multilinear functions functions from $V_1 \times \cdots \times V_n$ into W.
2. Let V be the direct product of the vector spaces $V_1, \ldots, V_k$, that is,

$$V = V_1 \times \cdots \times V_n.$$

For every $j \in \{1, \ldots, n\}$, define the function

$$\pi_j : V \to V$$

as follows: If $v = (v_1, \ldots, v_{j-1}, v_j, v_{j+1}, \ldots, v_n) \in V$, then

$$\pi(v) = \pi_j(v_1, \ldots, v_{j-1}, v_j, v_{j+1}, \ldots, v_n) = (0, \ldots, 0, v_j, 0, \ldots, 0).$$

Thus, $\pi_j(v)$ is the vector whose jth component is equal to the jth component of v, and whose other components are 0.

a. Prove that π_j is a linear transformation.
b. Prove that π_j is an involution, that is, $\pi_j^2 = \pi_j$.
c. Prove that $\pi_j \pi_k = 0$ if $j, k \in \{1, \ldots, n\}$ and $j \neq k$.
d. Prove that

$$\mathrm{id}_V = \sum_{j=1}^{n} \pi_j.$$

3.8 Permutations

A *permutation* of a set X is a function $\sigma : X \to X$ that is one-to-one and onto. We denote the set of all permutations of X by $\mathrm{Perm}(X)$. The function $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$ for all $x \in X$ is called the *identity* permutation. By Theorem **??** and Exercise **??** in Appendix **??**, every function that is one-to-one and onto has a unique inverse, for every permutation $\sigma \in \mathrm{Perm}(X)$ there exists a permutation $\sigma^{-1} \in \mathrm{Perm}(X)$ such that $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \mathrm{id}_X$.

An element $x \in X$ is a *fixed point* of the permutation σ if $\sigma(x) = x$. We write "σ fixes x" if x is a fixed point of σ. The identity permutation id_X is the unique permutation that fixes every element of X.

The permutation τ is called a *transposition* if there exist distinct elements $x_1, x_2 \in X$ such that $\tau(x_1) = x_2$, $\tau(x_2) = x_1$, and $\tau(x) = x$ for all $x \in X \setminus \{x_1, x_2\}$. Thus, a transposition interchanges two elements of X and fixes every other element of X.

The composite of functions $\sigma : X \to X$ and $\tau : X \to X$ is the function $\sigma\tau : X \to X$ defined by

$$(\sigma\tau)(x) = \sigma(\tau(x)).$$

Let σ and τ be permutations of X. Because the composite of one-to-one functions is a one-to-one function, and the composite of onto functions is an onto function, it follows that the composite of two permutations is a permutation. We also call the composite of two permutations the *product* of the permutations.

For example, the function $\sigma : \{1,2,3\} \to \{1,2,3\}$ defined by

$$\sigma(1) = 2, \qquad \sigma(2) = 3, \qquad \sigma(3) = 1 \tag{3.24}$$

is a permutation, and so $\sigma \in S_3$. The permutation σ has no fixed points. The inverse of σ is the permutation $\sigma^{-1} \in S_3$ defined by

$$\sigma^{-1}(1) = 3, \qquad \sigma^{-1}(2) = 1, \qquad \sigma^{-1}(3) = 2.$$

The function $\tau : \{1,2,3\} \to \{1,2,3\}$ defined by

$$\tau(1) = 2, \qquad \tau(2) = 1, \qquad \tau(3) = 3 \tag{3.25}$$

is a permutation in S_3, and $\tau^{-1} = \tau$. Moreover, τ is a transposition with fixed point 3.

The product of τ and σ is the permutation $\tau\sigma$ defined by

$$\tau\sigma(1) = 1, \qquad \tau\sigma(2) = 3, \qquad \tau\sigma(3) = 2.$$

The product of σ and τ is the permutation $\sigma\tau$ defined by

$$\sigma\tau(1) = 3, \qquad \sigma\tau(2) = 2, \qquad \sigma\tau(3) = 1.$$

Note that $\sigma\tau \neq \tau\sigma$. We also observe that $\tau\sigma$ and $\sigma\tau$ are transpositions, and so $(\tau\sigma)^{-1} = \tau\sigma$ and $(\sigma\tau)^{-1} = \sigma\tau$.

Theorem 3.12. *Every permutation in S_n is a product of transpositions.*

Proof. Every permutation is a product of disjoint cycles, and every cycle of length ℓ is a product of $\ell - 1$ permutations.

Theorem 3.13. *Let $\sigma \in S_n$. If $\tau_1, \tau_2, \ldots, \tau_\ell$ are transpositions in S_n such that $\sigma = \tau_\ell \cdots \tau_2 \tau_1$, and if $\tau_1, \tau_2, \ldots, \tau_m$ are transpositions in S_n such that $\sigma = \tau_m \cdots \tau_2 \tau_1$, then $(-1)^\ell = (-1)^m$. Thus, ℓ and m are both even integers or ℓ and m are both odd integers.*

Proof. Let I_n be the $n \times n$ identity matrix. Identity (3.13) in Theorem 3.4 implies that

$$\det(\sigma I_n) = (-1)^\ell \det(I_n) = (-1)^\ell$$

and also

$$\det(\sigma I_n) = (-1)^m \det(I_n) = (-1)^m.$$

Therefore, $(-1)^\ell = (-1)^m$ and so ℓ and m are integers with the same parity. This completes the proof.

A permutation $\sigma \in S_n$ is called *even* if σ is the product of an even number of transpositions. A permutation $\sigma \in S_n$ is called *odd* if σ is the product of an odd number of transpositions. For every permutation $\sigma \in S_n$, we define the *sign* of σ, denoted $\operatorname{sgn}(\sigma)$, as follows:

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Lemma 3.1. *If $\sigma, \sigma' \in S_n$, then*

$$sgn(\sigma\sigma') = sgn(\sigma)\, sgn(\sigma')$$

and

$$sgn\left(\sigma^{-1}\right) = sgn(\sigma).$$

Proof. If σ can be represented as a product of k transpositions, say, $\sigma = \tau_1 \cdots \tau_k$, and if σ' can be represented as a product of ℓ transpositions, say, $\sigma' = \tau_1' \cdots \tau_\ell'$, then

$$\sigma\sigma' = \tau_1 \cdots \tau_k \tau_1' \cdots \tau_\ell'$$

and so

$$\operatorname{sgn}(\sigma\sigma') = (-1)^{k+\ell} = (-1)^k (-1)^\ell = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma').$$

It follows that

$$1 = \operatorname{sgn}(\mathrm{id}) = \operatorname{sgn}\left(\sigma\sigma^{-1}\right) = \operatorname{sgn}(\sigma)\operatorname{sgn}\left(\sigma^{-1}\right)$$

and so $\operatorname{sgn}(\sigma) = \operatorname{sgn}\left(\sigma^{-1}\right)$. This completes the proof.

3.9 Construction of the determinant function

We begin with the construction of matrix minors.

Theorem 3.14. *If A is an $n \times n$ matrix and A^t is the transpose of A, then*

$$\det(A) = \det(A^t).$$

Proof. Let $A = (a_{i,j})$ and $A^t = \left(a^t_{i,j}\right)$, where

$$a^t_{i,j} = a_{j,i}$$

for $i, j = 1, \ldots, n$. For every permutation $\sigma \in S_n$ we have $\{\sigma(1), \sigma(2), \ldots, \sigma(n)\} = \{1, 2, \ldots, n\}$ and $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$. Then

$$\begin{aligned}
\det(A^t) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a^t_{\sigma(i),i} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma^{-1}(\sigma(i)),\sigma(i)} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{\sigma^{-1}(j),j} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) \prod_{j=1}^{n} a_{\sigma^{-1}(j),j} \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j} \\
&= \det(A).
\end{aligned}$$

This completes the proof.

3.10 Linear independence and determinants

Let $\mathbf{v}_j \in R^n$ for $j = 1, \ldots, n$. The set of column vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is *linearly dependent* if, for some $k \in \{1, \ldots, m\}$, there exist scalars $c_1, \ldots, c_{k-1}, c_{k+1}, \ldots, c_n \in R$ such that

$$\mathbf{v}_k = \sum_{\substack{j=1 \\ j \neq k}}^{n} c_j \mathbf{v}_j.$$

The set of column vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ *generates* R^n if, for every vector $\mathbf{v} \in R^n$, there exist scalars $c_1, \ldots, c_n \in R$ such that

$$\mathbf{v} = \sum_{j=1}^{n} c_j \mathbf{v}_j.$$

Theorem 3.15. *Let D be a nonzero alternating multilinear form on $M_n(R)$, and let $A = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be an $n \times n$ matrix in $M_n(R)$. If the set of column vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is linearly dependent, then* $\det(A) = 0$*. If the set of column vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ generates R^n, then* $\det(A) \neq 0$.

Proof. If the set of vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is linearly dependent, then for some $k \in \{1, \ldots, n\}$ there exist scalars $c_1, \ldots, c_{k-1}, c_{k+1}, \ldots, c_n \in R$ such that

$$\mathbf{v} = \sum_{j=1}^{n} c_j \mathbf{v}_j.$$

and so

$$\begin{aligned}
D(A) &= D(\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}, \mathbf{v}_k, \mathbf{v}_{k+1}, \mathbf{v}_n) \\
&= D\left(\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}, \sum_{\substack{j=1 \\ j \neq k}}^{n} c_j \mathbf{v}_j, \mathbf{v}_{k+1}, \mathbf{v}_n\right) \\
&= \sum_{\substack{j=1 \\ j \neq k}}^{n} c_j D(\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}, \mathbf{v}_j, \mathbf{v}_{k+1}, \mathbf{v}_n) \\
&= 0.
\end{aligned}$$

If the set of vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ generates R^n, then every vector in $\mathbf{F}^n$ is a linear combination of vectors in the set. Let $I = (\delta_{i,j})$ be the identity matrix. For $j = 1, \ldots, n$, the jth column of I is the vector $\mathbf{e}_j$, whose jth coordinate is 1 and whose other coordinates are 0. Because $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ generates R^n, there exist scalars $b_{1,j}, b_{2,j}, \ldots, b_{n,j}$ such that

$$\sum_{i=1}^{n} b_{i,j} \mathbf{v}_i = \mathbf{e}_j.$$

Consider the $n \times n$ matrix

$$B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,n} \\ \vdots & & \\ b_{n,1} & \cdots & b_{n,n} \end{pmatrix}.$$

The jth column of the product matrix AB is $\sum_{i=1}^{n} b_{i,j}\mathbf{v}_j = \mathbf{e}_j$, and so $AB = I$. By the product rule for determinants,

$$D(A)D(B) = D(I)D(AB) = D(I)^2 \neq 0$$

and so $D(A) \neq 0$. This completes the proof.

Corollary 3.4. *Let*

$$\begin{aligned} a_{1,1}x_1 + \cdots + a_{1,n}x_n &= 0 \\ a_{2,1}x_1 + \cdots + a_{2,n}x_n &= 0 \\ &\vdots \\ a_{n,1}x_1 + \cdots + a_{n,n}x_n &= 0 \end{aligned}$$

be a homogeneous system of n linear equations in n variables, with coefficients $a_{i,j}$ in the field $\mathbf{F}$. Let $A = (a_{i,j}) \in M_n(\mathbf{F})$ be the associated coefficient matrix. This system of equations has a nontrivial solution if and only if $\det(A) = 0$.

Corollary 3.5. *Let $\mathbf{F}$ be a field, let $b_1, \ldots, b_n \in \mathbf{F}$, and let*

$$\begin{aligned} a_{1,1}x_1 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + \cdots + a_{2,n}x_n &= b_2 \\ &\vdots \\ a_{n,1}x_1 + \cdots + a_{n,n}x_n &= b_n \end{aligned}$$

be a system of n linear equations in n variables with coefficients $a_{i,j} \in \mathbf{F}$. Let $A = (a_{i,j}) \in M_n(\mathbf{F})$ be the associated coefficient matrix. This system of equations has a unique solution for every vector $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbf{F}^n$ if and only if $\det(A) = 0$.

Exercises

3.11 Cramer's rule

Let $\mathbf{F}$ be a field, let $b_1, \dots, b_n \in \mathbf{F}$, and let

$$\begin{aligned} a_{1,1}x_1 + \cdots + a_{1,j}x_j + \cdots + a_{1,n}x_n &= b_1 \\ &\vdots \\ a_{i,1}x_1 + \cdots + a_{i,j}x_j + \cdots + a_{i,n}x_n &= b_i \\ &\vdots \\ a_{n,1}x_1 + \cdots + a_{n,j}x_j + \cdots + a_{n,n}x_n &= b_n \end{aligned}$$

be a system of n linear equations in n variables with coefficients $a_{i,j} \in \mathbf{F}$. Let $A = (a_{i,j}) \in M_n(\mathbf{F})$ be the associated coefficient matrix. We assume that

$$\det(A) \neq 0.$$

Let $\tilde{A}_{i,j}$ be the $(n-1) \times (n-1)$ matrix obtained from A by deleting the ith row and jth column, and let

$$C_{i,j} = (-1)^{i+j} \det\left(\tilde{A}_{i,j}\right)$$

be the corresponding cofactor of A. Let $k \in \{1, \dots, n\}$, and consider the system of linear equations derived from the given system by multiplying the ith equation by $C_{i,k}$. We obtain

$$\begin{aligned} a_{1,1}C_{1,k}x_1 + \cdots + a_{1,j}C_{1,k}x_j + \cdots + a_{1,n}C_{1,k}x_n &= b_1C_{1,k} \\ &\vdots \\ a_{i,1}C_{i,k}x_1 + \cdots + a_{i,j}C_{i,k}x_j + \cdots + a_{i,n}C_{i,k}x_n &= b_iC_{i,k} \\ &\vdots \\ a_{n,1}C_{n,k}x_1 + \cdots + a_{n,j}C_{n,k}x_j + \cdots + +a_{n,n}C_{n,k}x_n &= b_nC_{n,k} \end{aligned}$$

Adding these equations gives

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{n} a_{i,j}C_{i,k} \right) x_j = \sum_{i=1}^{n} C_{i,k}b_i.$$

Because

$$\sum_{i=1}^{n} a_{i,j}C_{i,k} = \begin{cases} \det(A) & \text{if } k = j \\ \det(A) & \text{if } k \neq j \end{cases}$$

we have

$$\det(A)x_k = \sum_{i=1}^{n} b_iC_{i,k}.$$

The right side of this equation is the determinant of the matrix B_k obtained from A by replacing the kth column by $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$, and so

$$x_k = \frac{\det(B_k)}{\det(A)}.$$

This is *Cramer's rule*.

Here is an example. Solve the system of equations

$$\begin{aligned} 3x_1 + 2x_2 - x_3 &= 0 \\ 2x_1 - x_2 + 8x_3 &= 1 \\ x_1 + x_2 + x_3 &= 2 \end{aligned}$$

Then

$$A = \begin{pmatrix} 3 & 2 & -1 \\ 2 & -1 & 8 \\ 1 & 1 & 1 \end{pmatrix} \qquad \text{and} \qquad \det(A) = -18$$

$$B_1 = \begin{pmatrix} 0 & 2 & -1 \\ 1 & -1 & 8 \\ 2 & 1 & 1 \end{pmatrix} \qquad \text{and} \qquad \det(B_1) = 27$$

$$B_2 = \begin{pmatrix} 3 & 0 & -1 \\ 2 & 1 & 8 \\ 1 & 2 & 1 \end{pmatrix} \qquad \text{and} \qquad \det(B_2) = -48$$

$$B_3 = \begin{pmatrix} 3 & 2 & 0 \\ 2 & -1 & 1 \\ 1 & 1 & 2 \end{pmatrix} \qquad \text{and} \qquad \det(B_3) = -15.$$

Applying Cramer's rule, we obtain

$$x_1 = -\frac{27}{18} = -\frac{3}{2} \qquad x_2 = \frac{48}{18} = \frac{8}{3} \qquad x_3 = \frac{15}{18} = \frac{5}{6}.$$

Exercises

Use Cramer's rule to solve the following systems of equations:

1.

$$\begin{aligned} 5x_1 - 3x_2 &= 4 \\ 2x_1 - x_2 &= -7 \end{aligned}$$

2.

$$\begin{aligned} 7x_1 + x_2 &= 13 \\ -3x_1 - x_2 &= 11 \end{aligned}$$

3.

$$\begin{aligned} x_1 + x_2 + x_3 &= \\ x_1 + x_2 + x_3 &= \\ x_1 + x_2 + x_3 &= \end{aligned}$$

4.

$$\begin{aligned} x_1 + x_2 + x_3 &= \\ x_1 + x_2 + x_3 &= \\ x_1 + x_2 + x_3 &= \end{aligned}$$

5.

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= \\ x_1 + x_2 + x_3 + x_4 &= \\ x_1 + x_2 + x_3 + x_4 &= \\ x_1 + x_2 + x_3 + x_4 &= \end{aligned}$$

Solutions

1.

$$A = \begin{pmatrix} 5 & -3 \\ 2 & -1 \end{pmatrix} \qquad \text{and} \qquad \det(A) = 1$$

$$B_1 = \begin{pmatrix} 4 & -3 \\ -7 & -1 \end{pmatrix} \qquad \text{and} \qquad \det(B_1) = -25$$

$$B_2 = \begin{pmatrix} 5 & 4 \\ 2 & -7 \end{pmatrix} \qquad \text{and} \qquad \det(B_2) = -43$$

Applying Cramer's rule, we obtain

$$x_1 = -25 \qquad x_2 = -43$$

3.12 Cayley-Hamilton theorem

An important application of the classical adjoint is the proof of the Cayley-Hamilton theorem.

Let R be a commutative ring, and let $R[t]$ be the ring of polynomials with coefficients in R. Let

$$f = a_d t^d + a_{d-1} t^{d-1} + \cdots + a_1 t + a_0 \in R[t].$$

Let A be an $n \times n$ matrix with coordinates in R. We define the $n \times n$ matrix

$$f(A) = a_d A^d + a_{d-1} A^{d-1} + \cdots + a_1 A + a_0 I$$

where I is the $n \times n$ identity matrix. The matrix A is a *root* of the polynomial f if $f(A) = \mathbf{0}$. A root is also called a *zero* of the polynomial.

For example, consider the quadratic polynomial

$$f = t^2 - 5t + 6.$$

and the matrices

$$A = \begin{pmatrix} 2 & 5 \\ -1 & 7 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 2 & 0 & 6 \\ 3 & 1 & 0 \\ -5 & 6 & -3 \end{pmatrix}.$$

We have

$$\begin{aligned} f(A) &= A^2 - 5A + 6I \\ &= \begin{pmatrix} -1 & 45 \\ -9 & 44 \end{pmatrix} - 5 \begin{pmatrix} 2 & 5 \\ -1 & 7 \end{pmatrix} + 6 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} -5 & 20 \\ -4 & 15 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} f(B) &= B^2 - 5B + 6I \\ &= \begin{pmatrix} -26 & 36 & -6 \\ 9 & 1 & 18 \\ 23 & -12 & -21 \end{pmatrix} - 5 \begin{pmatrix} 2 & 0 & 6 \\ 3 & 1 & 0 \\ -5 & 6 & -3 \end{pmatrix} + 6 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} -30 & 36 & -36 \\ -6 & 2 & 18 \\ 48 & -42 & 0 \end{pmatrix}. \end{aligned}$$

For the polynomial

$$g = t^2 - 9t + 19$$

we have

$$\begin{aligned} g(A) &= A^2 - 9A + 19I \\ &= \begin{pmatrix} -1 & 45 \\ -9 & 44 \end{pmatrix} - 9\begin{pmatrix} 2 & 5 \\ -1 & 7 \end{pmatrix} + 19\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

and so A is a root of g.

There is a remarkable polynomial identity for 2×2 matrices. From the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R).$$

we construct the matrix

$$tI - A = t\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} t-a & -b \\ -c & t-d \end{pmatrix}$$

with coordinates in the polynomial ring $R[t]$, and the quadratic polynomial

$$\begin{aligned} f(t) = \det(tI - A) &= (t-a)(t-d) - bc \\ &= t^2 - (a+d)t + (ad - bc) \\ &= t^2 - \mathrm{trace}(A)A + \det(A). \end{aligned}$$

Theorem 3.16. *For every 2×2 matrix A,*

$$A^2 - \mathit{trace}(A)A + \det(A)I = \mathbf{0}.$$

Proof. For the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with

$$\mathrm{trace}(A) = a + d \qquad \text{and} \qquad \det(A) = ad - bc$$

we have

$$A^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix}$$

and

$$\begin{aligned}
&A^2 - \mathrm{trace}(A)A + \det(A)I \\
&\quad = \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix} - (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
&\quad = \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix} - \begin{pmatrix} a^2+ad & ab+bd \\ ac+cd & ad+d^2 \end{pmatrix} + \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\
&\quad = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.
\end{aligned}$$

This completes the proof.

This result generalizes to $n \times n$ matrices for every positive integer n.

The *characteristic polynomial* of the $n \times n$ matrix A with coordinates in R is

$$\chi_A(t) = \det(tI - A).$$

This is a monic polynomial of degree n in the polynomial ring $R[t]$.

The Cayley-Hamilton theorem states that every square matrix is a root of its characteristic polynomial.

Theorem 3.17 (Cayley-Hamilton). *Every $n \times n$ matrix $A = (a_{i,j})$ with coordinates in R is a root of its characteristic polynomial.*

Equivalently, if $\chi_A(t) = \det(tI - A)$, then $\chi_A(A) = \mathbf{0}$.

Proof. The set $R[A]$ of polynomials in the matrix A with coordinates in R is a commutative ring (and a subring of noncommutative ring $M_n[R]$). For all $i, j = 1, \ldots, n$, let

$$B_{k,j} = \delta_{j,k}A - a_{j,k}I \in R[A].$$

Consider the $n \times n$ matrix $B = (B_{i,j})$ with coordinates in $R[A]$. The determinant of B is also a polynomial in A. Let $\tilde{B} = (\tilde{B}_{i,j})$ be the classical adjoint of B. By Theorem 3.10,

$$\tilde{B}B = \det(B)I = \begin{pmatrix} \det(B) & 0 & \ldots & 0 \\ 0 & \det(B) & \ldots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \ldots & \det(B) \end{pmatrix}.$$

The characteristic polynomial $\chi_A(t)$ is the determinant of the matrix $tI - A$, that is

$$\chi_A(t) = \det(\delta_{j,k}t - a_{j,k}).$$

It follows that

$$\chi_A(A) = \det(\delta_{j,k}A - a_{j,k}I) = \det(B).$$

Let $\mathbf{e}_j = (\delta_{i,j}) \in R^n$ be the standard unit vector in R^n, that is, the column vector whose jth coordinate is 1 and whose $n-1$ other coordinates are 0. For all $j \in \{1, \ldots, n\}$, we have

$$A\mathbf{e}_k = \mathrm{col}_A(k) = \begin{pmatrix} a_{1,k} \\ \vdots \\ a_{n,k} \end{pmatrix} = \sum_{j=1}^{n} a_{j,k}\mathbf{e}_j.$$

Equivalently,

$$\sum_{j=1}^{n} \delta_{j,k} A\mathbf{e}_j = \sum_{j=1}^{n} a_{j,k} I\mathbf{e}_j$$

and so

$$\sum_{j=1}^{n} B_{k,j}\mathbf{e}_j = \sum_{j=1}^{n} \left(\delta_{j,k}A - a_{j,k}I\right)\mathbf{e}_j = \mathbf{0}.$$

For all $i \in \{1,\ldots,n\}$, we have

$$\sum_{j=1}^{n} \tilde{B}_{i,k}B_{k,j}\mathbf{e}_j = \tilde{B}_{i,k}\sum_{j=1}^{n} B_{k,j}\mathbf{e}_j = \mathbf{0}$$

and so

$$\sum_{j=1}^{n}\sum_{k=1}^{n} \tilde{B}_{i,k}B_{k,j}\mathbf{e}_j = \sum_{k=1}^{n}\sum_{j=1}^{n} \tilde{B}_{i,k}B_{k,j}\mathbf{e}_j = \mathbf{0}.$$

The equation

$$\sum_{k=1}^{n} \tilde{B}_{i,k}B_{k,j} = (\tilde{B}B)_{i,j} = \delta_{i,j}\det(B)$$

implies that

$$\det(B)\mathbf{e}_i = \sum_{j=1}^{n} \delta_{i,j}\det(B)\mathbf{e}_j = \mathbf{0}$$

for all $i \in \{1,\ldots,n\}$, and so $\det(B)$ is the zero matrix, that is, $\chi_A(A) = \det(B) = \mathbf{0}$. This completes the proof.

3.13 Vandermonde determinant

The *Vandermonde matrix* associated to the sequence $(a_1,\ldots,a_n)$ of elements of the field F is the $n \times n$ matrix

$$V = V(a_1,\ldots,a_n) = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \cdots & & & & \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}.$$

Thus, for $i = 1,\ldots,n$, the ith row of the matrix V consists of the first n terms of the geometric progression with common ratio a_i. A *Vandermonde determinant* is the determinant of a Vandermonde matrix.

Theorem 3.18. *The determinant of the Vandermonde matrix*

$$V = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \cdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}$$

is

$$\det(V) = \prod_{1 \le i < j \le n} (a_j - a_i).$$

For example, the determinant of the Vandermonde matrix

$$V(1,2,3,4) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 27 \\ 1 & 4 & 16 & 64 \end{pmatrix}$$

is

$$\prod_{1 \le i < j \le 4} (j-1) = (2-1)(3-1)(4-1)(3-2)(4-2)(4-3) = 12.$$

3.14 Lie algebras

Norm of a matrix.
Trace of a matrix
$SL_2(\mathbf{R})$
$sl_2(\mathbf{R})$.
A_n Lie algebra.
Exponential of matrices.

Stuff to add

1. Factoring determinants and group characters and representations
2. Example of a matrix with minimal polynomial not equal to the characteristic polynomial.
3. Using CHT to compute powers of A.
4. Using CHT to compute e^A.
5. Hadamard's inequality
6. Volume of parallelepiped in 2 and in n dimensions
7. circulant matrix
8. a. Discriminants and multiple zeros of a polynomial.
   b. Resultants and common zeros of two polynomials

9. Block diagonal matrices and their determinants
10. Exercise:
    An $n \times n$ matrix $A = (a_{i,j})$ is *skew-symmetric* if $a_{i,j} = -a_{i,j}$ for all $i, j = 1, \ldots, n$.

    a. Prove that the diagonal elements of a skew-symmetric matrix are 0.
    b. For $n = 1, 2, 3, 4$, let A_n be the skew-symmetric matrix such that $a_{i,j} = 1$ for $1 \leq i < j \leq n$. Compute $\det(A_n)$.
    c. Prove that every odd-dimensional skew-symmetric matrix has determinant 0.

    Let $M_n(r,s,t) = (a_{i,j})$ be the *tridiagonal matrix* defined by

$$a_{i,j} = \begin{cases} r & \text{if } i = j \text{ for } i = 1, \ldots, n \\ s & \text{if } j = i+1 \text{ for } i = 1, \ldots, n-1 \\ t & \text{if } j = i-1 \text{ for } i = 2, \ldots, n. \end{cases}$$

Thus,

$$M_6(r,s,t) = \begin{pmatrix} r & s & 0 & 0 & 0 \\ t & r & s & 0 & 0 \\ 0 & t & r & s & 0 \\ 0 & 0 & t & r & s \\ 0 & 0 & 0 & t & r \end{pmatrix}$$

We have

$$\begin{aligned} \det(M_1(r,s,t)) &= r \\ \det(M_2(r,s,t)) &= r^2 - st \\ \det(M_3(r,s,t)) &= r^3 - 2rst \\ \det(M_4(r,s,t)) &= r^4 - 3r^2st + s^2t^2 \\ \det(M_5(r,s,t)) &= r^5 - 4r^3st + 3rs^2t^2 \end{aligned}$$

For $n \geq 3$, we have the recursion relation

$$M_n(r,s,t) = rM_{n-1}(r,s,t) - stM_{n-2}(r,s,t).$$

Exercises

1. Prove that, for every positive integer n, the determinant of the tridiagonal matrix $M_n(2,-1,-1)$ is $n+1$.

3.15 Additional topics

3.15.1 The exponential of a matrix

Let A be an $m \times n$ matrix with real or complex coefficients. The *norm* of A is

$$\|A\| = \max\left\{|a_{i,j}| : i = 1,\ldots,m \text{ and } j = 1,\ldots,n\right\}.$$

Lemma 3.2. *For all $m \times n$ matrices A and B and all scalars c,*

(i)
$$\|A\| \geq 0 \quad \textit{and} \quad \|A\| = 0 \textit{ if and only if } A = 0$$

(ii)
$$\|A+B\| \leq \|A\| + \|B\|$$

(iii)
$$\|cA\| = |c|\|A\|.$$

Let $A = (a_{i,j})$ be an $n \times n$ matrix, and let $A^{(N)} = \left(a_{i,j}^{(N)}\right)$ be an $n \times n$ matrix for all $N \geq 1$. The sequence $\left(A^{(N)}\right)_{N=1}^{\infty}$ converges to A, denoted $\lim_{N\to\infty} A^{(N)} = A$, if the matrices converge coordinate-wise, that is, if $\lim_{N\to\infty} a_{i,j}^{(N)} = a_{i,j}$ for all $i, j = 1,\ldots,n$.

Lemma 3.3. *Let $\left(A^{(N)}\right)_{N=1}^{\infty}$ be a sequence of $n \times n$ matrices, and let A be an $n \times n$ matrix. Then $\lim_{N\to\infty} A^{(N)} = A$ if and only if $\lim_{N\to\infty} \|A - A^{(N)}\| = 0$.*

Lemma 3.4. *If A be an $m \times n$ matrix and B is an $n \times p$ matrix, then*

$$\|AB\| \leq n\|A\|\|B\|.$$

If A is an $n \times n$ matrix, then

$$\|A^k\| \leq n^{k-1}\|A\|^k$$

for all $k \geq 1$.

Proof. If $A = (a_{i,j})$ and $B = (b_{i,j})$, then

$$\left|(AB)_{i,j}\right| = \left|\sum_{k=1}^{n} a_{i,k} b_{k,j}\right| \leq \sum_{k=1}^{n} \left|a_{i,k}\right| \left|b_{k,j}\right| \leq n\|A\|\|B\|$$

and so $\|AB\| \leq n\|A\|\|B\|$.

If A is an $n \times n$ matrix, then $\|A^2\| \leq n\|A\|^2$. If $k \geq 2$ and $\|A^k\| \leq n^{k-1}\|A\|^k$, then

$$\|A^{k+1}\| = \|AA^k\| \leq n\|A\|\|A^k\| \leq n\|A\|n^{k-1}\|A\|^k = n^k\|A\|^{k+1}.$$

This completes the proof.

Lemma 3.5. *Let A be an $n \times n$ matrix, and let*

$$S_N(A) = I + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \cdots + \frac{1}{N!}A^N = \sum_{k=0}^{N} \frac{1}{k!}A^k$$

for all $N \geq 0$. The sequence of matrices $(S_N(A))_{N=1}^{\infty}$ converges.

The limit of this sequence is called the *exponential of the matrix A*, and is denoted e^A. We write

$$e^A = \sum_{k=0}^{\infty} \frac{1}{k!}A^k.$$

Proof. The (i,j)th component of the matrix $S_N(A)$ is $S_N(A)_{i,j} = \sum_{k=0}^{N} \frac{1}{k!}A_{i,j}^k$. The norm of the matrix $S_N(A)$ is bounded above as follows:

$$\begin{aligned} \|S_N(A)\| &= \left\| \sum_{k=0}^{N} \frac{1}{k!}A^k \right\| \leq \sum_{k=0}^{N} \frac{1}{k!} \left\| A^k \right\| \\ &\leq \sum_{k=0}^{N} \frac{1}{k!} n^{k-1} \|A\|^k = \frac{1}{n} \sum_{k=0}^{N} \frac{1}{k!} (n\|A\|)^k \\ &< \frac{1}{n} e^{n\|A\|}. \end{aligned}$$

It follows that the infinite series $\sum_{k=0}^{\infty} \frac{1}{k!}A_{i,j}^k$ converges absolutely, and so the sequence of matrices $(S_N(A))_{N=1}^{\infty}$ converges.

For example, consider the diagonal matrix

$$A = \begin{pmatrix} a_{1,1} & 0 & 0 & \cdots & 0 \\ 0 & a_{2,2} & 0 & \cdots & 0 \\ 0 & 0 & a_{3,3} & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & a_{n,n} \end{pmatrix}.$$

For all $k \geq 0$, we have

$$A = \begin{pmatrix} a_{1,1}^k & 0 & 0 & \cdots & 0 \\ 0 & a_{2,2}^k & 0 & \cdots & 0 \\ 0 & 0 & a_{3,3}^k & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & a_{n,n}^k \end{pmatrix}$$

and so

$$e^A = \begin{pmatrix} e^{a_{1,1}} & 0 & 0 & \cdots & 0 \\ 0 & e^{a_{2,2}} & 0 & \cdots & 0 \\ 0 & 0 & e^{a_{3,3}} & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & e^{a_{n,n}}. \end{pmatrix}$$

Theorem 3.19. *If A and B are $n \times n$ matrices such that $AB = BA$, then $e^{A+B} = e^A e^B$.*

Corollary 3.6. *For every $n \times n$ matrix A, the matrix e^A is invertible.*

Proof. The matrices A and $-A$ commute, and so

$$e^A e^{-A} = eA - A = e^{\mathbf{0}} = I$$

and so e^A is invetible with inverse $\left(e^A\right)^{-1} = e^{-A}$.

Theorem 3.20 (Jacobi's identity). *For every $n \times n$ matrix A,*

$$\det(e^A) = e^{tr(A)}.$$

Corollary 3.7. *For every $n \times n$ matrix A with real coordinates, the matrix e^A is invertible.*

Proof. We have $e^t > 0$ for all $t \in \mathbf{R}$, and so $\det(e^A) = e^{\mathrm{tr}(A)} > 0$. A matrix with a nonzero determinant is invertible.

Exercises

1. Let Mat_n be the ring of $n \times n$ matrices. The *Lie bracket* of the matrices $A, B \in \mathrm{Mat}_n$ is the matrix
$$[A,B] = AB - BA \in \mathrm{Mat}_n\,.$$
Let
$$A = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & -4 \\ 1 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$
   a. Compute the matrices $[A,B]$, $[B,C]$, and $[C,A]$.
   b. Compute the matrices $[[A,B],C]$, $[[B,C],A]$, and $[[C,A],B]$.
   c. Compute the matrix $[[A,B],C] + [[B,C],A] + [[C,A],B]$.
2. Let $[A,B]$ be the Lie bracket of matrices $A, B \in \mathrm{Mat}_n$.
   a. Prove that $[A,B] = \mathbf{0}$ if and only if the matrices A and B commute.
   b. Prove that $[A,B] = -[B,A]$.
   c. Prove that
$$[[A,B],C] + [[B,C],A] + [[C,A],B] = \mathbf{0}$$
for all $A, B, C \in \mathrm{Mat}_n$.

Special matrices

3.15.2 Permutation matrices

Lemma 3.6. *The determinant of a permutation is the sign of the premutation.*

3.15.3 Circulant matrices

Let $c_1, \ldots, c_n$ be a sequence of n real numbers. Define the $n \times n$ matrix $A = (a_{i,j})$ as follows:

$$a_{1,j} = c_j \qquad \text{for } j \in \{1, \ldots, n\},$$

For $i \in \{2, \ldots, n\}$, let

$$a_{i,1} = a_{i-1,n}$$

and

$$a_{i,j} = a_{i-1,j-1} \qquad \text{for } j \in \{2, \ldots, n\}.$$

The matrix A is called a *circulant matrix*. The $n \times n$ circulant matrices for $n = 2, 3, 4$ have the following forms:

$$\begin{pmatrix} c_1 & c_2 \\ c_2 & c_1 \end{pmatrix}, \qquad \begin{pmatrix} c_1 & c_2 & c_3 \\ c_3 & c_1 & c_2 \\ c_2 & c_3 & c_1 \end{pmatrix}, \qquad \begin{pmatrix} c_1 & c_2 & c_3 & c_4 \\ c_4 & c_1 & c_2 & c_3 \\ c_3 & c_4 & c_1 & c_2 \\ c_2 & c_3 & c_4 & c_1 \end{pmatrix}.$$

1. Prove that the set of circulant matrices is a commutative algebra.
2. Compute the determinants of these matrices (related to nth roots of unity).
3. Prove that if the determinant is nonzero, then the inverse of a circulant matrix is a circulant matrix.

3.15.4 Vandermonde determinant

3.15.5 Jacobian

Consider the function $f : \mathbf{R}^n \to \mathbf{R}^n$ with coordinate functions $f = (f_1, \ldots, f_n)$. If the coordinate functions have partial derivatives, the *Jacobian matrix* of f is the $n \times n$ matrix $J(f)$ whose (i, j)-th coordinate is

$$\frac{\partial f_i}{\partial x_j}$$

The *Jacobian determinant* of f is the determinant of the Jacobian matrix of f.

For example, let $f:\mathbf{R}^2\to\mathbf{R}^2$ be the function $f(x,y)=(xy,x^2+y^2)$. The Jacobian matrix of f is

$$J(f)=\begin{pmatrix} y & x \\ 2x+y^2 & x^2+2y \end{pmatrix}$$

and the Jacobian determinant of f is

$$\det(J(f))=x^2y-xy^2+2y^2-2x^2.$$

For example, let $f:\mathbf{R}^2\to\mathbf{R}^2$ be the function

$$f(x,y)=(2xy^3,3x^2y^2).$$

The Jacobian matrix of f is

$$J(f)=\begin{pmatrix} 2y^3 & 6xy^2 \\ 6xy^2 & 6x^2y \end{pmatrix}$$

and the Jacobian determinant of f is

$$\det(J(f))=-24x^2y^4.$$

3.15.6 Hessian

Consider a function $f:\mathbf{R}^n\to\mathbf{R}$ such that $f(x_1,\ldots,x_n)$ has continuous second partial derivatives. The *Hessian matrix* of f is the symmetric $n\times n$ matrix $H(f)$ whose (i,j)-th coordinate is

$$\frac{\partial^2 f}{\partial x_i \partial x_j}$$

The *Hessian determinant* of f is the determinant of the Hessian matrix of f.

For example, if $f(x,y)=x^2y^3$, then the Hessian matrix of f is

$$H(f)=\begin{pmatrix} 2y^3 & 6xy^2 \\ 6xy^2 & 6x^2y \end{pmatrix}$$

and the Hessian determinant of f is

$$\det(H(f))=-24x^2y^4.$$

1. Compute the Hessian determinant of the function $f(x,y)=x^my^n$.
2. Compute the Hessian determinant of the function $f(x,y)=\sin(x+y)$.
3. Compute the Hessian determinant of the function $f(x,y,z)=xyz$.
4. Compute the Hessian determinant of the function $f(x,y,z)=x+y+z$.

5. Consider a function $f : \mathbf{R}^n \to \mathbf{R}$ such that $f(x_1,\ldots,x_n)$ has continuous second partial derivatives. The *gradient* of f is the function $\nabla f : \mathbf{R}^n \to \mathbf{R}^n$ defined by

$$\nabla f = \left(\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n}\right).$$

   Compute $J(\nabla f)$ for the following functions:

   a.
$$f(x,y) = x^3y^5.$$

   b.
$$f(x,y,z = xyz.$$

6. Consider a function $f : \mathbf{R}^n \to \mathbf{R}$ such that $f(x_1,\ldots,x_n)$ has continuous second partial derivatives. Prove that

$$H(f) = J(\nabla f).$$

3.15.7 Determinant identities

1. Sylvester's identity: Let A be an $n \times m$ matrix and let B be an $m \times n$ matrix.

$$\det(I_n + AB) = \det(I_m + BA).$$

   Proof. By block multiplication of matrices, we have

$$\begin{pmatrix} I_n & A \\ 0 & I_m \end{pmatrix} \begin{pmatrix} I_n & -A \\ B & I_m \end{pmatrix} = \begin{pmatrix} I_n + AB & 0 \\ B & I_m \end{pmatrix}$$

   and

$$\begin{pmatrix} I_n & -A \\ B & I_m \end{pmatrix} \begin{pmatrix} I_n & A \\ 0 & I_m \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ B & I_m + BA \end{pmatrix}.$$

   Therefore,

$$\begin{aligned}
\det(I_n + AB) &= \det \begin{pmatrix} I_n + AB & 0 \\ B & I_m \end{pmatrix} \\
&= \det \begin{pmatrix} I_n & A \\ 0 & I_m \end{pmatrix} \begin{pmatrix} I_n & -A \\ B & I_m \end{pmatrix} \\
&= \det \begin{pmatrix} I_n & -A \\ B & I_m \end{pmatrix} \begin{pmatrix} I_n & A \\ 0 & I_m \end{pmatrix} \\
&= \det \begin{pmatrix} I_n & 0 \\ B & I_m + BA \end{pmatrix} \\
&= \det(I_m + BA).
\end{aligned}$$

Here is an example: Let

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 0 \\ 0 & 8 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} -1 & 0 & 3 & 2 \\ 0 & 5 & 0 & 1 \end{pmatrix}.$$

We have

$$AB = \begin{pmatrix} -1 & 10 & 3 & 4 \\ -3 & 20 & 9 & 10 \\ -5 & 0 & 15 & 10 \\ 0 & 40 & 0 & 8 \end{pmatrix} \qquad \text{and} \qquad I_4 + AB = \begin{pmatrix} 0 & 10 & 3 & 4 \\ -3 & 21 & 9 & 10 \\ -5 & 0 & 16 & 10 \\ 0 & 40 & 0 & 9 \end{pmatrix}$$

and

$$BA = \begin{pmatrix} 14 & 14 \\ 15 & 28 \end{pmatrix} \qquad \text{and} \qquad I_2 + BA = \begin{pmatrix} 15 & 14 \\ 15 & 29 \end{pmatrix}.$$

By Sylvester's identity,

$$\begin{aligned} \det \begin{pmatrix} 0 & 10 & 3 & 4 \\ -3 & 21 & 9 & 10 \\ -5 & 0 & 16 & 10 \\ 0 & 40 & 0 & 9 \end{pmatrix} &= \det(I_4 + AB) \\ &= \det(I_2 + BA) \\ &= \det \begin{pmatrix} 15 & 14 \\ 15 & 29 \end{pmatrix} \\ &= 225. \end{aligned}$$

To appreciate the computational advantage of Sylvester's identity, the reader should use pencil and paper to compute the determinant of the 4×4 matrix $I_4 + AB$.

2. Upper and lower triangular block matrices:

$$\det \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \det(A)\det(D) \tag{3.26}$$

and

$$\det \begin{pmatrix} A & 0 \\ C & D \end{pmatrix} = \det(A)\det(D) \tag{3.27}$$

This extends by induction to $\ell \times \ell$ upper and lower triangular block matrices.

Proof. For lower triangular matrices, we prove the determinant identity (3.26) by induction on m. Let $m = 1$ and $A = \begin{pmatrix} a_{1,1} \end{pmatrix}$. For all $k \geq 1$, we have

$$M = \begin{pmatrix} A & 0 \\ C & D \end{pmatrix} = \begin{pmatrix} a_{1,1} & C \\ 0 & D \end{pmatrix} = \begin{pmatrix} a_{1,1} & 0 & \dots & 0 \\ c_{1,1} & d_{1,1} & \dots & d_{1,k} \\ c_{2,1} & d_{2,1} & \dots & d_{2,k} \\ \vdots & \vdots & & \vdots \\ c_{k,1} & d_{k,1} & \dots, & d_{k,k} \end{pmatrix}$$

and

$$\det(M) = a_{1,1} \det(D) = \det(A) \det(D).$$

Let $m \geq 2$. Assume that the identity is true for $m-1$ and all $k \geq 1$. Let A be an $m \times m$ matrix, let C be an $k \times m$ matrix, and let D be a $k \times k$ matrix. We have

$$M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \begin{pmatrix} a_{1,1} & \dots & a_{1,m} & 0 & \dots & 0 \\ a_{2,1} & \dots & a_{2,m} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,m} & 0 & \dots & 0 \\ c_{1,1} & \dots & c_{1,m} & d_{1,1} & \dots & d_{1,k} \\ c_{2,1} & \dots & c_{2,m} & d_{2,1} & \dots & d_{2,k} \\ \vdots & & \vdots & \vdots & & \vdots \\ c_{k,1} & \dots & c_{k,m} & d_{k,1} & \dots, & d_{k,k} \end{pmatrix}$$

For $i, j = 1, \dots, m$, the (i, j)th-minor of M is an $(n-1) \times (n-1)$ lower triangular block matrix

$$\tilde{M}_{i,j} = \begin{pmatrix} \tilde{A}_{i,j} & 0 \\ C' & D \end{pmatrix}$$

where the $k \times (m-1)$ matrix C' is the matrix C with the jth column deleted. and let $\operatorname{cof}(\tilde{A}_{i,j})$ be the $(1, j)$th-cofactor of A. We have

$$\det(M) = \sum_{j=1}^{m} a_{1,j} \operatorname{cof}(\tilde{M}_{1,j})$$

The proof of the upper triangular identity (3.27) is similar (or use the fact that the transpose of a lower triangular block matrix is an upper triangular block matrix). Let A be an $m \times m$ matrix, let B be an $m \times k$ matrix, and let D be a $k \times k$ matrix. We have

$$M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \begin{pmatrix} a_{1,1} & \dots & a_{1,m} & b_{1,1} & \dots & b_{1,k} \\ a_{2,1} & \dots & a_{2,m} & b_{2,1} & \dots & b_{2,k} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,m} & b_{m,1} & \dots & b_{m,k} \\ 0 & \dots & 0 & d_{1,1} & \dots & d_{1,k} \\ 0 & \dots & 0 & d_{2,1} & \dots & d_{2,k} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & d_{k,1} & \dots, & d_{k,k} \end{pmatrix}$$

3. Schur's identity: Let $n = m + k$, and let

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

be an $n \times n$ matrix, where where A is an invertible $m \times m$ matrix, and B is an $m \times k$ matrix, C is an $k \times m$ matrix, and D is an $k \times k$ matrix. Then

$$\det(M) = \det(A)\det(D - CA^{-1}B).$$

Proof. We have

$$\begin{aligned} M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} &= \begin{pmatrix} A & 0 \\ 0 & I_k \end{pmatrix} \begin{pmatrix} I_m & A^{-1}B \\ C & D \end{pmatrix} \\ &= \begin{pmatrix} A & 0 \\ 0 & I_k \end{pmatrix} \begin{pmatrix} I_m & 0 \\ C & I_k \end{pmatrix} \begin{pmatrix} I_m & A^{-1}B \\ 0 & D - CA^{-1}B \end{pmatrix}. \end{aligned}$$

3.16 Solutions to exercises

Section 3.1

Exercise 1.

$$AB = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

$$BA = \begin{pmatrix} ae+cf & be+df \\ ag+ch & bg+dh \end{pmatrix}$$

$$\begin{aligned}\det(A)\det(B) &= (ad-bc)(eh-fg)\\ &= adeh-adfg-bceh+bcfg\end{aligned}$$

$$\begin{aligned}\det(AB) &= (ae+bg)(cf+dh)-(af+bh)(ce+dg)\\ &= (acef+adeh+bcfg+bdgh)-(acef+adfg+bceh+bdgh)\\ &= adeh-adfg-bceh+bcfg\end{aligned}$$

$$\begin{aligned}\det(BA) &= (ae+cf)(bg+dh))-(ag+ch)(be+df)\\ &= (abeg+adeh+bcfg+cdfh)-(abeg+adfg+bceh+cdfh)\\ &= adeh-adfg-bceh+bcgh\end{aligned}$$

$$\mathrm{trace}(AB) = ae+bg+cf+dh = \mathrm{trace}(BA).$$

Part II
Vector spaces and linear transformations

Chapter 4
Linear Transformations

4.1 Linear transformations and matrices

Let V and W be a vector spaces over the field $\mathbf{F}$. A *linear transformation* from V to W is a function $T : V \to W$ such that, for all vectors $\mathbf{v}, \mathbf{v}'$ in V and all scalars c in $\mathbf{F}$,

$$T(\mathbf{v}+\mathbf{v}') = T(\mathbf{v}) + T(\mathbf{v}') \tag{4.1}$$

and

$$T(c\mathbf{v}) = cT(\mathbf{v}). \tag{4.2}$$

A linear transformation $T : V \to V$, that is, a linear transformation from a vector space to itself, is called a *linear operator*. The core of linear algebra is the study of linear transformations and linear operators on finite-dimensional vector spaces.

It is important to state explicitly that we define linear transformations only between vector spaces over the same field. For example, we do not consider linear transformations from a complex vector space to a real vector space.

Here are simple examples of linear transformations.

Example 4.1.

The *identity function* $I_V : V \to V$ is defined by $I_V(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v} \in V$. Because $I_V(\mathbf{v}_1+\mathbf{v}_2) = \mathbf{v}_1+\mathbf{v}_2 = I_V(\mathbf{v}_1)+I_V(\mathbf{v}_2)$ and $I_V(c\mathbf{v}) = c\mathbf{v} = cI_V(\mathbf{v})$ for all $\mathbf{v}, \mathbf{v}_1, \mathbf{v}_2 \in V$ and $c \in \mathbf{F}$, it follows that I_V is a linear operator.

Example 4.2.

Let $\mathbf{0}_W$ be the zero vector in W. The *zero function* $0 : V \to W$, defined by $0(\mathbf{v}) = \mathbf{0}_W$ for all $\mathbf{v} \in V$, is a linear transformation.

Example 4.3.

Let V be a vector space, and let $V_1, V_2, \ldots, V_r$ be subspaces of V such that

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r.$$

Every vector $\mathbf{v} \in V$ can be represented uniquely in the form

$$\mathbf{v} = \mathbf{v}_1 \oplus \mathbf{v}_2 \oplus \cdots \oplus \mathbf{v}_r$$

with $\mathbf{v}_i \in V_i$ for $i = 1, \ldots, r$. Define the function $\pi_i : V \to V$ by

$$\pi_i(\mathbf{v}) = \mathbf{v}_i.$$

The function π_i is called the *projection* onto the subspace V_i. If $\mathbf{v}' \in V$ has the unique representation

$$\mathbf{v}' = \mathbf{v}'_1 \oplus \mathbf{v}'_2 \oplus \cdots \oplus \mathbf{v}'_r$$

with $\mathbf{v}'_i \in V_i$ for $i = 1, \ldots, r$, then

$$\mathbf{v} + \mathbf{v}' = (\mathbf{v}_1 + \mathbf{v}'_1) \oplus (\mathbf{v}_2 + \mathbf{v}'_2) \oplus \cdots \oplus (\mathbf{v}_r + \mathbf{v}'_r)$$

and, for every scalar c,

$$c\mathbf{v} = c\mathbf{v}_1 \oplus c\mathbf{v}_2 \oplus \cdots \oplus c\mathbf{v}_r$$

with $\mathbf{v}_i + \mathbf{v}'_i \in V_i$ and $c\mathbf{v}_i \in V_i$ for $i = 1, \ldots, r$. It follows that

$$\pi_i(\mathbf{v} + \mathbf{v}') = \mathbf{v}_i + \mathbf{v}'_i = \pi_i(\mathbf{v}) + \pi_i(\mathbf{v}')$$

and

$$\pi_i(c\mathbf{v}) = c\mathbf{v}_i = c\pi_i(\mathbf{v}).$$

Thus, π_i is a linear transformation for $i = 1, \ldots, r$.

The projections $\pi_1, \ldots, \pi_r$ have the following properties:

(i) $\pi_i^2 = \pi_i$ for $i = 1, \ldots, r$,
(ii) $\pi_i \pi_j = 0$ for $i \neq j$,
(iii) $I_V = \pi_1 + \pi_2 + \cdots + \pi_r$.

Example 4.4.

Let $T : V \to W$ be a linear transformation, and let V' be a subspace of V. The *restriction* of T to V' is the function $T|_{V'} : V' \to W$ defined by $T|_{V'}(\mathbf{v}') = T(\mathbf{v}')$ for all $\mathbf{v}' \in V'$. This is a linear transformation.

Example 4.5.

Let $V = \mathbf{R}^2$, and let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a 2×2 matrix with $a, b, c, d \in \mathbf{R}$. We define the function $T : V \to V$ by matrix multiplication:

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{R}^2$ and $s \in \mathbf{R}$. If $\mathbf{v}_1 = \begin{pmatrix} x_1 \\ y_2 \end{pmatrix}$ and $\mathbf{v}_2 = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$, then $\mathbf{v}_1 + \mathbf{v}_2 = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \end{pmatrix}$ and $s\mathbf{v} = \begin{pmatrix} sx \\ sy \end{pmatrix}$. We have

$$
\begin{aligned}
T(\mathbf{v}_1+\mathbf{v}_2) &= T\begin{pmatrix} x_1+x_2 \\ y_1+y_2 \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_1+x_2 \\ y_1+y_2 \end{pmatrix} \\
&= \begin{pmatrix} a(x_1+x_2)+b(y_1+y_2) \\ c(x_1+x_2)+d(y_1+y_2) \end{pmatrix} \\
&= \begin{pmatrix} (ax_1+by_1)+(ax_2+by_2) \\ (cx_1+dy_1)+(cx_2+dy_2) \end{pmatrix} \\
&= \begin{pmatrix} ax_1+by_1 \\ cx_1+dy_1 \end{pmatrix} + \begin{pmatrix} ax_2+by_2 \\ cx_2+dy_2 \end{pmatrix} \\
&= T\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + T\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \\
&= T(\mathbf{v}_1)+T(\mathbf{v}_2)
\end{aligned}
$$

and

$$
\begin{aligned}
T(s\mathbf{v}) = T\begin{pmatrix} sx \\ sy \end{pmatrix} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} sx \\ sy_1 \end{pmatrix} \\
&= \begin{pmatrix} asx+bsy \\ csx+dsy \end{pmatrix} = \begin{pmatrix} s(ax+by) \\ s(cx+dy) \end{pmatrix} \\
&= s\begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} = sT(\mathbf{v}).
\end{aligned}
$$

Thus, T is a linear transformation.

Example 4.6.

There is an important generalization of this example. Consider an $m \times n$ matrix

$$
A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,1} & a_{1m,2} & \cdots & a_{m,n}. \end{pmatrix}
$$

We define the function $T_A : \mathbf{R}^n \to \mathbf{R}^m$ as follows: For $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, let

$$
T_A(x) = Ax = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,1} & a_{1m,2} & \cdots & a_{m,n}. \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n a_{1,j}x_j \\ \sum_{j=1}^n a_{2,j}x_j \\ \vdots \\ \sum_{j=1}^n a_{n,j}x_j \end{pmatrix}
$$

For $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and $\mathbf{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, we have

$$\begin{aligned}
T_A(\mathbf{x}+\mathbf{y}) &= \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,1} & a_{1m,2} & \cdots & a_{m,n}. \end{pmatrix} \begin{pmatrix} x_1+y_1 \\ x_2+y_2 \\ \vdots \\ x_n+y_n \end{pmatrix} \\
&= \begin{pmatrix} \sum_{j=1}^n a_{1,j}(x_j+y_j) \\ \sum_{j=1}^n a_{2,j}(x_j+y_j) \\ \vdots \\ \sum_{j=1}^n a_{n,j}(x_j+y_j) \end{pmatrix} \\
&= \begin{pmatrix} \sum_{j=1}^n a_{1,j}x_j \\ \sum_{j=1}^n a_{2,j}x_j \\ \vdots \\ \sum_{j=1}^n a_{n,j}x_j \end{pmatrix} + \begin{pmatrix} \sum_{j=1}^n a_{1,j}y_j \\ \sum_{j=1}^n a_{2,j}y_j \\ \vdots \\ \sum_{j=1}^n a_{n,j}y_j \end{pmatrix} \\
&= T_A(x) + T_A(y).
\end{aligned}$$

Similarly, for $s \in \mathbf{F}$ we have

$$\begin{aligned}
T_A(s\mathbf{x}) &= \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,1} & a_{1m,2} & \cdots & a_{m,n}. \end{pmatrix} \begin{pmatrix} sx_1 \\ sx_2 \\ \vdots \\ sx_n \end{pmatrix} \\
&= \begin{pmatrix} \sum_{j=1}^n a_{1,j}(sx_j) \\ \sum_{j=1}^n a_{2,j}(sx_j) \\ \vdots \\ \sum_{j=1}^n a_{n,j}(sx_j) \end{pmatrix} = \begin{pmatrix} s\sum_{j=1}^n a_{1,j}x_j \\ s\sum_{j=1}^n a_{2,j}x_j \\ \vdots \\ s\sum_{j=1}^n a_{n,j}x_j \end{pmatrix} \\
&= s\begin{pmatrix} \sum_{j=1}^n a_{1,j}x_j \\ \sum_{j=1}^n a_{2,j}x_j \\ \vdots \\ \sum_{j=1}^n a_{n,j}x_j \end{pmatrix} \\
&= sT_A(\mathbf{x}).
\end{aligned}$$

Thus, every $m \times n$ matrix A induces a linear transformation $T_A : \mathbf{R}^n \to \mathbf{R}^m$.

Example 4.7.

Let V be a vector space, and let $V_1, \ldots, V_r$ be subspaces of V such that $V = \oplus_{i=1}^r V_i$. Let W be a vector space, and let $W_1, \ldots, W_r$ be subspaces of W such that $W = \oplus_{i=1}^r W_i$. For $i = 1, \ldots, r$, let $T_i : V_i \to W_i$ be a linear transformation. Define the function $T : V \to W$ as follows: Every vector $\mathbf{v} \in V$ has a unique representation in the form $\mathbf{v} = \mathbf{v}_1 + \cdots + \mathbf{v}_r$, where $\mathbf{v}_i \in V_i$ for $i = 1, \ldots, r$. Define

$$T(\mathbf{v}) = T_1(\mathbf{v}_1) + T_2(\mathbf{v}_2) + \cdots + T_1(\mathbf{v}_n).$$

If $\mathbf{v}' = \mathbf{v}'_1 + \cdots + \mathbf{v}'_r$, where $\mathbf{v}'_i \in V_i$ for $i = 1, \ldots, r$, then

$$\begin{aligned} \mathbf{v} + \mathbf{v}' &= (\mathbf{v}_1 + \cdots + \mathbf{v}_r) + (\mathbf{v}'_1 + \cdots + \mathbf{v}'_r) \\ &= (\mathbf{v}_1 + \mathbf{v}'_1) + \cdots + (\mathbf{v}_r + \mathbf{v}'_r) \end{aligned}$$

and so

$$\begin{aligned} T(\mathbf{v} + \mathbf{v}') &= T\left((\mathbf{v}_1 + \mathbf{v}'_1) + \cdots + (\mathbf{v}_r + \mathbf{v}'_r)\right) \\ &= T_1(\mathbf{v}_1 + \mathbf{v}'_1) + \cdots + T_r(\mathbf{v}_r + \mathbf{v}'_r) \\ &= T_1(\mathbf{v}_1) + T_1(\mathbf{v}'_1) + \cdots + T_r(\mathbf{v}_r) + T_1(\mathbf{v}'_r) \\ &= (T_1(\mathbf{v}_1) + \cdots + T_1(\mathbf{v}_r)) + \left(T_1(\mathbf{v}'_1) + \cdots + T_1(\mathbf{v}'_r)\right) \\ &= T(\mathbf{v}) + T(\mathbf{v}'). \end{aligned}$$

Similarly,

$$\begin{aligned} T(c\mathbf{v}) &= T\left(c(\mathbf{v}_1 + \cdots + \mathbf{v}_r)\right) \\ &= T\left(c\mathbf{v}_1 + \cdots + c\mathbf{v}_r\right) \\ &= T_1(c\mathbf{v}_1) + \cdots + T_r(c\mathbf{v}_r) \\ &= cT_1(\mathbf{v}_1) + \cdots + cT_r(\mathbf{v}_r) \\ &= c\left(T_1(\mathbf{v}_1) + \cdots + T_r(\mathbf{v}_r)\right) \\ &= cT(\mathbf{v}) \end{aligned}$$

for all $\mathbf{v} \in V$ and $c \in \mathbf{F}$, and so T is a linear transformation.

Lemma 4.1. *Let V and W be a vector spaces over the field $\mathbf{F}$ with zero vectors $\mathbf{0}_V$ and $\mathbf{0}_W$, respectively. If $T : V \to W$ is a linear transformation, then*

(i) $T(\mathbf{0}_V) = \mathbf{0}_W$
(ii) . $T(-\mathbf{v}) = -T(\mathbf{v})$ *for all* $\mathbf{v} \in V$
(iii) If $\mathbf{v}_1, \ldots, \mathbf{v}_r \in V$ *and* $c_1, \ldots, c_r \in \mathbf{F}$*, then*

$$T(c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_r\mathbf{v}_r) = c_1T(\mathbf{v}_1) + c_2T(\mathbf{v}_2) + \cdots + c_rT(\mathbf{v}_r)$$

Proof. We have $\mathbf{0}_V = \mathbf{0}_V + \mathbf{0}_V$ and so

$$T(\mathbf{0}_V) = T(\mathbf{0}_V + \mathbf{0}_V) = T(\mathbf{0}_V) + T(\mathbf{0}_V).$$

Adding the vector $-T(\mathbf{0}_V)$ to both sides of this vector equation, we obtain

$$\begin{aligned}
\mathbf{0}_W &= T(\mathbf{0}_V) + (-T(\mathbf{0}_V)) \\
&= (T(\mathbf{0}_V) + T(\mathbf{0}_V)) + (-T(\mathbf{0}_V)) \\
&= T(\mathbf{0}_V) + (T(\mathbf{0}_V) + (-T(\mathbf{0}_V)) \\
&= T(\mathbf{0}_V) + \mathbf{0}_W \\
&= T(\mathbf{0}_V).
\end{aligned}$$

This proves (i). Similarly,

$$T(\mathbf{v}) + T(-\mathbf{v}) = T(\mathbf{v} + (-\mathbf{v})) = T(\mathbf{0}_V) = \mathbf{0}_W$$

and so $T(-\mathbf{v}) = -T(\mathbf{v})$. This proves (ii).

We prove (iii) by induction on r. For $r = 1$ we have $T(c_1\mathbf{v}_1) = c_1T(\mathbf{v}_1)$ because a linear transformation satisfies (4.2). Let $r \geq 2$ and assume that (iii) holds for linear combinations of $r-1$ vectors. We can write the linear combination $c_1\mathbf{v}_1 + \cdots + c_r\mathbf{v}_r$ as the sum of the two vectors $c_1\mathbf{v}_1 + \cdots + c_{r-1}\mathbf{v}_{r-1}$ and $c_r\mathbf{v}_r$. Using property (4.1), we have

$$\begin{aligned}
T(c_1\mathbf{v}_1 + \cdots + c_r\mathbf{v}_r) &= T((c_1\mathbf{v}_1 + \cdots + c_{r-1}\mathbf{v}_{r-1}) + c_r\mathbf{v}_r) \\
&= T(c_1\mathbf{v}_1 + \cdots + c_{r-1}\mathbf{v}_{r-1}) + T(c_r\mathbf{v}_r)) \\
&= \sum_{i=1}^{r-1} c_iT(\mathbf{v}_i) + c_rT(\mathbf{v}_r) \\
&= \sum_{i=1}^{r} c_iT(\mathbf{v}_i)
\end{aligned}$$

This completes the induction.

Lemma 4.2. *Let U, V, and W be a vector spaces over the field $\mathbf{F}$, and let $S : U \to V$ and $T : V \to W$ be linear transformations. The composite function $TS : U \to W$ defined by*

$$TS(\mathbf{u}) = T(S(\mathbf{u})) \qquad \text{for all } \mathbf{u} \in U$$

is a linear transformation. Moreover, composition of linear transformations is associative: If $V_1, \ldots, V_4$ are vector spaces and $T_i : V_i \to V_{i+1}$ is a linear transformation for $i = 1, 2, 3$, then

$$T_3(T_2T_1) = (T_3T_2)T_1.$$

Proof. For all $\mathbf{u}, \mathbf{u}' \in U$ and $c \in \mathbf{F}$ we have

$$\begin{aligned}
TS(\mathbf{u} + \mathbf{u}') &= T(S(\mathbf{u} + \mathbf{u}')) \\
&= T(S(\mathbf{u}) + S(\mathbf{u}')) \\
&= T(S(\mathbf{u})) + T(S(\mathbf{u}')) \\
&= TS(\mathbf{u}) + TS(\mathbf{u}')
\end{aligned}$$

and

$$TS(c\mathbf{u}) = T(S(c\mathbf{u})) = T(cS(\mathbf{u})) = cT(S(\mathbf{u})) = cTS(\mathbf{u})$$

and so TS is a linear transformation.

Next we prove associativity of composition. For all $\mathbf{v}_1 \in V_1$, we have

$$\begin{aligned}((T_3T_2)T_1)(\mathbf{v}_1) &= (T_3T_2)(T_1(\mathbf{v}_1)) = T_3(T_2(T_1(\mathbf{v}_1))) \\ &= T_3((T_2T_1)(\mathbf{v}_1)) = (T_3(T_2T_1))(\mathbf{v}_1).\end{aligned}$$

This completes the proof.

Let $T : V \to W$ be a linear transformation. The *image* of a subset X of V is

$$T(X) = \{T(\mathbf{v}) : \mathbf{v} \in X\} = \{w \in W : w = T(\mathbf{v}) \text{ for some } \mathbf{v} \in X\}.$$

The *inverse image* of a subset Y of W is

$$T^{-1}(Y) = \{\mathbf{v} \in V : T(\mathbf{v}) \in Y\}.$$

Lemma 4.3. *Let V and W be vector spaces over the field $\mathbf{F}$, and let $T : V \to W$ be a linear transformation. If V' is a subspace of V, then $T(V')$ is a subspace of W. If W' is a subspace of W, then $T^{-1}(W')$ is a subspace of V.*

Proof. Let V' be a subspace of V. Because $\mathbf{0} \in V'$ we have $T(\mathbf{0}) = \mathbf{0} \in T(V')$. If $\mathbf{w}_1, \mathbf{w}_2 \in T(V')$, then there exist vectors $\mathbf{v}_1, \mathbf{v}_2 \in V'$ such that $T(\mathbf{v}_1) = \mathbf{w}_1$ and $T(\mathbf{v}_2) = \mathbf{w}_2$. Because V' is a subspace, we have $\mathbf{v}_1 + \mathbf{v}_2 \in V'$ and so

$$\mathbf{w}_1 + \mathbf{w}_2 = T(\mathbf{v}_1) + T(\mathbf{v}_2) = T(\mathbf{v}_1 + \mathbf{v}_2) \in T(V').$$

Similarly, if $c \in \mathbf{F}$, then $c\mathbf{v}_1 \in V'$ and

$$c\mathbf{w}_1 = cT(\mathbf{v}_1) = T(c\mathbf{v}_1) \in T(V').$$

This proves that the image of V' is a subspace of W.

Let W' be a subspace of W. If $\mathbf{v}_1, \mathbf{v}_2 \in T^{-1}(W')$ and $c \in \mathbf{F}$, then $T(\mathbf{v}_1) \in W'$, $T(\mathbf{v}_1) \in W'$, and so

$$T(\mathbf{v}_1 + \mathbf{v}_2) = T(\mathbf{v}_1) + T(\mathbf{v}_2) \in W'$$

and so $\mathbf{v}_1 + \mathbf{v}_2 \in T^{-1}(W')$. Similarly, if $c \in \mathbf{F}$, then

$$T(c\mathbf{v}_1) = cT(\mathbf{v}_1) \in W'$$

and so $c\mathbf{v}_1 \in T^{-1}(W')$. Thus, $T^{-1}(W')$ is a subspace of V. This completes the proof.

Let V and W be vector spaces over the field $\mathbf{F}$, and let $T : V \to W$ be a linear transformation. The *image* of T is

$$\text{image}(T) = \{\mathbf{w} \in W : \mathbf{w} = T(V) \text{ for some } V \in V\} = T(V).$$

The *kernel* of T is

$$\text{kernel}(T) = \{V \in V : T(V) = \mathbf{0}\} = T^{-1}(\{\mathbf{0}\}).$$

Lemma 4.4. *The kernel of T is a subspace of V, and the image of T is a subspace of W.*

Proof. Because V is a subspace of V and $\{\mathbf{0}\}$ is a subspace of W, Lemma 4.3 implies that $\mathrm{image}(T) = T(V)$ and $\mathrm{kernel}(T) = T^{-1}(\{\mathbf{0}\})$ are subspaces of of W and V, respectively.

The dimension of the image of T is called the *rank* of T, that is,

$$\mathrm{rank}(T) = \dim(\mathrm{image}(T)).$$

The dimension of the kernel of T is called the *nullity* of T, that is,

$$\mathrm{nullity}(T) = \dim(\mathrm{kernel}(T)).$$

Here are some computations of kernels and images of linear operators on $\mathbf{R}^2$.

Example 4.8.

Consider the linear transformation $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by $T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix}$. We have

$$\begin{aligned}
\mathrm{kernel}(T) &= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 : T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \\
&= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 : \begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \\
&= \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 : x = 0 \right\} \\
&= \left\{ \begin{pmatrix} 0 \\ y \end{pmatrix} \in \mathbf{R}^2 \right\} \\
&= \left\{ y\begin{pmatrix} 0 \\ 1 \end{pmatrix} : y \in \mathbf{R}^2 \right\}.
\end{aligned}$$

Thus, the kernel of T is the one-dimensional subspace of $\mathbf{R}^2$ spanned by the vector $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, that is, the y-axis in the plane.

Similarly,

$$\begin{aligned}
\mathrm{image}(T) &= \left\{ T\begin{pmatrix} x \\ y \end{pmatrix} : \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 \right\} \\
&= \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} \in \mathbf{R}^2 \right\} \\
&= \left\{ x\begin{pmatrix} 1 \\ 0 \end{pmatrix} : x \in \mathbf{R}^2 \right\}.
\end{aligned}$$

Thus, the image of T is the one-dimensional subspace of $\mathbf{R}^2$ spanned by the vector $\begin{pmatrix}1\\0\end{pmatrix}$, that is, the x-axis in the plane.

Example 4.9.

Consider the linear transformation $T:\mathbf{R}^2\to\mathbf{R}^2$ defined by $T\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}y\\x\end{pmatrix}$. We have

$$\begin{aligned}
\text{kernel}(T) &= \left\{\begin{pmatrix}x\\y\end{pmatrix}\in\mathbf{R}^2 : T\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}\right\}\\
&= \left\{\begin{pmatrix}x\\y\end{pmatrix}\in\mathbf{R}^2 : \begin{pmatrix}y\\x\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}\right\}\\
&= \left\{\begin{pmatrix}x\\y\end{pmatrix}\in\mathbf{R}^2 : x=y=0\right\}\\
&= \left\{\begin{pmatrix}0\\0\end{pmatrix}\in\mathbf{R}^2\right\}
\end{aligned}$$

and so the kernel of T is the zero-dimensional subspace of $\mathbf{R}^2$. For every vector $\begin{pmatrix}x\\y\end{pmatrix}\in\mathbf{R}^2$ we have $\begin{pmatrix}y\\x\end{pmatrix}\in\mathbf{R}^2$ and $T\begin{pmatrix}y\\x\end{pmatrix}=\begin{pmatrix}x\\y\end{pmatrix}$. Therefore, every vector in $\mathbf{R}^2$ is in the image of T, and so the image of T is the two-dimensional subspace $\mathbf{R}^2$.

Example 3. Consider the linear transformation $T:\mathbf{R}^2\to\mathbf{R}^2$ defined by the matrix $T=\begin{pmatrix}1&2\\2&4\end{pmatrix}$. Thus, $T\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x+2y\\2x+4y\end{pmatrix}$ for all $\begin{pmatrix}x\\y\end{pmatrix}\in\mathbf{R}^2$. We have

$$\begin{aligned}
\text{kernel}(T) &= \left\{\begin{pmatrix}x\\y\end{pmatrix}\in\mathbf{R}^2 : \begin{pmatrix}x+2y\\2x+4y\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}\right\}\\
&= \left\{\begin{pmatrix}x\\y\end{pmatrix}\in\mathbf{R}^2 : \begin{pmatrix}x+2y\\2(x+2y)\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}\right\}\\
&= \left\{\begin{pmatrix}x\\y\end{pmatrix}\in\mathbf{R}^2 : x+2y=0\right\}\\
&= \left\{\begin{pmatrix}-2y\\y\end{pmatrix}\in\mathbf{R}^2 : y\in\mathbf{R}\right\}\\
&= \left\{y\begin{pmatrix}-2\\1\end{pmatrix}\in\mathbf{R}^2 :\right\}
\end{aligned}$$

and so the kernel of T is the one-dimensional subspace generated by the vector $\begin{pmatrix}-2\\1\end{pmatrix}$, or, equivalently, the line $y=-x/2$ in the Euclidean plane.

If $\begin{pmatrix}x\\y\end{pmatrix}\in\text{image}(T)$, then there exists $\begin{pmatrix}x'\\y'\end{pmatrix}\in\mathbf{R}^2$ such that

$$\begin{pmatrix} x \\ y \end{pmatrix} = T\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x'+2y' \\ 2x'+4y' \end{pmatrix}$$

and so

$$y = 2x'+4y' = 2(x'+2y') = 2x.$$

ConVersely, if $y = 2x$, then

$$T\begin{pmatrix} x \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ 2x \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

and so

$$\text{image}(T) = \left\{ \begin{pmatrix} x \\ 2x \end{pmatrix} \in \mathbf{R}^2 : x \in \mathbf{R} \right\} = \left\{ x\begin{pmatrix} 1 \\ 2 \end{pmatrix} \in \mathbf{R}^2 : x \in \mathbf{R} \right\}.$$

Thus, the image of T is the one-dimensional subspace generated by the vector $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$, or, equivalently, the line $y = 2x$ in the Euclidean plane.

The linear transformation $T : V \to W$ is *one-to-one* if for all vectors $\mathbf{v}, \mathbf{v}' \in V$ we have $T(\mathbf{v}) = T(\mathbf{v}')$ if and only if $\mathbf{v} = \mathbf{v}'$. A one-to-one function is also called an *injection* or a *monomorphism*.

For example, the linear transformation $T : \mathbf{R} \to \mathbf{R}^2$ defined by $T(x) = \begin{pmatrix} x \\ 2x \end{pmatrix}$ is one-to-one.

Lemma 4.5. *The linear transformation $T : V \to W$ is one-to-one if and only if kernel$(T) = \{0\}$.*

Proof. Suppose that T is one-to-one. If $\mathbf{v} \in \text{kernel}(T)$, then $T(\mathbf{v}) = 0 = T(0)$, and so $\mathbf{v} = 0$, that is, $\text{kernel}(T) = \{0\}$.

ConVersely, suppose that $\text{kernel}(T) = \{0\}$. If $\mathbf{v}, \mathbf{v}' \in V$ and $T(\mathbf{v}) = T(\mathbf{v}')$, then

$$0 = T(\mathbf{v}) - T(\mathbf{v}') = T(\mathbf{v} - \mathbf{v}')$$

and so $\mathbf{v} - \mathbf{v}' \in \text{kernel}(T) = \{0\}$. Therefore, $\mathbf{v} - \mathbf{v}' = 0$ or, equivalently, $\mathbf{v} = \mathbf{v}'$ and so the linear transformation T is one-to-one. This completes the proof.

Lemma 4.6. *Let $T_A : \mathbf{R}^n \to \mathbf{R}^m$ be the linear transformation defined by the $m \times n$ matrix*

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,1} & a_{1m,2} & \cdots & a_{m,n} \end{pmatrix}.$$

For $j = 1, \ldots, n$, let

$$\mathbf{w}_j = \begin{pmatrix} a_{1,j} \\ a_{2,j} \\ \vdots \\ a_{m,j} \end{pmatrix} \in \mathbf{R}^m$$

be the vector whose coordinates are the coordinates in the jth column of A. The image of T_A is the subspace of $\mathbf{R}^m$ spanned by the set of vectors $\{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n\}$.

The linear transformation T_A is one-to-one if and only if the set of vectors $\{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n\}$ is linearly independent.

Proof. We have $y \in \text{image}(T_A)$ if and only if there exists a vector $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{R}^n$ such that

$$\begin{aligned} y = T_A(x) &= \begin{pmatrix} \sum_{j=1}^n a_{1,j}x_j \\ \sum_{j=1}^n a_{2,j}x_j \\ \vdots \\ \sum_{j=1}^n a_{m,j}x_j \end{pmatrix} \\ &= x_1 \begin{pmatrix} a_{1,1} \\ a_{2,1} \\ \vdots \\ a_{m,1} \end{pmatrix} + x_2 \begin{pmatrix} a_{1,2} \\ a_{2,2} \\ \vdots \\ a_{m,2} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{1,n} \\ a_{2,n} \\ \vdots \\ a_{m,n} \end{pmatrix} \\ &= x_1\mathbf{w}_1 + x_2\mathbf{w}_2 + \cdots + x_n\mathbf{w}_n \end{aligned}$$

if and only if $y \in \langle\{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n\}\rangle$.

Moreover, $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \text{kernel}(T_A)$ if and only if $\sum_{i=1}^n x_i\mathbf{w}_i = 0$, and so $\text{kernel}(T_A) \neq \{0\}$ if and only if the set $\{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n\}$ is linearly dependent. This completes the proof.

The linear transformation $T : V \to W$ is *onto* if, for each $\mathbf{w} \in W$ there exists $\mathbf{v} \in V$ such that $T(\mathbf{v}) = \mathbf{w}$. EquiValently, T is onto if $\text{image}(T) = W$. An onto function is also called a *surjection* or an *epimorphism*.

For example, the linear transformation $T : \mathbf{R}^2 \to \mathbf{R}$ defined by $T \begin{pmatrix} x \\ y \end{pmatrix} = x$ is onto.

The linear transformation $T : V \to W$ is an *isomorphism* if T is one-to-one and onto. vector spaces V and W are *isomorphic* if there exists an isomorphism from $T : V \to W$. An isomorphism from a vector space to itself is called an *automorphismautomorphism*.

For example, the linear transformation $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by $T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}$ is an automorphism.

For every vector space V, the identity operator $\text{id}_V : V \to V$ defined by $\text{id}_V(\mathbf{v}) = \mathbf{v}$ for all $\mathbf{v} \in V$ is an automorphism. If $T :\to W$ is a linear transformation, then

$$T \,\mathrm{id}_V = \mathrm{id}_W \, T = T.$$

The linear transformation $T : V \to W$ is *invertible* if there exists a linear transformation $S : W \to V$ such that $ST = \mathrm{id}_V$ and $TS = \mathrm{id}_W$. The linear transformation S is called an *inverse* of T. If $S' : W \to V$ is also an inverse of T, then

$$S' = S' \,\mathrm{id}_W = S'(TS) = (S'T)S = \mathrm{id}_V \, S = S$$

and so the inverse of T, if it exists, is unique. We denote the inverse of T by T^{-1}. Moreover, if T is invertible, then T^{-1} is invertible, and

$$\left(T^{-1}\right)^{-1} = T.$$

Lemma 4.7. *A linear transformation $T : V \to W$ is invertible if and only if it is one-to-one and onto.*

Proof. Suppose that T is invertible with inverse $T^{-1} : W \to V$. If $V \in \mathrm{kernel}(T)$, then $T(V) = 0$ and so

$$0 = T^{-1}(0) = T^{-1}(T(V)) = \left(T^{-1}T\right)(V) = \mathrm{id}_V(V) = V$$

and $\mathrm{kernel}(T) = \{0\}$. By Lemma 4.5, the linear transformation T is one-to-one. If $w \in W$, then $T^{-1}(w) \in V$ and so $w = T\left(T^{-1}(w)\right) \in T(V)$. Thus, $T(V) = W$ and T is onto.

Suppose that T is one-to-one and onto. Let $w \in W$. Because T is onto, there exists $V \in V$ such that $T(V) = w$. Moreover, because T is one-to-one, V is the unique vector in V such that $T(V) = w$. Define $S : W \to V$ by $S(w) = V$. Then $TS(w) = T(V) = w$ for all $w \in W$, or, equivalently, $TS = \mathrm{id}_W$. Moreover, if $V \in V$, then $w = T(V) \in W$, and V is the unique vector in V such that $T(V) = w$. Therefore, $V = S(w) = ST(V)$ and $ST = \mathrm{id}_V$.

We must prove that S is a linear transformation. Let $w, w' \in W$ and let $V, V' \in V$ satisfy $S(w) = V$ and $S(w') = V'$. Then $T(V) = w$ and $T(V') = w'$. It follows that $T(V + V') = T(V) + T(V') = w + w'$ and so $S(w + w') = V + V' = S(w) + S(w')$. Similarly, if $c \in \mathbf{F}$, then $T(cV) = cT(V) = cw$ and so $S(cw) = cV = cS(w)$. Thus, S is a linear transformation. This completes the proof.

Exercises

1. Define the function $T : \mathbf{R}^2 \to \mathbf{R}^2$ by

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ x \end{pmatrix}.$$

   a. Prove that T is a linear transformation and that $T^2 = T$.
   b. Prove that $T^n = T$ for all positive integers n.

c. Compute kernel(T) and image(T).

2. Define the function $T : \mathbf{R}^2 \to \mathbf{R}^2$ by
$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ 0 \end{pmatrix}.$$
a. Prove that T is a linear transformation such that $T^2 = 0$.
b. Compute kernel(T) and image(T).

3. Define the function $T : \mathbf{C}^2 \to \mathbf{C}^2$ by
$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ix \\ -y \end{pmatrix}.$$
a. Prove that T is a linear transformation.
b. Prove that $T^4 = I_2$.

4. $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by
$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}.$$
a. Prove that T is a linear transformation.
b. Prove that $T^2 = I_2$.
c. Compute
$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2 : T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \right\}.$$

5. Let $V = \mathbf{R}[t]$ be the vector space of polynomials with real coefficients. Define the function $D : V \to V$ by differentiation:
$$D(a_n t^n + a_{n-1}t^{n-1} + \cdots + a_2t^2 + a_1t + a_0) = \\ na_nt^{n-1} + (n-1)a_{n-2}t^{n-2} + \cdots + 2a_2t + a_1$$
It is proved in calculus that differentiation is a linear transformation: If f and g are polynomials, and if $c \in \mathbf{R}$, then $D(f+g) = D(f) + D(g)$ and $D(cf) = cD(f)$. It follows that $D^k : V \to V$ is a linear transformation for all positive integers k.

a. Compute the kernel of D.
b. Compute the kernel of D^2.
c. Compute the kernel of D^k for all positive integers k.

6. Let $T : V \to V$ be a linear operator. A *fixed point* of T is a vector $V \in V$ such that $T(V) = V$. Prove that the set of fixed points
$$\{V \in V : T(V) = V\}$$
is a subspace of V.

7. Let $T : V \to V$ be a linear operator on the finite-dimensional vector space V.

a. Prove that $T^{i+1}(V) \subseteq T^i(V)$ for all nonnegative integers i.
b. Prove that if $T^{i+1}(V) = T^i(V)$, then $T^j(V) = T^i(V)$ for all $j \geq i$.

8. Let V be a vector space, and consider the vector space

$$V \oplus V = \{(V_1, V_2) : V_1, V_2 \in V\}.$$

a. Prove that the function $T : V \oplus V \to V$ defined by

$$T(V_1, V_2) = V_1 - V_2$$

is a linear transformation.
b. Prove that the function $S : V \to V \oplus V$ defined by

$$S(V) = (V, V)$$

is a linear transformation.
c. Prove that image$(S) =$ kernel(T).
d. Prove that

$$0 \longrightarrow V \xrightarrow{S} V \oplus V \xrightarrow{T} V \longrightarrow 0$$

is a short exact sequence of vector spaces.

4.2 Kernel and image of a linear transformation

The *nullity* of T is the dimension of the kernel of T:

$$\text{nullity}(T) = \dim(\text{kernel}(T))$$

The *rank* of T is the dimension of the image of T:

$$\text{rank}(T) = \dim(\text{image}(T)).$$

Theorem 4.1. *Let $T : V \to W$ be a linear transformation. If V is a finite-dimensional vector space, then*

$$\dim(V) = \mathit{nullity}(T) + \mathit{rank}(T).$$

Proof. If V is finite-dimensional, then $\mathbf{F} = \text{kernel}(T)$ is a finite-dimensional subspace of V. Let $n = \dim(V)$ and $k = \text{nullity}(T) = \dim(\text{kernel}(T))$. Let $S = \{V_1, \ldots, V_k\}$ be a basis for kernel(T). By Theorem **??**, there is a set $S' = \{V_{k+1}, \ldots, V_n\}$ such that $S \cup S'$ is a basis for V.

If $V \in V$, then there exist unique scalars $x_1, \ldots, x_n$ such that $V = \sum_{i=1}^n x_i V_i$ and so

$$T(V) = T\left(\sum_{i=1}^n x_i V_i\right) = \sum_{i=1}^n x_i T(V_i) = \sum_{i=k+1}^n x_i T(V_i)$$

because $T(V_i) = 0$ for $i = 1, \ldots, k$. It follows that the set $\{T(V_i) : i = k+1, \ldots, n\}$ spans image(T).

We shall prove that the set $\{T(V_i) : i = k+1, \ldots, n\}$ is linearly independent. If $c_{k+1}, \ldots, c_n$ are scalars such that

$$\sum_{i=k+1}^{n} c_i T(V_i) = 0$$

then the linearity of T implies that

$$T\left(\sum_{i=k+1}^{n} c_i V_i\right) = 0$$

and so

$$\sum_{i=k+1}^{n} c_i V_i \in \text{kernel}(T).$$

Because $\{V_1, \ldots, V_k\}$ is a basis for kernel$)T)$, there exist scalars $c_1, \ldots, c_k$ such that

$$\sum_{i=k+1}^{n} c_i V_i = \sum_{i=1}^{k} c_i V_i$$

and so

$$\sum_{i=1}^{k} (-c_i) V_i + \sum_{i=k+1}^{n} c_i V_i = 0.$$

The linear independence of the set $\{V_1, \ldots, V_n\}$ implies that $c_i = 0$ for $i = k+1, \ldots, n$, and so the set $\{T(V_i) : i = k+1, \ldots, n\}$ is linearly independent. Thus, $\{T(V_i) : i = k+1, \ldots, n\}$ is a basis for image(T), and so

$$\begin{aligned}
\text{rank}(T) &= \dim(\text{image}(T)) \\
&= n - k \\
&= \dim(V) - \dim(\text{kernel}(T)) \\
&= \dim(V) - \text{nullity}(T).
\end{aligned}$$

This completes the proof.

Corollary 4.1. *Let V and W be finite-dimensional vector spaces, with* $\dim(V) = \dim(W)$. *Let $T : V \to W$ be a linear transformation. The following are equivalent:*

1. *kernel$(T) = \{0\}$*
2. *image$(T) = W$*
3. *T is an isomorphism.*

Proof. Let $\dim(V) = \dim(W) = n$. By Theorem 4.1, if kernel$(T) = \{0\}$, then nullity$(T) = 0$ and

$$\dim(W) = \dim(V) = \text{nullity}(T) + \text{rank}(T) = \text{rank}(T)$$

and $\text{image}(T) = W$, and so T is an isomorphism.

ConVersely, if $\text{image}(T) = W$, then $\text{rank}(T) = \dim(W) = \dim(V)$ and so

$$\dim(V) = \text{nullity}(T) + \text{rank}(T) = \text{nullity}(T) + \dim(V).$$

This implies that $\text{nullity}(T) = 0$, and so $\text{kernel}(T) = \{0\}$ and T is an isomorphism. This completes the proof.

Let V and W be finite dimensional vector spaces of dimensions n and m, respectively, $T : V \to W$ be a linear transformation. Let r be the rank of T, that is, the dimension of the image of T. It follows that $\text{nullity}(T) = \dim(\text{kernel}(T)) = n - r$. Let $\mathscr{B} = \{\mathbf{e}_1, \ldots, \mathbf{e}_{n-r}\}$ be a basis for the kernel of T. Choose vectors $\{\mathbf{e}_{n-r+1}, \ldots, \mathbf{e}_n\}$ in V such that $\{\mathbf{e}_1, \ldots, \mathbf{e}_{n-r}, \mathbf{e}_{n-r+1}, \ldots, \mathbf{e}_n\}$ is a basis for V. Let $\mathbf{e}_k = \mathbf{0}_V$ for $k = n+1, \ldots, n+m-r$.

Let $\mathbf{f}_i = \mathbf{0}_W$ for $i = 1, \ldots, n-r$. For $j = n-r+1, \ldots, n$, let $\mathbf{f}_j = T(\mathbf{e}_j) \in W$. The set $\{\mathbf{f}_{n-r+1}, \ldots, \mathbf{f}_n\}$ is a basis for the image of T. Choose vectors $\{\mathbf{f}_{n+1}, \ldots, \mathbf{f}_{n+m-r}\}$ in W such that $\{\mathbf{f}_{n-r+1}, \ldots, \mathbf{f}_n, \mathbf{f}_{n+1}, \ldots, \mathbf{f}_{n+m-r}\}$ is a basis for W. For $i = 1, \ldots, n+m-r$, let V_i be the subspace of V generated by $\mathbf{e}_i$ and let W_i be the subspace of W generated by $\mathbf{f}_i$. Note that $V_i = \{\mathbf{0}_V\}$ for $i = n+1, \ldots, n+m-r$ and that $W_i = \{\mathbf{0}_W\}$ for $i = 1, \ldots, n-r$. Define $T_i : V_i \to W_i$ by $T_i(\mathbf{e}_i) = \mathbf{f}_i$.

We obtain the direct sum decompositions

$$V = \bigoplus_{i=1}^{n+m-r} V_i$$

$$W = \bigoplus_{i=1}^{n+m-r} W_i$$

and, with respect to these decompositions,

$$T = \bigoplus_{i=1}^{n+m-r} T_i.$$

Note that

$$(\dim(V_i), \dim(W_i)) = \begin{cases} (1,0) & \text{for } i = 1, \ldots, r \\ (1,1) & \text{for } i = r+1, \ldots, n \\ (0,1) & \text{for } i = n+1, \ldots, n+m-r. \end{cases}$$

Here is an alternate construction/proof.. Let $r = \text{rank}(T)$, and let $\{\mathbf{f}_1,\ldots,\mathbf{f}_r\}$ be a basis for image(T). For $i = 1,\ldots,r$, choose $\mathbf{e}_i \in V$ such that $T(\mathbf{e}_i) = \mathbf{f}_i$. Let $s =$ nullity(T), and let $\{\mathbf{e}_{r+1},\ldots,\mathbf{e}_{r+s}\}$ be a basis for kernel(T). We shall prove that $n = r+s$ and that $\{\mathbf{e}_1,\ldots,\mathbf{e}_r,\mathbf{e}_{r+1},\ldots,\mathbf{e}_{r+s}\}$ is a basis for V. If $c_1,\ldots,c_{r+s}$ are scalars such that

$$\mathbf{0} = \sum_{i=1}^{r+s} c_i\mathbf{e}_i$$

then $T(\mathbf{e}_i) = \mathbf{0}$ for $i = r+1,\ldots,r+s$, and so

$$\mathbf{0} = T(\mathbf{0}) = T\left(\sum_{i=1}^{r+s} c_i\mathbf{e}_i\right) = \sum_{i=1}^{r+s} c_iT(\mathbf{e}_i) = \sum_{i=1}^{r} c_iT(\mathbf{e}_i) = \sum_{i=1}^{r} c_i\mathbf{f}_i.$$

The linear independence of $\{\mathbf{f}_1,\ldots,\mathbf{f}_r\}$ implies that $c_i = 0$ for $i = 1,\ldots,r$, and so

$$\mathbf{0} = \sum_{i=r+1}^{r+s} c_i\mathbf{e}_i.$$

The linear independence of $\{\mathbf{e}_{r+1},\ldots,\mathbf{e}_{r+s}\}$ implies that $c_i = 0$ for $i = r+1,\ldots,r+s$, and so the set $\{\mathbf{e}_1,\ldots,\mathbf{e}_{r+s}\}$ is linearly independent.

We shall prove that $\{\mathbf{e}_1,\ldots,\mathbf{e}_{r+s}\}$ generates V. Let $\mathbf{v} \in V$. Because $\{\mathbf{f}_1,\ldots,\mathbf{f}_r\}$ is a basis for image(T), there exist scalars $c_1,\ldots,c_r$ such that

$$T(\mathbf{v}) = \sum_{i=1}^{r} c_i\mathbf{f}_i = \sum_{i=1}^{r} c_iT(\mathbf{e}_i)$$

and so

$$T\left(\mathbf{v} - \sum_{i=1}^{r} c_i\mathbf{e}_i\right) = 0.$$

Therefore $\mathbf{v} - \sum_{i=1}^{r} c_i\mathbf{e}_i \in$ kernel(T). Because $\{\mathbf{e}_{r+s},\ldots,\mathbf{e}_{r+s}\}$ is a basis for kernel(T), there exist scalars $c_{r+1},\ldots,c_{r+s}$ such that

$$\mathbf{v} - \sum_{i=1}^{r} c_i\mathbf{e}_i = \sum_{i=r+1}^{r+s} c_i\mathbf{e}_i.$$

It follows that $\mathbf{v} = \sum_{i=1}^{r+s} c_i\mathbf{e}_i$, and so $\{\mathbf{e}_1,\ldots,\mathbf{e}_{r+s}\}$ generates V. Therefore, $\{\mathbf{e}_1,\ldots,\mathbf{e}_{r+s}\}$ is a basis for V, and

$$n = r+s = \text{rank}(T) + \text{nullity}(T).$$

The $m \times n$ matrix for T with respect to the bases $\mathscr{B}$ and $\mathscr{C}$ has the $r \times r$ identity matrix in the upper left corner and 0s everywhere else:

$$\begin{pmatrix}
1\,0\,0 \cdots 0\,0\,0 \ldots 0\\
0\,1\,0 \cdots 0\,0\,0 \ldots 0\\
0\,0\,1 \cdots 0\,0\,0 \ldots 0\\
\vdots \quad\quad \vdots \quad\quad\quad\quad\\
0\,0\,0 \cdots 1\,0\,0 \ldots 0\\
0\,0\,0 \cdots 0\,1\,0 \ldots 0\\
0\,0\,0 \cdots 0\,0\,0 \ldots 0\\
0\,0\,0 \cdots 0\,0\,0 \ldots 0\\
\vdots \quad\quad \vdots \quad\quad\quad\quad\\
0\,0\,0 \cdots 0\,0\,0 \ldots 0
\end{pmatrix}$$

Let V_1 be the subspace of V generated by $\{\mathbf{e}_1, \ldots, \mathbf{e}_r\}$, and let V_2 be the subspace of V generated by $\{\mathbf{e}_{r+1}, \ldots, \mathbf{e}_n\}$. Let $\mathbf{e}_i = \mathbf{0}_V$ for $i = n+1, \ldots, n+m-r$.

Let W_1 be the subspace of W generated by $\{\mathbf{f}_1, \ldots, \mathbf{f}_r\}$, and let W_2 be the subspace of W generated by $\{\mathbf{f}_{r+1}, \ldots, \mathbf{f}_m\}$. We have $\text{kernel}(T) = W_2$ and $\text{image}(T) = W_1$. The function $T|_{V_1} : V_1 \to W_1$ defined by $T|_{V_1}(\mathbf{e}_i) = \mathbf{f}_i$ for $i = 1, \ldots r$ is an isomorphism.

We call W_2 the *cokernel* of T, and we call V_1 the *coimage* of T.

For $i = 1, \ldots, r$, let V_i' be the one-dimensional subspace of V generated by $\mathbf{e}_i$ and let W_i' be the one-dimensional subspace of W generated by $\mathbf{f}_i$. Define the linear transformation $T_i' : V_i' \to W_i'$ by $T_i'(\mathbf{e}_i) = \mathbf{f}_i$.

For $i = n-r+1, \ldots, n$, let V_i' be the one-dimensional subspace of V generated by $\mathbf{e}_i$ and let $W_i' = \{\mathbf{0}_W\}$ be the zero-dimensional subspace of W. Define the linear transformation $T_i' : V_i' \to W_i'$ by $T_i'(\mathbf{e}_i) = \mathbf{0}_W$.

For $i = m-r+1, \ldots, m$, let $V_i' = \{\mathbf{0}_V\}$ be the zero-dimensional subspace of V, and let W_i' be the one-dimensional subspace of W generated by $\mathbf{f}_i$. Define the linear transformation $T_i' : V_i' \to W_i'$ by $T_i'(\mathbf{0}_V) = \mathbf{0}_W$.

We write

$$T = \oplus_{i=1}^{n+m-r} T_i.$$

We have

$$V = \bigoplus_{i=1}^{n} V_i'$$

$$W = \bigoplus_{i=1}^{m} W_i'$$

and

$$T = \bigoplus_{i=1}^{m} T_i'.$$

Exercises

1. Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the linear transformation

$$T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}.$$

   Compute the matrix for T with respect to the standard basis for $\mathbf{R}^3$. Compute kernel(T), nullity(T), image(T), and rank(T), and Verify that nullity$(T)+$ rank$(T) = 3$.

2. Let $T : \mathbf{R}^4 \to \mathbf{R}^2$ be the linear transformation

$$T\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ x_3 + x_4 \end{pmatrix}.$$

   Compute the matrix for T with respect to the standard bases for $\mathbf{R}^4$ and $\mathbf{R}^2$. Compute kernel(T), nullity(T), image(T), and rank(T), and Verify that nullity$(T)+$ rank$(T) = 4$.

3. Let $T : \mathbf{R}^4 \to \mathbf{R}^3$ be the linear transformation

$$T\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ x_3 + x_4 \\ x_1 + x_2 + x_3 + x_4 \end{pmatrix}.$$

   Compute the matrix for T with respect to the standard bases for $\mathbf{R}^4$ and $\mathbf{R}^3$. Compute kernel(T), nullity(T), image(T), and rank(T), and Verify that nullity$(T)+$ rank$(T) = 4$.

4. Let $T : V \to W$ be a linear transformation with $\dim(V) = n$. Let $\{f_1, \ldots, f_k\}$ be a linearly independent subset of kernel(T). Prove that if $V \in V$ and $T(V) \neq 0$, then $\{V + f_1, \ldots, V + f_k\}$ is a linearly independent subset of V.

5. Consider the linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^2$ defined by $T(x,y,z) = (x,y,0)$. Compute kernel(T) and nullity(T). Construct three linearly independent vectors in $V \setminus$ kernel(T).

4.3 Matrix representation of a linear transformation

Let V and W be finite-dimensional vector spaces. Let $\dim(V) = n$, and let $\mathscr{E} = \{e_1, \ldots, e_n\}$ be an ordered basis for V. If $V = \sum_{j=1}^{n} x_j e_j \in V$, then the coordinate vector of V with respect to the basis $\mathscr{E}$ is $[V]_{\mathscr{E}} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

Let $\dim(W) = m$, and let $\mathscr{F} = \{f_1, \ldots, f_m\}$ be an ordered basis for W. If $w = \sum_{i=1}^{m} y_i f_i \in W$, then the coordinate vector of w with respect to the basis $\mathscr{V}$ is $[w]_{\mathscr{F}} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$.

Let $T : V \to W$ be a linear transformation. The linearity of T implies that

$$T(V) = T\left(\sum_{j=1}^{n} x_j e_j\right) = \sum_{j=1}^{n} x_j T(e_j)$$

and so the linear transformation T is completely determined by the finite set of vectors $\{T(e_1), \ldots, T(e_n)\} \subseteq W$. For $j = 1, \ldots, n$, let

$$T(e_j) = \sum_{i=1}^{m} a_{i,j} f_i.$$

Then

$$\begin{aligned} T(V) &= \sum_{i=j}^{n} x_j T(e_j) \\ &= \sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{i,j} f_i \\ &= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{i,j} x_j\right) f_i \\ &= \sum_{i=1}^{m} y_i f_i \end{aligned}$$

where $y_i = \sum_{j=1}^{n} a_{ij} x_j$ for $i = 1, \ldots, m$. Therefore, $[T(V)]_{\mathscr{F}} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$.

Consider the $m \times n$ matrix

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n-1} & a_{2,n} \\ \vdots & & & \vdots & \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n-1} & a_{m,n} \end{pmatrix}.$$

We have the crucial identity

$$[T(V)]_{\mathscr{F}} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A[V]_{\mathscr{E}}.$$

The $m \times n$ matrix A is the matrix for the linear transformation T with respect to the ordered bases $\mathscr{E}$ and $\mathscr{F}$ for the vector spaces V and W, respectively. We write $[T]_{\mathscr{E}}^{\mathscr{F}} = A$.

Theorem 4.2. *Let U, V, and W be finite-dimensional vector spaces over the field $\mathbf{F}$ of dimensions p, n, and m, respectively. Let $\mathscr{D} = \{d_1, \ldots, d_p\}$, $\mathscr{E} = \{e_1, \ldots, e_n\}$, and $\mathscr{F} = \{f_1, \ldots, f_m\}$ be bases for U, V, and W, respectively. Let $T : V \to W$ and $S : U \to V$ be linear transformations. Let $A = [T]_{\mathscr{E}}^{\mathscr{F}}$ be the $m \times n$ matrix for T with respect to the bases $\mathscr{E}$ and $\mathscr{F}$, and let $B = [S]_{\mathscr{D}}^{\mathscr{E}}$ be the $p \times n$ matrix for S with respect to the bases $\mathscr{E}$ and $\mathscr{F}$. With respect to the bases $\mathscr{D}$ and $\mathscr{F}$, the linear transformation $TS : U \to W$ has the $m \times p$ matrix $C = [TS]_{\mathscr{D}}^{\mathscr{F}}$. Then $AB = C$ or, equivalently,*

$$[T]_{\mathscr{E}}^{\mathscr{F}} [S]_{\mathscr{D}}^{\mathscr{E}} = [TS]_{\mathscr{D}}^{\mathscr{F}}.$$

Proof. For $j = 1, \ldots, n$, let

$$T(e_j) = \sum_{i=1}^{m} a_{i,j} f_i.$$

These vector equations determine the $m \times n$ matrix $A = (a_{i,j}) = [T]_{\mathscr{E}}^{\mathscr{F}}$.

For $k = 1, \ldots, p$, let

$$S(d_k) = \sum_{j=1}^{n} b_{k,j} e_j$$

and let

$$TS(d_k) = \sum_{i=1}^{m} c_{k,i} f_i.$$

These vector equations determine the $n \times p$ matrix $B = (b_{k,j}) = [S]_{\mathscr{D}}^{\mathscr{E}}$ and the $m \times p$ matrix $C = (c_{k,i}) = [TS]_{\mathscr{D}}^{\mathscr{F}}$.

For $k = 1, \ldots, p$, we have

$$
\begin{aligned}
TS(d_k) &= T\left(\sum_{j=1}^{n} b_{j,k} e_j\right) \\
&= \sum_{j=1}^{n} b_{j,k} T\left(e_j\right) \\
&= \sum_{j=1}^{n} b_{j,k} \sum_{i=1}^{m} a_{i,j} f_i \\
&= \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} b_{j,k} f_i
\end{aligned}
$$

and so

$$\sum_{j=1}^{n} a_{i,j} b_{j,k} = c_{k,i}$$

for $i = 1, \ldots, m$ and $k = 1, \ldots, p$. Therefore, $AB = C$. This completes the proof.

Consider the vector space $V = \mathbf{R}^2$ with the ordered bases

$$\mathscr{F} = \left\{ f_1 = \begin{pmatrix} 2 \\ 3 \end{pmatrix}, f_2 = \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right\} \quad \text{and} \quad \mathscr{G} = \left\{ g_1 = \begin{pmatrix} -3 \\ 1 \end{pmatrix}, g_2 = \begin{pmatrix} -7 \\ 2 \end{pmatrix} \right\}.$$

The change of basis matrices

$$P = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} \qquad \text{and} \qquad Q = \begin{pmatrix} -3 & -7 \\ 1 & 2 \end{pmatrix}$$

satisfy

$$[V]_{\mathscr{E}} = P[V]_{\mathscr{F}} \qquad \text{and} \qquad [V]_{\mathscr{E}} = Q[V]_{\mathscr{G}}$$

for all $V \in \mathbf{R}^2$. We have

$$P^{-1} = \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} \qquad \text{and} \qquad Q^{-1} = \begin{pmatrix} 2 & 7 \\ -1 & -3 \end{pmatrix}$$

satisfy

$$[V]_{\mathscr{F}} = P^{-1}[V]_{\mathscr{E}} \qquad \text{and} \qquad [V]_{\mathscr{G}} = Q^{-1}[V]_{\mathscr{E}}$$

for all $V \in \mathbf{R}^2$.

Let $T : V \to V$ be the linear transformation defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3x + 5y \\ 5x + 8y \end{pmatrix}.$$

The matrix for T with respect to the standard basis $\mathscr{E}$ is

$$[T]_{\mathscr{E}} = \begin{pmatrix} 3 & 5 \\ 5 & 8 \end{pmatrix}.$$

To compute the matrix $[T]_{\mathscr{F}}$, we solve the systems of equations

$$\begin{cases} 2x+3y=21 \\ 3x+4y=34 \end{cases} \quad \text{and} \quad \begin{cases} 2x+3y=29 \\ 3x+4y=47 \end{cases}$$

and obtain

$$T(f_1) = T\begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 21 \\ 34 \end{pmatrix} = 18\begin{pmatrix} 2 \\ 3 \end{pmatrix} - 5\begin{pmatrix} 3 \\ 4 \end{pmatrix} = 18f_1 - 5f_2$$
$$T(f_2) = T\begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 29 \\ 47 \end{pmatrix} = 25\begin{pmatrix} 2 \\ 3 \end{pmatrix} - 7\begin{pmatrix} 3 \\ 4 \end{pmatrix} = 25f_1 - 7f_2.$$

The matrix of T with respect to the ordered basis $\mathscr{F}$ is

$$[T]_{\mathscr{F}} = \begin{pmatrix} 18 & 25 \\ -5 & -7 \end{pmatrix}$$

and so

$$[T(V)]_{\mathscr{F}} = [T]_{\mathscr{F}}[V]_{\mathscr{F}}$$

for all $V \in \mathbf{R}^2$. Moreover,

$$P[T]_{\mathscr{F}}P^{-1}[V]_{\mathscr{E}} = P[T]_{\mathscr{F}}[V]_{\mathscr{F}} = P[T(V)]_{\mathscr{F}} = [T(V)]_{\mathscr{E}} = [T]_{\mathscr{E}}[V]_{\mathscr{E}}$$

and so

$$P[T]_{\mathscr{F}}P^{-1} = [T]_{\mathscr{E}}.$$

Check:

$$P[T]_{\mathscr{F}}P^{-1} = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 18 & 25 \\ -5 & -7 \end{pmatrix}\begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ 5 & 8 \end{pmatrix} = [T]_{\mathscr{E}}.$$

Similarly,

$$T(g_1) = T\begin{pmatrix} -3 \\ 1 \end{pmatrix} = \begin{pmatrix} -4 \\ -7 \end{pmatrix} = -57g_1 + 25g_2$$
$$T(g_2) = T\begin{pmatrix} -7 \\ 2 \end{pmatrix} = \begin{pmatrix} -11 \\ -19 \end{pmatrix} = -155g_1 + 68g_2.$$

The matrix of T with respect to the ordered basis $\mathscr{G}$ is

$$[T]_{\mathscr{G}} = \begin{pmatrix} -57 & -155 \\ 25 & 68 \end{pmatrix}$$

and so

$$[T(V)]_{\mathscr{G}} = [T]_{\mathscr{G}}[V]_{\mathscr{G}}$$

for all $V \in \mathbf{R}^2$.

The change of basis identity is

$$\begin{aligned} Q[T]_{\mathscr{G}}P &= \begin{pmatrix} 15 & 34 \\ -11 & -25 \end{pmatrix} \begin{pmatrix} -57 & -155 \\ 25 & 68 \end{pmatrix} \begin{pmatrix} 25 & 34 \\ -11 & -15 \end{pmatrix} \\ &= \begin{pmatrix} 18 & 25 \\ -5 & -7 \end{pmatrix} \\ &= [T]_{\mathscr{G}}. \end{aligned}$$

Exercises

1. Define the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ by $T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5x - y \\ 3x + 2y \end{pmatrix}$.

   a. Compute the matrix of T with respect to the basis $\mathscr{E}^{(2)} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$.
   b. Compute the matrix of T with respect to the basis $\mathscr{B}_1 = \left\{ \begin{pmatrix} 11 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 7 \end{pmatrix} \right\}$.
   c. Compute the matrix of T with respect to the basis $\mathscr{B}_2 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\}$.

2. Define the linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^2$ by $T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 5x - y + z \\ 3x + 2y - z \end{pmatrix}$.

   a. Compute the matrix of T with respect to the bases
   $\mathscr{E}^{(3)} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$ and $\mathscr{E}^{(2)} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$.
   b. Compute the matrix of T with respect to the bases
   $\mathscr{B}^{(3)} = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}$ and $\mathscr{B}^{(2)} = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$.

3. a. In the vector space $\mathbf{R}^2$, let

   $$\mathscr{F} = \left\{ \mathbf{f}_1 = \begin{pmatrix} 8 \\ -3 \end{pmatrix}, \mathbf{f}_2 = \begin{pmatrix} -5 \\ 2 \end{pmatrix} \right\}.$$

   For every vector $\mathbf{v} = \binom{a}{b} \in \mathbf{R}^2$, solve the vector equation

   $$x\mathbf{f}_1 + y\mathbf{f}_2 = \mathbf{v}.$$

   Prove that $\mathscr{F}$ is a basis for $\mathbf{R}^2$.

   b. Let

   $$\mathscr{E} = \left\{ \mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

   be the standard basis for $\mathbf{R}^2$.

i. Compute the change of basis matrix P such that

$$P[v]_{\mathscr{F}} = [v]_{\mathscr{E}}.$$

ii. Compute $[\mathbf{e}_1]_{\mathscr{F}}$ and $[\mathbf{e}_2]_{\mathscr{F}}$.

iii. Compute the change of basis matrix Q such that

$$Q[v]_{\mathscr{E}} = [v]_{\mathscr{F}}.$$

iv. Compute the product matrices PQ and QP to see directly that $Q = P^{-1}$.

c. Consider the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 7x - y \\ 3x + 4y \end{pmatrix}.$$

i. Compute the matrix $[T]_{\mathscr{E}}$ of T with respect to the basis $\mathscr{E}$.

ii. Compute $[T(\mathbf{f}_1)]_{\mathscr{F}}$ and $[T(\mathbf{f}_2)]_{\mathscr{F}}$.

iii. Compute the matrix $[T]_{\mathscr{F}}$ of T with respect to the basis $\mathscr{F}$.

iv. Prove that

$$[T]_{\mathscr{F}} = P^{-1}[T]_{\mathscr{E}}P.$$

Answer:

$$P = \begin{pmatrix} 8 & -5 \\ -3 & 2 \end{pmatrix}$$

$$Q = \begin{pmatrix} 2 & 5 \\ 3 & 8 \end{pmatrix}$$

$$[T]_{\mathscr{E}} = \begin{pmatrix} 7 & 3 \\ -1 & 4 \end{pmatrix}$$

$$[T]_{\mathscr{F}} = \begin{pmatrix} 178 & -109 \\ 273 & -167 \end{pmatrix}$$

4. a. Let

$$A = \begin{pmatrix} 1 & 0 & 3 \\ -2 & 5 & -1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 4 & 1 \\ 0 & -5 \\ -1 & 2 \end{pmatrix}.$$

Compute $\det(AB)$.

b. Prove that if A is a 3×2 matrix and B is a 2×3 matrix, then $\det(AB) = 0$.

c. Let $n < m$. Prove that if A is a $n \times m$ matrix and B is a $m \times n$ matrix, then $\det(AB) = 0$,

4.4 Rotations and reflections in $\mathbf{R}^2$

The vector space $\mathbf{R}^2$ is the Euclidean plane. The *standard basis* for $\mathbf{R}^2$ is

$$\mathscr{E} = \{\mathbf{e}_1, \mathbf{e}_2\}$$

where

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

If $T : \mathbf{R}^2 \to \mathbf{R}^2$ is a linear operator, we denote the matrix for T with respect to the standard basis $\mathscr{E}$ by $[T]$ instead of $[T]_{\mathscr{E}}$.

We measure angles in the plane by radians: 2π radians = 360 degrees. The direction of positive rotation in the plane $\mathbf{R}^2$ is counterclockwise around the origin. The *polar coordinates* of the vector $\mathbf{v} = \begin{pmatrix} x \\ y \end{pmatrix}$ are r and θ, where $r = \sqrt{x^2 + y^2}$ is the distance from $\mathbf{v}$ to the origin and θ is the angle between the positive x-axis and the ray from the origin to $\mathbf{v}$. We have $x = r\cos\theta$ and $y = r\sin\theta$.

Recall the addition formulas for the cosine and sine:

$$\cos(\alpha + \theta) = \cos\alpha\cos\theta - \sin\alpha\sin\theta$$

and

$$\sin(\alpha + \theta) = \cos\alpha\sin\theta + \sin\alpha\cos\theta.$$

For a fixed angle α, let $R_\alpha : \mathbf{R}^2 \to \mathbf{R}^2$ be the function that rotates a vector in the positive direction around the origin by α radians.

Consider the vector $\mathbf{v} = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2$, and let

$$R_\alpha(\mathbf{v}) = R_\alpha \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Rotation of the vector $\mathbf{v}$ by α radians in the positive direction around the origin does not change the distance r from the vector to the origin, but does increase by α the angle with respect to the positive x-axis. Thus, if the polar coordinates of $\mathbf{v}$ are r and θ, then the polar coordinates of $R_\alpha(\mathbf{v})$ are r and $\alpha + \theta$. It follows that

$$\begin{aligned} x' &= r\cos(\alpha + \theta) \\ &= r\cos\alpha\cos\theta - r\sin\alpha\sin\theta \\ &= x\cos\alpha - y\sin\alpha \end{aligned}$$

and

$$\begin{aligned} y' &= r\sin(\alpha + \theta) \\ &= r\cos\alpha\sin\theta + r\sin\alpha\cos\theta \\ &= x\sin\alpha + y\cos\alpha. \end{aligned}$$

EquiValently,

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

Thus, the function $R_\alpha : \mathbf{R}^2 \to \mathbf{R}^2$ that rotates every vector by the angle α is the linear operator with matrix

$$[R_\alpha] = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

Note that

$$\det([R_\alpha]) = \cos^2\alpha + \sin^2\alpha = 1$$

and

$$\begin{aligned}
[R_\alpha][R_\beta] &= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \\
&= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{pmatrix} \\
&= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} \\
&= [R_{\alpha+\beta}].
\end{aligned}$$

In a vector space V over the field $\mathbf{F}$, a *line* is a one-dimensional subspace, that is, a subspace of the form $\langle V_0 \rangle = \{tV_0 : t \in \mathbf{F}\}$, where V_0 is a nonzero vector in V.

In the Euclidean plane $\mathbf{R}^2$, if $V_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, then the line through V_0 is the one-dimensional subspace

$$\langle V_0 \rangle = \{tV_0 : t \in \mathbf{R}\} = \left\{ \begin{pmatrix} tx_0 \\ ty_0 \end{pmatrix} : t \in \mathbf{R} \right\}.$$

For eVer nonzero real number s, this is also the line through the nonzero vector $sV_0 = \begin{pmatrix} sx_0 \\ sy_0 \end{pmatrix}$. Thus, we can assume that $x_0 \geq 0$. If $x_0 > 0$, then this line makes an angle $\alpha = \arctan(y_0/x_0) \in (-\pi/2, \pi/2)$ with respect to the positive x-axis. If $x_0 = 0$, then $y_0 \neq 0$, and the line is the y-axis, which makes an angle $\pi/2$ with respect to the positive x-axis.

For every $\alpha \in \mathbf{R}$,

$$\begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} = - \begin{pmatrix} \cos(\alpha+\pi) \\ \sin(\alpha+\pi) \end{pmatrix}$$

and so the vectors $\begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$ and $\begin{pmatrix} \cos(\alpha+\pi) \\ \sin(\alpha+\pi) \end{pmatrix}$ generate the same line in $\mathbf{R}^2$. We denote by ℓ_α the line in $\mathbf{R}^2$ generated by $\begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$.

We define the *reflection* S_α through the line ℓ_α as follows: If V is a nonzero vector in $\mathbf{R}^2$ with polar coordinates (r, θ), then the angle between V and ℓ_α is $\theta - \alpha$, and the reflection of V through the line ℓ_α is the vector with polar coordinates (r, θ'), where

$$\theta' = \alpha - (\theta - \alpha) = 2\alpha - \theta.$$

Thus, if $V = \begin{pmatrix} x \\ y \end{pmatrix}$, then $S_\alpha(V) = \begin{pmatrix} x' \\ y' \end{pmatrix}$, where

$$x' = r\cos(2\alpha - \theta) = r(\cos 2\alpha \cos\theta + \sin 2\alpha \sin\theta) = x\cos 2\alpha + y\sin 2\alpha$$

and

$$y' = r\sin(2\alpha - \theta) = r(\sin 2\alpha \cos\theta - \cos 2\alpha \sin\theta) = x\sin 2\alpha - y\cos 2\alpha.$$

We define $S_\alpha \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Thus, the function $S_\alpha : \mathbf{R}^2 \to \mathbf{R}^2$ that reflects every vector through the line ℓ_α is a linear transformation with matrix

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

Note that $[S_{\alpha+\pi}] = [S_\alpha]$ and

$$\det([S_\alpha]) = -\cos^2 2\alpha - \sin^2 2\alpha = -1.$$

Lemma 4.8. *Let ℓ_α be the line in $\mathbf{R}^2$ that makes an angle α with respect to the positive x-axis, and let S_{ℓ_α} be the reflection through ℓ_α. Let I_2 be the identity function on $\mathbf{R}^2$. Then $S_\alpha^2 = I_2$, and $S_\alpha(V) = V$ if and only if $V \in \ell_\alpha$.*

Proof. The matrix identity

$$\begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

implies that

$$S_\alpha^2 = I_2.$$

If V is a vector in $\mathbf{R}^2$ with polar coordinates r and θ, then $S_\alpha(V)$ is the vector in $\mathbf{R}^2$ with polar coordinates r and $2\alpha - \theta$. If $S_\alpha(V) = V$, then $2\alpha - \theta = \theta + 2\pi n$ for some integer n. EquiValently, $\theta = \alpha - \pi n$ and so V lies on the line ℓ_α. This completes the proof.

Here are three examples. If $\alpha = 0$, then S_0 is reflection through the x-axis, and

$$S_0 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -y \end{pmatrix}.$$

If $\alpha = \pi/2$, then $S_{\pi/2}$ is reflection through the y-axis, and

$$S_{\pi/2} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -x \\ y \end{pmatrix}.$$

If $\alpha = \pi/4$, then $S_{\pi/4}$ is reflection through the line $x = y$, and

$$S_{\pi/4}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}.$$

Theorem 4.3. *In the vector space* $\mathbf{R}^2$*,*

(i) The product of two rotations is a rotation.
(ii) The product of two reflections is a rotation.
(iii) The product of a rotation and a reflection is a reflection.

Proof. Let $\alpha, \beta \in \mathbf{R}$. The product of the matrices of the rotations R_α and R_β is

$$\begin{aligned}
[R_\alpha][R_\beta] &= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \\
&= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\sin\alpha\cos\beta - \cos\alpha\sin\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{pmatrix} \\
&= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} \\
&= [R_{\alpha+\beta}]
\end{aligned}$$

and so $R_\alpha R_\beta = R_{\alpha+\beta}$. This proves (i).

The product of the matrices of the reflections S_α and S_β is

$$\begin{aligned}
[S_\alpha][S_\beta] &= \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}\begin{pmatrix} \cos 2\beta & \sin 2\beta \\ \sin 2\beta & -\cos 2\beta \end{pmatrix} \\
&= \begin{pmatrix} \cos 2\alpha\cos 2\beta + \sin 2\alpha\sin 2\beta & -\sin 2\alpha\cos 2\beta + \cos 2\alpha\sin 2\beta \\ \sin 2\alpha\cos 2\beta - \cos 2\alpha\sin 2\beta & \cos 2\alpha\cos 2\beta + \sin 2\alpha\sin 2\beta \end{pmatrix} \\
&= \begin{pmatrix} \cos 2(\alpha-\beta) & -\sin 2(\alpha-\beta) \\ \sin 2(\alpha-\beta) & \cos 2(\alpha-\beta) \end{pmatrix} \\
&= [R_{2(\alpha-\beta)}]
\end{aligned}$$

and so $S_\alpha S_\beta = R_{2(\alpha-\beta)}$. This proves (ii).

Similarly,

$$\begin{aligned}
[S_\alpha][R_\beta] &= \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}\begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \\
&= \begin{pmatrix} \cos 2\alpha\cos\beta - \sin 2\alpha\sin\beta & \sin 2\alpha\cos\beta - \cos 2\alpha\sin\beta \\ \sin 2\alpha\cos\beta - \cos 2\alpha\sin\beta & -\cos 2\alpha\cos\beta - \sin 2\alpha\sin\beta \end{pmatrix} \\
&= \begin{pmatrix} \cos(2\alpha-\beta) & \sin(2\alpha-\beta) \\ \sin(2\alpha-\beta) & -\cos(2\alpha-\beta) \end{pmatrix} \\
&= \begin{pmatrix} \cos 2(\alpha-\beta/2) & \sin 2(\alpha-\beta/2) \\ \sin 2(\alpha-\beta/2) & -\cos 2(\alpha-\beta/2) \end{pmatrix} \\
&= [S_{\alpha-\beta/2}]
\end{aligned}$$

and

$$
\begin{aligned}
[R_\beta][S_\alpha] &= \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix} \\
&= \begin{pmatrix} \cos 2\alpha\cos\beta - \sin 2\alpha \sin\beta & \sin 2\alpha\cos\beta + \cos 2\alpha\sin\beta \\ \sin 2\alpha\cos\beta + \cos 2\alpha\sin\beta & -\cos 2\alpha\cos\beta + \sin 2\alpha\sin\beta \end{pmatrix} \\
&= \begin{pmatrix} \cos(2\alpha+\beta) & \sin(2\alpha+\beta) \\ \sin(2\alpha+\beta) & -\cos(2\alpha+\beta) \end{pmatrix} \\
&= \begin{pmatrix} \cos 2(\alpha+\beta/2) & \sin 2(\alpha+\beta/2) \\ \sin 2(\alpha+\beta/2) & -\cos 2(\alpha+\beta/2) \end{pmatrix} \\
&= [S_{\alpha+\beta/2}]
\end{aligned}
$$

This proves (iii).

Let $V_0, w_0 \in \mathbf{R}^2$, where $V_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ and $w_0 = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$. We have the affine line

$$
\begin{aligned}
\ell = \{tV_0 + w_0 : t \in \mathbf{R}\} &= \left\{ \begin{pmatrix} tx_0 + a_0 \\ ty_0 + b_0 \end{pmatrix} : t \in \mathbf{R} \right\} \\
&= \ell_\alpha + w_0
\end{aligned}
$$

where $\alpha = \arctan(y_0/x_0)$ and ℓ_α is the line generated by V_0.

For example, the vectors $V_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $w_0 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$ generate the affine line

$$
\ell = \langle V_0 \rangle + w_0 = \left\{ \begin{pmatrix} t \\ t+2 \end{pmatrix} : t \in \mathbf{R} \right\} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : y = x + 2 \right\}.
$$

In vector form, the line $y = mx + b$ is

$$
\left\{ \begin{pmatrix} x \\ y \end{pmatrix} : y = mx + b \right\} = \left\{ \begin{pmatrix} x \\ mx+b \end{pmatrix} : x \in \mathbf{R} \right\} = \left\{ x \begin{pmatrix} 1 \\ m \end{pmatrix} + \begin{pmatrix} 0 \\ b \end{pmatrix} : x \in \mathbf{R} \right\}
$$

We define the reflection S_ℓ of a vector $V \in \mathbf{R}^2$ through the affine line $\ell = \{tV_0 + w_0 : t \in \mathbf{R}\}$ as follows: Translate V by $-w_0$, reflect through the line $\langle V_0 \rangle$, and translate back by w_0. EquiValently,

$$
V \mapsto V - w_0 \mapsto S_\alpha(V - w_0) \mapsto S_\alpha(V - w_0) + w_0 = S_\alpha(V) + w_0 - S_\alpha(w_0)
$$

and so

$$
S_\ell(V) = S_\alpha(V) + w_0 - S_\alpha(w_0).
$$

Lemma 4.9. *Let ℓ be an affine line in $\mathbf{R}^2$, and let S_ℓ be the reflection through ℓ. Then $S_\ell^2 = I_2$, and $S_\ell(V) = V$ if and only if $V \in \ell$.*

Proof. We apply Lemma 4.8. Because $S_\alpha^2 = I_2$, it follows that

$$
\begin{aligned}
S_\ell^2(V) &= S_\ell\left(S_\alpha(V) + w_0 - S_\alpha(w_0)\right) \\
&= S_\alpha\left(S_\alpha(V) + w_0 - S_\alpha(w_0)\right) + w_0 - S_\alpha(w_0) \\
&= S_\alpha^2(V) + S_\alpha(w_0) - S_\alpha^2(w_0) + w_0 - S_\alpha(w_0) \\
&= V + S_\alpha(w_0) - w_0 + w_0 - S_\alpha(w_0) \\
&= V
\end{aligned}
$$

and so $S_\ell^2 = I_2$.

We have

$$S_\ell(V) = S_\alpha(V) + w_0 - S_\alpha(w_0) = V$$

if and only if

$$S_\alpha(V - w_0) = V - w_0$$

if and only if $V - w_0 \in \ell_\alpha$ if and only if $V \in \ell_\alpha + w_0 = \ell$. This completes the proof.

For example, let $V_0 = \begin{pmatrix}1\\1\end{pmatrix}$ and $w_0 = \begin{pmatrix}0\\2\end{pmatrix}$. The line generated by V_0 is $\ell_{\pi/4}$. Reflecting the vector $V = \begin{pmatrix}x\\y\end{pmatrix}$ through the affine line $\ell = \langle V_0 \rangle + w_0$, we obtain

$$
\begin{aligned}
\begin{pmatrix}x\\y\end{pmatrix} &\mapsto \begin{pmatrix}x\\y\end{pmatrix} - \begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}x\\y-2\end{pmatrix} \\
&\mapsto S_{\pi/4}\begin{pmatrix}x\\y-2\end{pmatrix} = \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}x\\y-2\end{pmatrix} = \begin{pmatrix}y-2\\x\end{pmatrix} \\
&\mapsto \begin{pmatrix}y-2\\x\end{pmatrix} + \begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}y-2\\x+2\end{pmatrix} = S_\ell\begin{pmatrix}x\\y\end{pmatrix}.
\end{aligned}
$$

Thus,

$$S_\ell\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}-1\\3\end{pmatrix}, \quad S_\ell\begin{pmatrix}-5\\6\end{pmatrix} = \begin{pmatrix}4\\-3\end{pmatrix}, \quad \text{and} \quad S_\ell\begin{pmatrix}-4\\7\end{pmatrix} = \begin{pmatrix}5\\-2\end{pmatrix}.$$

Because

$$\begin{pmatrix}-4\\7\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix} + \begin{pmatrix}-5\\6\end{pmatrix}$$

and

$$S_\ell\begin{pmatrix}-4\\7\end{pmatrix} = \begin{pmatrix}5\\-2\end{pmatrix} \neq \begin{pmatrix}-1\\3\end{pmatrix} + \begin{pmatrix}4\\-3\end{pmatrix} = S_\ell\begin{pmatrix}1\\1\end{pmatrix} + S_\ell\begin{pmatrix}-5\\6\end{pmatrix}$$

it follows that the reflection S_ℓ is not a linear transformation.

In Chapter **??**, we shall use the inner product on a real vector space to giVe another description of reflections.

Exercises

1. a. In the vector space $\mathbf{R}^2$, compute the matrix (with respect to the standard basis) of the linear transformation that rotates a vector by $\pi/6$ radians.
   b. In the vector space $\mathbf{R}^2$, compute the matrix (with respect to the standard basis) of the linear transformation that rotates a vector by $\pi/2$ radians.
   c. In the vector space $\mathbf{R}^2$, compute the matrix (with respect to the standard basis) of the linear transformation that rotates a vector by π radians.
2. a. In the vector space $\mathbf{R}^2$, compute the matrix (with respect to the standard basis) of the linear transformation that reflects a vector through the line that makes an angle $\pi/6$ with the positive x-axis.
   b. In the vector space $\mathbf{R}^2$, compute the matrix (with respect to the standard basis) of the linear transformation that reflects a vector through the line that makes an angle $-\pi/3$ with the positive x-axis.
   c. In the vector space $\mathbf{R}^2$, compute the matrix (with respect to the standard basis) of the linear transformation that reflects a vector through the line $y = -x$.
3. Prove that composition of rotations is commutative, that is, $R_\alpha R_\beta = R_\beta R_\alpha$ for all $\alpha, \beta \in \mathbf{R}$.
4. Compute $S_0 S_{\pi/4} \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ and $S_{\pi/4} S_0 \begin{pmatrix} 2 \\ 1 \end{pmatrix}$. Prove that composition of reflections is not commutative.
5. Prove that every line in $\mathbf{R}^2$ can be represented uniquely in the form ℓ_α, where $\pi/2 < \alpha \leq \pi/2$.
6. Let ℓ_α be the line through the origin in $\mathbf{R}^2$ that makes an angle α with respect to the positive x-axis. Prove that $\ell_\alpha = \ell_\beta$ if and only if $\beta - \alpha = n\pi$ for some integer n.
7. Prove that reflection through an affine line ℓ in $\mathbf{R}^2$ is a linear transformation if and only if the affine line is a line through the origin.
8. a. Prove that the area of the parallelogram generated by the vectors $\begin{pmatrix} A \\ 0 \end{pmatrix}$ and $\begin{pmatrix} C \\ D \end{pmatrix}$ is $|AD|$.
   b. Let $\mathbf{v} = \begin{pmatrix} a \\ b \end{pmatrix}$ be a nonzero vector in $\mathbf{R}^2$, and let $A = \sqrt{a^2 + b^2}$. Let $\alpha = \arctan b/a$, where $\alpha = \pi/2$ if $a = 0$ and $b > 0$, and $\alpha = -\pi/2$ if $a = 0$ and $b < 0$. Prove that the vector $R_{-\alpha}(\mathbf{v}) = \begin{pmatrix} A \\ 0 \end{pmatrix}$.

   Solution:
$$R_{-\alpha} = \begin{pmatrix} a/A & b/A \\ -b/A & a/A \end{pmatrix}$$
   and
$$R_{-\alpha}(\mathbf{v}) = R_{-\alpha} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a/A & b/A \\ -b/A & a/A \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} A \\ 0 \end{pmatrix}.$$

c. Let $\mathbf{w} = \begin{pmatrix} c \\ d \end{pmatrix}$ be a nonzero vector in $\mathbf{R}^2$, and let $R_{-\alpha}(\mathbf{w}) = \begin{pmatrix} C \\ D \end{pmatrix}$. Compute D.

Solution:

$$\begin{aligned} R_{-\alpha}(\mathbf{w}) = R_{-\alpha}\begin{pmatrix} c \\ d \end{pmatrix} &= \begin{pmatrix} a/A & b/A \\ -b/A & a/A \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix} \\ &= \begin{pmatrix} (ac+bd)/A \\ (ad-bc)/A \end{pmatrix}. \end{aligned}$$

d. Prove that the area of the parallelogram with vertices $\mathbf{0}, \mathbf{v}, \mathbf{w}$, and $\mathbf{v}+\mathbf{w}$ is $|AD| = |ad - bc|$.

4.5 Eigenvalues and eigenvectors

Let V be a vector space over the field $\mathbf{F}$, and let $T : V \to V$ be a linear operator. A scalar $\lambda \in \mathbf{F}$ is an *eigenValue* of T if there exists a nonzero vector $\mathbf{v} \in V$ such that $T(\mathbf{v}) = \lambda \mathbf{v}$. The vector $\mathbf{v}$ is called an *eigenvector* of T associated with the eigenValue λ. The *spectrum* of the linear operator T, denoted $\mathrm{Spec}(T)$, is the set of eigenValues of T, that is,

$$\mathrm{Spec}(T) = \{\lambda \in \mathbf{F} : T(\mathbf{v}) = \lambda \mathbf{v} \text{ for some nonzero vector } \mathbf{v} \in V\}.$$

A *fixed point* of an operator T is a vector $\mathbf{v}$ such that $T(\mathbf{v}) = \mathbf{v}$. An operator has a nonzero fixed point if and only if $1 \in \mathrm{Spec}(T)$.

Lemma 4.10. *Let $T : V \to V$ be a linear operator. Then kernel$(T) \neq \{\mathbf{0}\}$ if and only if 0 is an eigenValue of T.*

Proof. There exists a nonzero vector $\mathbf{v} \in \mathrm{kernel}(T)$ if and only if $\mathbf{v} \neq 0$ and $T(\mathbf{v}) = 0$ if and only if $\mathbf{v} \neq 0$ and $T(\mathbf{v}) = 0 \cdot \mathbf{v}$ if and only if 0 is an eigenValue of the linear operator T.

Lemma 4.11. *Let V be a vector space over the field $\mathbf{F}$, and let $T : V \to V$ be a linear operator. For every scalar $\lambda \in \mathbf{F}$,*

$$\{\mathbf{v} \in V : T(\mathbf{v}) = \lambda \mathbf{v}\}$$

is a subspace of V.

Note that $E(\lambda) \neq \{0\}$ if and only if λ is an eigenValue of T. The subspace $E(\lambda)$ is called the *eigenspace* associated with the eigenValue λ.

Proof. If $\mathbf{v}_1, \mathbf{v}_2 \in E(\lambda)$ and $c \in \mathbf{F}$, then

$$T(\mathbf{v}_1 + c\mathbf{v}_2) = T(\mathbf{v}_1) + cT(\mathbf{v}_2) = \lambda \mathbf{v}_1 + c\lambda \mathbf{v}_2 = \lambda(\mathbf{v}_1 + c\mathbf{v}_2)$$

and so $\mathbf{v}_1 + c\mathbf{v}_2 \in E(\lambda)$. This proves that $E(\lambda)$ is a subspace.

Theorem 4.4. *Let V be a vector space over the field $\mathbf{F}$, let $\lambda \in \mathbf{F}$, and let $T : V \to V$ be a linear operator. Let I be the identity operator on V. The scalar $\lambda \in \mathbf{F}$ is an eigenValue of T if and only if kernel$(\lambda I - T) \neq \{0\}$.*

Proof. The scalar $\lambda \in \mathbf{F}$ is an eigenValue of T if and only if there exists a nonzero vector $\mathbf{v} \in V$ such that $T(\mathbf{v}) = \lambda \mathbf{v}$ if and only if there exists a nonzero vector $\mathbf{v} \in V$ such that $T(\mathbf{v}) = \lambda I(\mathbf{v})$ if and only if there exists a nonzero vector $\mathbf{v} \in V$ such that $(\lambda I - T)(\mathbf{v}) = 0$ if and only if there exists a nonzero vector $V \in \text{kernel}(\lambda I - T)$. This completes the proof.

Let V be a finite-dimensional vector space over the field $\mathbf{F}$. We shall prove that the kernel of a linear operator on V is nonzero if and only the determinant of the operator is 0. Consider the linear operator $T : V \to V$. It follows that the scalar $\lambda \in \mathbf{F}$ is an eigenValue of T if and only if $\det(\lambda I - T) = 0$. If V is an n-dimensional vector space, then $\det(\lambda I - T)$ is a polynomial in λ of degree n. Because a polynomial of degree n has at most n roots, it follows that a linear operator on an n-dimensional vector space has at most n distinct eigenValues.

Theorem 4.5. *Let V be a finite-dimensional vector space over the field $\mathbf{F}$, let $T : V \to V$ be a linear operator, and let*

$$Spec(T) = \{\lambda_1, \ldots, \lambda_k\}$$

be the set of distinct eigenValues of T. For $i = 1, \ldots, k$, let $V_i \in V$ be an eigenvector with eigenValue λ_i. Then the set $\{V_1, \ldots, V_k\}$ is linearly independent.

Proof. By induction on k. If $k = 1$, then the set $\{V_1\}$ consists of one nonzero vector, and is linearly independent.

Let $k = 2$, and let λ_1 and λ_2 be distinct eigenValues of T with eigenvectors V_1 and V_2, respectively. We have

$$T(V_1) = \lambda_1 V_1 \qquad \text{and} \qquad T(V_2) = \lambda_2 V_2.$$

Let c_1 and c_2 be scalars such that

$$0 = c_1 V_1 + c_2 V_2. \tag{4.3}$$

We must prove that $c_1 = c_2 = 0$. Applying the operator T to (4.3), we obtain

$$0 = T(0) = T(c_1 V_1 + c_2 V_2) = c_1 T(V_1) + c_2 T(V_2) = c_1 \lambda_1 V_1 + c_2 \lambda_2 V_2.$$

Multiplication of (4.3) by λ_2 giVes

$$0 = c_1 \lambda_2 V_1 + c_2 \lambda_2 V_2.$$

Subtraction yields

$$0 = c_1(\lambda_1 - \lambda_2) V_1.$$

Because V_1 is a nonzero vector and $\lambda_1 - \lambda_2$ is a nonzero scalar, it follows that $c_1 = 0$, and so $c_2V_2 = 0$. Because V_2 is a nonzero vector, it follows that $c_2 = 0$, and so the set of vectors $\{V_1, V_2\}$ is linearly independent.

4.6 The spectrum of linear operators on $\mathbf{R}^2$

We shall consider only linear operators $T : \mathbf{R}^2 \to \mathbf{R}^2$. In this case, we have $\lambda \in \mathrm{Spec}(T)$ if and only if there exists $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2$ such that $\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ and

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}. \tag{4.4}$$

We begin with some examples.

Consider the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x \\ 3y \end{pmatrix}.$$

Comparing this with (4.4), we have $\lambda \in \mathrm{Spec}(T)$ if and only if $\begin{pmatrix} 2x \\ 3y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}$ if and only if $\lambda x = 2x$ and $\lambda y = 3y$ for some $\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. If $x \neq 0$, then $\lambda = 2$ and $y = 0$. If $y \neq 0$, then $\lambda = 3$ and $x = 0$. Thus, $\mathrm{Spec}(T) = \{2, 3\}$, and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is an eigenvector associated with the eigenValue 2, and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is an eigenvector associated with the eigenValue 3.

Consider the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -y \\ x \end{pmatrix}.$$

Comparing this with (4.4), we have $\lambda \in \mathrm{Spec}(T)$ if and only if $\lambda x = -y$ and $\lambda y = x$ for some $\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. These equations imply that

$$x = \lambda y = \lambda(-\lambda x) = -\lambda^2 x$$

and so

$$(\lambda^2 + 1)x = 0.$$

Because $\lambda^2 + 1 \neq 0$ for all $\lambda \in \mathbf{R}$, it follows that $x = 0$ and $y = 0$. Thus, the operator T has no eigenValue, and $\mathrm{Spec}(T) = \emptyset$.

Consider the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3x+2y \\ x+4y \end{pmatrix}.$$

The real number λ is an eigenValue of T if and only if there exists a nonzero vector $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2$ such that

$$\begin{pmatrix} 3x+2y \\ x+4y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}.$$

This is equivalent to the existence of a nonzero solution of the homogeneous system of linear equations

$$\begin{cases} (\lambda-3)x - 2y = 0 \\ -x + (\lambda-4)y = 0 \end{cases} \tag{4.5}$$

and this happens if and only

$$\det \begin{pmatrix} \lambda-3 & -2 \\ -1 & \lambda-4 \end{pmatrix} = \lambda^2 - 7\lambda + 10 = (\lambda-2)(\lambda-5) = 0.$$

It follows that $\mathrm{Spec}(T) = \{2, 5\}$.

If $\lambda = 2$, then equations (4.5) reduce to

$$-x - 2y = 0$$

and so $x = -2y$. Thus, the vector $\begin{pmatrix} -2 \\ 1 \end{pmatrix}$ is an eigenvector with eigenValue 2.

If $\lambda = 5$, then equations (4.5) reduce to

$$2x - 2y = 0$$

and so $x = y$. It follows that the vector $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ is an eigenvector with eigenValue 5.

We check this directly as follows:

$$\begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} -2 \\ 1 \end{pmatrix} = \begin{pmatrix} -4 \\ 2 \end{pmatrix} = 2 \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ 5 \end{pmatrix} = 5 \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be the linear operator defined by the 2×2 matrix $[T] = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Thus,

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}, \tag{4.6}$$

The real number λ is an eigenValue of T if and only if there exists a nonzero vector $\begin{pmatrix} x \\ y \end{pmatrix}$ such that

$$\begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} = T\begin{pmatrix} x \\ y \end{pmatrix} = \lambda\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}$$

if and only if the system of homogeneous linear equations

$$\begin{aligned} (\lambda-a)x-by &= 0 \\ -cx+(\lambda-d)y &= 0 \end{aligned}$$

has a nonzero solution. This is equivalent to

$$\det\begin{pmatrix} \lambda-a & -b \\ -c & \lambda-d \end{pmatrix} = \lambda^2-(a+d)\lambda+(ad-bc) = 0.$$

If $b \neq 0$, then $\begin{pmatrix} b \\ \lambda-a \end{pmatrix}$ is an eigenvector with eigenValue λ. If $c \neq 0$, then $\begin{pmatrix} \lambda-d \\ c \end{pmatrix}$ is an eigenvector with eigenValue λ. If $b = c = 0$, then $\mathrm{Spec}(T) = \{a,d\}$ and the vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are eigenvectors with eigenValues a and d, respectively.

ObserVe that

$$\lambda I - T = \lambda\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda-a & -b \\ -c & \lambda-d \end{pmatrix}$$

and so $\lambda \in \mathrm{Spec}(T)$ if and only if $\det(\lambda I - T) = 0$.

We define the eigenValues and eigenvectors of a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{R})$ as the eigenValues and eigenvectors of the linear operator defined by (4.6).

Exercises

1. Consider the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 117x+80y \\ -168x-115y \end{pmatrix}.$$

   Compute the eigenValues of this operator, and an eigenvector for each eigenValue.
2. Consider the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 8x-6y \\ 5x-3y \end{pmatrix}.$$

Compute $\mathrm{Spec}(T)$, and construct an eigenvector for each eigenValue $\lambda \in \mathrm{Spec}(T)$.

3. Consider the eigenValues and eigenvectors of the matrix

$$\begin{pmatrix} 5 & 6 \\ 3 & -2 \end{pmatrix}.$$

4. Compute the eigenValues and eigenvectors for the following matrices:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

5. The function $R_\alpha : \mathbf{R}^2 \to \mathbf{R}^2$ that rotates every vector by the angle α is the linear operator with matrix

$$[R_\alpha] = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

Prove that the rotation R_α has an eigenValue if and only if $\alpha = n\pi$ for some $n \in \mathbf{Z}$, and that $\mathrm{Spec}(R_{n\pi}) = \{(-1)^n\}$. Compute an eigenvector for this eigenValue.

6. Let $-\pi/2 < \alpha \leq \pi/2$, and let ℓ_α be the line through the origin with slope $\tan\alpha$. EquiValently, ℓ_α is the one-dimensional subspace spanned by the vector $\begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$. The function $S_\alpha : \mathbf{R}^2 \to \mathbf{R}^2$ that reflects every vector through the line ℓ_α is the linear operator with matrix

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

Prove that $\mathrm{Spec}(S_\alpha) = \{1, -1\}$. Compute an eigenvector for each of these eigenValues.

Solutions

1. $\mathrm{Spec}(T) = \{-3, 5\}$. Eigenvector -3 has eigenValue $\begin{pmatrix} 2 \\ -3 \end{pmatrix}$. Eigenvector 5 has eigenValue $\begin{pmatrix} 5 \\ -7 \end{pmatrix}$.
2. $\mathrm{Spec}(T) = \{2, 3\}$. Eigenvector 2 has eigenValue $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Eigenvector 3 has eigenValue $\begin{pmatrix} 6 \\ 5 \end{pmatrix}$.
3. EigenValues 7 and -4, with eigenvectors $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} -2 \\ 3 \end{pmatrix}$, respectively.
4. Left to reader.
5. The real number λ is an eigenValue of R_α if and only if λ is a solution of the quadratic equation

$$\begin{aligned}\det(\lambda I - [R_\alpha]) &= \det\begin{pmatrix}\lambda - \cos\alpha & \sin\alpha \\ -\sin\alpha & \lambda - \cos\alpha\end{pmatrix}\\ &= \lambda^2 - 2\cos\alpha\lambda + 1\\ &= 0.\end{aligned}$$

By the quadratic formula,

$$\lambda = \cos\alpha \pm \sqrt{\cos^2\alpha - 1}$$

and λ is real if and only if $\cos\alpha = \pm 1$ if and only if $\alpha = n\pi$ for some $n \in \mathbf{Z}$. In this case, $\mathrm{Spec}(R_\alpha) = \{\cos n\pi\} = \{(-1)^n\}$.

6. The real number λ is an eigenValue of S_α if and only if λ is a solution of the quadratic equation

$$\begin{aligned}\det(\lambda I - S_\alpha) &= \det\begin{pmatrix}\lambda - \cos 2\alpha & -\sin 2\alpha \\ -\sin 2\alpha & \lambda + \cos 2\alpha\end{pmatrix}\\ &= \lambda^2 - 1\\ &= 0\end{aligned}$$

and so $\mathrm{Spec}(S_\alpha) = \{1, -1\}$. If $\alpha \neq 0, \pi/2$, then $\sin 2\alpha \neq 0$ and $\sin\alpha \neq 0$. An eigenvector with eigenValue 1 is

$$\begin{aligned}\begin{pmatrix}\sin 2\alpha \\ 1 - \cos 2\alpha\end{pmatrix} &= \begin{pmatrix}2\sin\alpha\cos\alpha \\ 1 - \cos^2\alpha + \sin^2\alpha\end{pmatrix} = \begin{pmatrix}2\sin\alpha\cos\alpha \\ 2\sin^2\alpha\end{pmatrix}\\ &= 2\sin\alpha\begin{pmatrix}\cos\alpha \\ \sin\alpha\end{pmatrix}.\end{aligned}$$

Thus, every nonzero vector on the line ℓ_α is an eigenvector with eigenValue 1 for reflection through ℓ_α.
An eigenvector with eigenValue -1 is

$$\begin{aligned}\begin{pmatrix}\sin 2\alpha \\ -1 - \cos 2\alpha\end{pmatrix} &= \begin{pmatrix}2\sin\alpha\cos\alpha \\ -1 - \cos^2\alpha + \sin^2\alpha\end{pmatrix}\\ &= \begin{pmatrix}2\sin\alpha\cos\alpha \\ -2\cos^2\alpha\end{pmatrix} = -2\cos\alpha\begin{pmatrix}-\sin\alpha \\ \cos\alpha\end{pmatrix}\\ &= -2\cos\alpha\begin{pmatrix}\cos(\alpha + \pi/2) \\ \sin(\alpha + \pi/2)\end{pmatrix}.\end{aligned}$$

Thus, every nonzero vector on the line perpendicular to ℓ_α is an eigenvector with eigenValue -1 for reflection through ℓ_α.
The case $\alpha \in \{0, \pi/2\}$ is left to the reader.

4.7 vector spaces of linear transformations

Let V and W be vector spaces, and let $\mathscr{L}(V,W)$ be the set of all linear transformations from V to W. If $T_1, T_2 \in \mathscr{L}(V,W)$ and $c \in \mathbf{F}$, we define the functions $T_1 + T_2$ and cT_1 as follows:

$$(T_1 + T_2)(V) = T_1(V) + T_2(V)$$

and

$$(cT_1)(V) = cT_1(V).$$

If $V, V' \in V$ and $a \in \mathbf{F}$, then

$$\begin{aligned}(T_1 + T_2)(V + V') &= T_1(V + V') + T_2(V + V') \\ &= T_1(V) + T_1(V') + T_2(V) + T_2(V') \\ &= T_1(V) + T_2(V) + T_1(V') + T_2(V') \\ &= (T_1 + T_2)(V) + (T_1 + T_2)(V')\end{aligned}$$

and

$$\begin{aligned}(T_1 + T_2)(aV) &= T_1(aV) + T_2(aV) \\ &= aT_1(V) + aT_2(V) \\ &= a(T_1(V) + T_2(V)) \\ &= a(T_1 + T_2)(V).\end{aligned}$$

Thus, $T_1 + T_2$ is a linear transformation, that is, $T_1 + T_2 \in \mathscr{L}(V,W)$.

Similarly,

$$\begin{aligned}(cT_1)(V + V') &= cT_1(V + V') \\ &= c(T_1(V) + T_1(V')) \\ &= cT_1(V) + cT_1(V') \\ &= (cT_1)(V) + (cT_1)(V')\end{aligned}$$

and

$$\begin{aligned}(cT_1)(aV) &= cT_1(aV) \\ &= caT_1(V) \\ &= acT_1(V) \\ &= a(cT_1)(V).\end{aligned}$$

Thus, cT_1 is a linear transformation, that is, $cT_1 \in \mathscr{L}(V,W)$.

Theorem 4.6. *If V and W are vector spaces over the field $\mathbf{F}$, then $\mathscr{L}(V,W)$ is a vector space over the field $\mathbf{F}$. If $\dim(V) = n$ and $\dim(W) = m$, then $\dim(\mathscr{L}(V,W)) = mn$.*

4.8 Linear functionals

Let V be a vector space over the field $\mathbf{F}$. A *linear functional* on V is a linear transformation from the vector space V to the one-dimensional vector space $\mathbf{F}$ $\varphi : V \to \mathbf{F}$. Thus, $\varphi(V) \in \mathbf{F}$ for all $V \in V$, and

$$\varphi(cV + c'V') = c\varphi(V) + c'\varphi(V')$$

for all $V, V' \in V$ and $c, c' \in \mathbf{F}$. If φ_1 and φ_2 are linear functionals and c_1 and c_2 are scalars, then we define the function $c_1\varphi_1 + c_2\varphi_2$ from V to $\mathbf{F}$ by

$$(c_1\varphi_1 + c_2\varphi_2)(V) = c_1\varphi_1(V) + c_2\varphi_2(V)$$

for all $V \in V$. It is straightforward to check that $c_1\varphi_1 + c_2\varphi_2$ is also a linear functional, and that the set V^* consisting of all linear functionals on V is also a vector space over $\mathbf{F}$. We call V^* the *dual space* of V.

Let V be an n-dimensional vector space over $\mathbf{F}$ with basis $\mathscr{B} = \{e_1, \ldots, e_n\}$, and let φ be a linear functional on V. Let $a_i = \varphi(e_i) \in \mathbf{F}$ for $i = 1, \ldots, n$. If $V = x_1e_1 + \cdots + x_ne_n \in V$, then

$$\begin{aligned}\varphi(V) &= \varphi\left(\sum_{i=1}^{n} x_ie_i\right)\\ &= \sum_{i=1}^{n} x_i\varphi(e_i)\\ &= \sum_{i=1}^{n} a_ix_i.\end{aligned}$$

Thus, with respect to a fixed basis $\mathscr{B}$ on the vector space, every linear functional can be represented as a homogeneous linear polynomial in n Variables, that is, as a linear form with coefficients in $\mathbf{F}$. For $\mathscr{V} \in V$, the coordinate vector $[\mathscr{V}]_{\mathscr{B}}$ is a column vector in $\mathbf{F}^n$. The matrix $[\varphi]_{\mathscr{B}}$ is the row vector $(a_1, a_2, \ldots, a_n)$. Thus,

$$[\varphi(\mathscr{V})]_{\mathscr{B}} = [\varphi]_{\mathscr{B}}[\mathscr{V}]_{\mathscr{B}} = (a_1, \ldots, a_n)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^{n} a_ix_i.$$

We denote by $(\mathbf{F}^n)^*$ the vector space of n-dimensional row vectors with coordinates in $\mathbf{F}$.

Theorem 4.7. *Let V be a finite-dimensional vector space, let $n = \dim_{\mathbf{F}}(V)$, and let $\mathscr{B} = \{e_1, \ldots, e_n\}$ be a basis for V. For $i = 1, \ldots, n$, define the linear functional $\varphi_i^* \in V^*$ as follows:*

$$\varphi_i^*(e_j) = \delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

The set $\mathscr{B}^* = \{\varphi_1^*, \ldots, \varphi_n^*\}$ is a basis for the dual space V^*.

The set of linear functionals $\mathscr{B}^* = \{\varphi_1^*, \ldots, \varphi_n^*\}$ is called the *dual basis* for V^* with respect to the basis $\mathscr{B} = \{e_1, \ldots, e_n\}$ of V.

Proof. Let $c_1, \ldots, c_n \in \mathbf{F}$. If $\varphi = c_1\varphi_1^* + \cdots + c_n\varphi_n^* = 0$, then

$$0 = \varphi(e_j) = \sum_{i=1}^{n} c_i \varphi_i^*(e_j) = \sum_{i=1}^{n} c_i \delta_{ij} = c_i$$

for all $i = 1, \ldots, n$, and so the linear functionals $\varphi_1^*, \ldots, \varphi_n^*$ are linearly independent.

Let $\psi \in V^*$. We define $\psi' \in V^*$ by

$$\psi' = \sum_{i=1}^{n} \psi(e_i)\varphi_i^*.$$

We have

$$\psi'(e_j) = \sum_{i=1}^{n} \psi(e_i)\varphi_i^*(e_j) = \psi(e_j).$$

Because the linear functionals ψ and ψ' agree on a basis for the vector space V, it follows that $\psi = \psi'$, and so the set $\mathscr{B}^* = \{\varphi_1^*, \ldots, \varphi_n^*\}$ spans V^*. This completes the proof.

Let V and W be finite-dimensional vector spaces with $\dim(V) = n$ and $\dim(W) = m$. Let $T : V \to W$ be a linear transformation. If $\psi \in W^*$, then the composite function $\psi \circ T$ is a linear functional from V to $\mathbf{F}$, that is, an element of V^*. Define the function $T^* : W^* \to V^*$ by $T^*(\psi) = \psi \circ T$. Thus, for all $V \in V$ we have

$$T^*(\psi)(V) = \psi(T(V)).$$

Theorem 4.8. *Let V and W be finite-dimensional vector spaces, and let $T : V \to W$ be a linear transformation. Define $T^* : W^* \to V^*$ by $T^*(\psi)(V) = \psi \circ T$. Let $\mathscr{B}$ and $\mathscr{C}$ be ordered bases for V and W, respectively, and let $\mathscr{B}^*$ and $\mathscr{C}^*$ be the associated dual bases for V^* and W^*. If A is the matrix of T with respect to $\mathscr{B}$ and $\mathscr{C}$, then the matrix of T^* with respect to the dual bases $\mathscr{B}^*$ and $\mathscr{C}^*$ is the transpose of A.*

Proof. Let $\dim(V) = n$ and $\dim(W) = m$, and let $\mathscr{B} = \{e_1, \ldots, e_n\}$ and $\mathscr{C} = \{f_1, \ldots, f_m\}$. Let $A = (a_{i,j})$, where

$$T(e_j) = \sum_{i=1}^{m} a_{i,j} f_i$$

for $j = 1, \ldots, n$. Consider the dual bases $\mathscr{B}^* = \{e_1^*, \ldots, e_n^*\}$ and $\mathscr{C}^* = \{f_1^*, \ldots, f_m^*\}$ defined by $e_i^*(e_j) = \delta_{i,j}$ for $i, j = 1, \ldots, n$ and $f_i^*(f_j) = \delta_{i,j}$ for $i, j = 1, \ldots, m$. The $m \times m$ matrix $B = \{b_{i,j}$ for T^* with respect to $\mathscr{C}^*$ and $\mathscr{B}^*$ is determined by the equations

$$T^*(f_j^*) = \sum_{k=1}^{n} b_{k,j} e_k^*$$

for $j = 1, \ldots, m$. Because

$$\sum_{k=1}^{n} b_{k,j} e_k^*(e_i) = b_{i,j}$$

and

$$T^*(f_j^*)(e_i) = f_j^*(T(e_i)) = f_j^*\left(\sum_{k=1}^{m} a_{k,i} f_k\right) = \sum_{k=1}^{m} a_{k,i} f_j^*(f_k) = a_{j,i}$$

it follows that

$$b_{i,j} = a_{j,i}$$

and so B is the transpose of the matrix A. This completes the proof.

Lemma 4.12. *Let $S : U \to V$ and $T : V \to W$ be linear transformation. The composite function $TS : U \to W$ satisfies*

$$(TS)^* = S^* T^*.$$

A linear operator T is *self-adjoint* or *symmetric* if $T = T^*$.

4.9 Deleted stuff

4.10 Eigenvectors and eigenValues in R^2

Let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be a linear operator.

The real number λ is an *eigenValue* of T if there exists a nonzero vector $w \in \mathbf{R}^2$ such that

$$T(w) = \lambda w. \tag{4.7}$$

A nonzero vector w that satisfies (4.7) is called an *eigenvector* with eigenValue λ.

Lemma 4.13. *For every real number λ,*

$$E_T(\lambda) = \{w \in \mathbf{R}^2 : T(w) = \lambda w\}$$

is a subspace of $\mathbf{R}^2$.

If T is a linear operator, then $\lambda I - T$ is a linear operator for all $\lambda \in \mathbf{R}$. If $[T] = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then

$$[\lambda I - T] = \begin{pmatrix} \lambda - a & -b \\ -c & \lambda - d \end{pmatrix}.$$

The vector equation $T(w) = \lambda w$ is equivalent to

$$(\lambda I - T)(w) = 0$$

and so λ is an eigenValue of T if and only

$$\text{kernel}(\lambda I - T) \neq \{0\}$$

if and only if

$$\det \begin{pmatrix} \lambda - a & -b \\ -c & \lambda - d \end{pmatrix} = (\lambda - a)(\lambda - d) - bc = 0$$

if and only if λ is a root of the quadratic equation

$$t^2 - (a+d)t + ad - bc = 0.$$

Example of linear transformation:

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x + by \\ 7x + y \end{pmatrix}.$$

Let $V, V' \in \mathbf{R}^2$ and $c \in \mathbf{R}$. If $V = \begin{pmatrix} x \\ y \end{pmatrix}$ and $V' = \begin{pmatrix} x' \\ y' \end{pmatrix}$, then $V + V' = \begin{pmatrix} x + x' \\ y + y' \end{pmatrix}$ and $cV = \begin{pmatrix} cx \\ cy \end{pmatrix}$. We have

$$
\begin{aligned}
T(V+V') = T\begin{pmatrix} x+x' \\ y+y' \end{pmatrix} &= \begin{pmatrix} 2(x+x')-3(y+y') \\ 7(x+x')+(y+y') \end{pmatrix} \\
&= \begin{pmatrix} (2x+by)+(2x'-3y') \\ (7x+y)+(7x'+y') \end{pmatrix} \\
&= \begin{pmatrix} 2x+by \\ 7x+y \end{pmatrix} + \begin{pmatrix} 2x'-3y' \\ 7x'+y' \end{pmatrix} \\
&= T\begin{pmatrix} x \\ y \end{pmatrix} + T\begin{pmatrix} x' \\ y' \end{pmatrix} \\
&= T(V)+T(V')
\end{aligned}
$$

and

$$
T(cV) = T\begin{pmatrix} cx \\ cy \end{pmatrix} = \begin{pmatrix} 2cx-3cy \\ 7cx+cy \end{pmatrix} = \begin{pmatrix} c(2x-3y) \\ c(7x+y) \end{pmatrix} = c\begin{pmatrix} 2x-3y \\ 7x+y \end{pmatrix} = cT(V).
$$

Thus, T is a linear transformation.

To add

1. One-to-one = injective = monomorphism.
   $f : V \to W$ is a monomorphism if and only if : GiVen $g_i : U_i \to V$ and $fg_i : U_i \to W$, we have
   $$fg_1 = fg_2 \text{ if and only } g_1 = g_2.$$
   $$
   \begin{tikzcd}
   U_1 \arrow[dr, "g_1"'] \arrow[drr, "fg_1"] & & \\
   & V \arrow[r, "f"] & W \\
   U_2 \arrow[ur, "g_2"] \arrow[urr, "fg_2"'] & &
   \end{tikzcd}
   $$
2. Onto = surjective = epimorphism.
   $f : U \to V$ is an epimorphism if and only if : GiVen $g_i : V \to W_i$ and $g_i f : U \to W_i$, we have
   $$f \text{ if and only } g_1 = g_2.$$

$$\begin{tikzcd}
& & W_1 \\
U \arrow[r, "f"] \arrow[urr, bend left, "g_1 f"] \arrow[drr, bend right, "g_2 f"'] & V \arrow[ur, "g_1"] \arrow[dr, "g_2"'] & \\
& & W_2
\end{tikzcd}$$

3. Categorical definitions of kernel and cokernel.
4. For $i = 1, \dots, r$, let V_i and W_i be vector spaces over the field $\mathbf{F}$, and let $T_i : V_i \to W_i$ be a linear transformation. Consider the direct sums

$$V = V_1 \oplus \cdots \oplus V_r$$

and

$$W = W_1 \oplus \cdots \oplus W_r.$$

We define the function $T : V \to W$ by

$$T(V_1, \dots, V_r) = (T(V_1), \dots, T(V_r)).$$

For $(V_1, \dots, V_r), (V_1', \dots, V_r') \in V$ and $c \in \mathbf{F}$, we have

$$\begin{aligned}
T((V_1, \dots, V_r) + c(V_1', \dots, V_r')) &= T\left((V_1 + cV_1', \dots, V_r + cV_r')\right) \\
&= \left(T_1(V_1 + cV_1'), \dots, T_r(V_r + cV_r')\right) \\
&= \left(T_1(V_1) + cT_1(V_1'), \dots, T_r(V_r) + cT_r(V_r')\right) \\
&= (T_1(V_1), \dots, T_r(V_r)) + c\left(T_1(V_1'), \dots, T_r(V_r')\right) \\
&= T(V_1, \dots, V_r) + cT(V_1', \dots, V_r')
\end{aligned}$$

and so T is a linear transformation.
5. Let V be a vector space over the field $\mathbf{F}$.
   a. Prove that $\mathrm{End}_{\mathbf{F}}(V)$ is a noncommutative ring.
   b. Let $\mathbf{F}[t]$ be the commutative ring of polynomials with coefficiets in $\mathbf{F}$. Let $T \in \mathrm{End}(V)$. Prove the function $\Phi : \mathbf{F}[t] \to \mathrm{End}_{\mathbf{F}}(V)$ defined by $\Phi(f(t)) = f(T)$ is a ring homomorphism.

to add

1. Reflection through an affine line, i.e. a line not going through the origin.
2. If $W \subseteq V$ and $\dim(W) = \dim(V) < \infty$, then $W = V$.
   Counterexample if $\dim(V) = \infty$: $V = \mathbf{F}[t]$ and $W = \mathbf{F}[t^2]$.
3. Let $\alpha_1 \in V^*$ and $w_1 \in W$. Define $T : V \to W$ by

$$T(V) = \alpha_1(V)w_1.$$

Prove that T is a linear transformation, i.e. $T \in \mathscr{L}(V,W)$.

4. Let $\dim(W) = n$ and let $\{w_1,\ldots,w_n\}$ be a basis for W. Prove that if $T \in \mathscr{L}(V,W)$, then there exist unique linear functionals $\alpha_1,\ldots,\alpha_n \in V^*$ such that

$$T(V) = \sum_{i=1}^{n} \alpha_i(V)w_i.$$

5. Let $\mathbf{F}[t]$ be the infinite-dimensional vector space of polynomials with coefficients in the field $\mathbf{F}$, and let $\mathbf{F}^{(n)}[t]$ be the finite-dimensional vector space of polynomials of degree less than n with coefficients in the field $\mathbf{F}$. Let $V = \mathbf{F}[t]$ or $\mathbf{F}^{(n)}[t]$. Let $D \in \mathscr{L}(V)$ be the differentiation operator on V, and let $J \in \mathscr{L}(V)$ be the integration operator. Prove that D is onto but not one-to-one, and that J is one-to-one but not onto.
6. Let $\mathbf{F}[t]$ be the infinite-dimensional vector space of polynomials with coefficients in the field $\mathbf{F}$, and let $\mathbf{F}^{(n)}[t]$ be the finite-dimensional vector space of polynomials of degree less than n with coefficients in the field $\mathbf{F}$. Note that $\dim\left(\mathbf{F}^{(n)}[t]\right) = n$. Let $V = \mathbf{F}[t]$ or $\mathbf{F}^{(n)}[t]$. Let $D \in \mathscr{L}(V)$ be the differentiation operator, and let $T \in \mathscr{L}(V)$ be multiplication by t. For every polynomial $p(t) \in V$ we have

$$DT(p(t)) = D(tp(t)) = p(t) + tp'(t)$$

and

$$TD(p(t)) = tp'(t)$$

and so

$$DT(p(t)) - TD(p(t)) = \big(p(t) + tp'(t)\big) - tp'(t) = p(t).$$

Thus,

$$DT - TD = I.$$

7. An operator $S \in \mathscr{L}(V)$ is a *zero diVisor* if S is nonzero and there exists a nonzero operator $T \in \mathscr{L}(V)$ such that $ST = TS = 0$. Define the nonzero linear operators $S,T \in \mathscr{L}(\mathbf{R}^2)$ with respect to the standard basis by

$$S\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ 0 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ y \end{pmatrix}.$$

Prove that $ST = TS = 0$.

8. Zero-diVisors in $\mathscr{L}(\mathbf{R}^2)$. Define the linear operators $S,T \in \mathscr{L}(\mathbf{R}^2)$ with respect to the standard basis by the nonzero matrices

$$S = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

Prove that $ST = TS = 0$.

9. Consider the linear operator $S \in \mathscr{L}(\mathbf{R}^3)$ whose matrix, with respect to the standard basis $\mathscr{E}$, is
$$A = [S]_{\mathscr{E}} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$
   a. Compute bases for kernel(S) and range(S).
   b. Compute the matrix of S with respect to this new basis for V.
10. Prove or disprove the statement: On a finite-dimensional vector space, every nonzero singular operator is a zero diVisor.
11. Let A be an $n \times n$ matrix, and let $i, j \in \{1, 2, \ldots, n\}$ with $i \neq j$. Obtain the matrix B from A by, first, interchanging rows i and j, and then interchanging columns i and j. Obtain the matrix C from A by, first, interchanging columns i and j, and then interchanging rows i and j. Prove that $B = C$.
12. An *idempotent* in $\mathscr{L}(V)$ is an operator E such that $E^2 = E$. An *involution* in $\mathscr{L}(V)$ is an operator U such that $U^2 = I$.
   a. Prove that if E is an idempotent, then $U = 2E - I$ is an involution.
   b. Prove that if U is an involution, then $E = (1/2)(U + I)$ is an idempotent.

Chapter 5
Eigenvalues and the spectral theorem

Exercises to add

1. Compute the determinants and the characteristic polynomials of the following matrices:

   a.
   $$\begin{pmatrix} 2 & 3 \\ 1 & 0 \end{pmatrix}$$

   b.
   $$\begin{pmatrix} 2 & 3 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

   c.
   $$\begin{pmatrix} 2 & 3 & 5 & -7 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

   d.
   $$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

   e.
   $$\begin{pmatrix} 2 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

2. Find the eigenvalues and the eigenvectors of the matrix

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}$$

3. Let T be a linear operator on the vector space V, and let W be a one-dimensional T-invariant subspace of V. Prove that every nonzero vector in W is an eigenvector.
4. Let V be the n-dimensional vector space consisting of all polynomials in $\mathbf{R}[t]$ of degree at most $n-1$, and let D be the differentiation operator on V.

   a. Compute the characteristic polynomial of the linear operator D. Prove that $\mathrm{Spec}(D) = \{0\}$ and that the eigenvalue 0 has algebraic multiplicity n.
   b. Prove that the eigenspace associated with the eigenvalue 0 is the one-dimensional subspace of constant polynomials, and so the eigenvalue 0 has geometric multiplicity 1.

5. **Theorem 5.1.** *The geometric multiplicity of an eigenvalue does not exceed the algebraic multiplicity of the eigenvalue.*

   Proof. Let T be a linear operator on the finite-dimensional vector space V, and let λ be an eigenvalue of T. Let $W(\lambda) = \{v \in V : T(w) = \lambda w\}$ be the eigenspace of λ, and let $k = \dim(W(\lambda))$ be the geometric multiplicity of λ. Let $\{w_1, \ldots, w_k\}$ be a basis for $W(\lambda)$, The subspace $W(\lambda)$ is T-invariant, and the characteristic polynomial of T restricted to W is $(t-\lambda)^k$.
   Choose vectors $\{w_{k+1}, \ldots, w_n\}$ such that $\mathscr{B} = \{w_1, \ldots, w_k, w_{k+1}, \ldots, w_n\}$ is a basis for V, and let $[T]_{\mathscr{B}} = A = (a_{i,j})$ be the matrix of T with respect to the basis $\mathscr{B}$. Then $a_{i,i} = \lambda$ and $a_{i,j} = 0$ for $i = 1, \ldots, k$ and $j \neq i$. Let $B = (b_{i,j})$ be the $(n-k) \times (n-k)$ matrix such that

   $$b_{i,j} = a_{k+i,k+j}$$

   for $i, j = 1, \ldots, n-k$. We can write

   $$\det(tI - B) = (t-\lambda)^{\ell} h(t)$$

   where $h(t) \in K[t]$ is a polynomial such that $h(\lambda) \neq 0$. The characteristic polynomial of A is

   $$\begin{aligned} \det(tI - A) &= (t-\lambda)^k \det(tI - B) \\ &= (t-\lambda)^k (t-\lambda)^{\ell} h(t) \\ &= (t-\lambda)^{k+\ell} h(t) \end{aligned}$$

   and so λ has algebraic multiplicity $k + \ell \geq k$. This completes the proof.

6. Let T be a linear operator on a finite-dimensional vector space V, and let $\mathrm{Spec}(T) = \{\lambda_1, \ldots, \lambda_s\}$ be the spectrum of T. Let m_i be the geometric multiplicity of λ_i for $i = 1, \ldots, s$. Prove that if $\sum_{i=1}^{s} m_i = \dim(V)$, then the geometric multiplicity of λ_i equals the algebraic multiplicity of λ_i for every eigenvalue λ_i.

7. Let $K_n[t]$ be the n-dimensional vector space of polynomials of degree at most $n-1$, and let $D : K_n[t] \to K_n[t]$ be the differentiation operator. Prove that $K_n[t]$ is not completely reducible with respect to T, that is, prove that there do not exist nonzero T-invariant subspaces W_1 and W_2 of $K_n[t]$ such that $K_n[t] = W_1 \oplus W_2$.
8. Let V be a finite-dimensional inner product space, let $T : V \to V$, and let $T^* : V \to V$ be the adjoint of T, that is,

$$(T(v_1), v_2) = (v_1, T^*(v_2)) \qquad \text{for all } v_1, v_2 \in V.$$

If W^* is a T^*-invariant subspace of V, then $(W^*)^{\perp}$ is a T-invariant subspace of V.

Proof. For all $w^* \in W^*$ we have $T^*(w^*) \in W^*$. If $w \in (W^*)^{\perp}$, then

$$(T(w), w^*) = (w, T^*(w^*)) = 0$$

and so $T(w) \in (W^*)^{\perp}$. Therefore, $(W^*)^{\perp}$ is T-invariant.

9. On an n-dimensional complex inner product space, every linear operator has an $(n-1)$-dimensional invariant subspace.

Proof. Let V be a finite-dimensional complex inner product space, and let $T : V \to V$ be a linear operator with adjoint T^*. Every linear operator on a complex vector space has an eigenvector. Let w^* be an eigenvector of T^*, and let W^* be the one-dimensional subspace spanned by $\{w^*\}$. Then $(W^*)^{\perp}$ is a T-invariant subspace of V, and

$$\dim (W^*)^{\perp} = \dim(V) - \dim (W^*) = n - 1.$$

10. Let $\lambda_1, \lambda_2 \in \mathbf{R}$, and let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be the linear operator defined by

$$T(x_1, x_2) = (\lambda_1 x_1, \lambda_2 x_2).$$

a. Prove that $\mathrm{Spec}(T) = \{\lambda_1, \lambda_2\}$.
b. Prove that if $\lambda_1 = \lambda_2$, then every one-dimensional subspace of $\mathbf{R}^2$ is T-invariant.
c. Prove that if $\lambda_1 \neq \lambda_2$, then the only one-dimensional T-invariant subspaces of $\mathbf{R}^2$ are $\{x_1, 0) : x_1 \in \mathbf{R}\}$ and $\{0, x_2) : x_2 \in \mathbf{R}\}$.

5.1 Simple proof of the existence of eigenvalues

LEMMA NOT NEEDED:

Lemma 5.1. *Let $k \geq 2$, and, for $i = 1, 2, \ldots, k-1, k$, let $T_i : V \to V$ be a linear operator on the vector space V. If T_i is invertible for all i, then the composite operator $T_k T_{k-1} \cdots T_2 T_1$ is invertible.*

Proof. Let T_i^{-1} be the inverse of T_i for $i = 1, 2, \ldots, k-1, k$. Then

$$\begin{aligned}\mathrm{id}_V &= (T_k T_{k-1} \cdots T_2 T_1)\left(T_1^{-1} T_2^{-1} \cdots T_{k-1}^{-1} T_k^{-1}\right) \\ &= \left(T_1^{-1} T_2^{-1} \cdots T_{k-1}^{-1} T_k^{-1}\right)(T_k T_{k-1} \cdots T_2 T_1)\end{aligned}$$

and so $T_k T_{k-1} \cdots T_2 T_1$ is invertible. This completes the proof.

Theorem 5.2. *Every linear operator on a finite-dimensional complex vector space has an eigenvalue.*

Proof. Let $n = \dim(V)$, and let $T : V \to V$ be a linear operator. For every nonzero vector $v \in V$, the sequence of $n+1$ vectors

$$(v, T(v), T^2(v), \ldots, T^n(v))$$

is linearly dependent, and so there exist complex numbers $a_0, a_1, \ldots, a_n$ not all 0 such that

$$a_0 v + a_1 T(v) + a_2 T^2(v) + \cdots + a_n T^n(v) = 0.$$

Let k be the largest integer such that $0 \leq k \leq n$ and $a_k \neq 0$. Then

$$a_0 v + a_1 T(v) + a_2 T^2(v) + \cdots + a_{k-1} T^{k-1}(v) + a_k T^k(v) = 0.$$

Dividing by a_k, we obtain

$$a_0' v + a_1' T(v) + a_2' T^2(v) + \cdots + a_{k-1}' T^{k-1}(v) + T^k(v) = 0$$

where $a_i' = a_i / a_k$ for $i = 0, 1, \ldots, k-1$. If $k = 0$, then $v = 0$, which contradicts the choice of v as a nonzero vector. Therefore, $1 \leq k \leq n$ and the polynomial

$$f(t) = a_0' + a_1' t + a_2' t^2 + \cdots + a_{k-1}' t^{k-1} + t^k$$

is nonconstant. By the Fundamental Theorem of Algebra, $f(t)$ is a product of linear factors, and so there is a sequence of not necessarily distinct complex numbers $\lambda_1, \ldots, \lambda_k$ such that

$$f(t) = (t - \lambda_k)(t - \lambda_{k-1}) \cdots (t - \lambda_1).$$

It follows that

$$\begin{aligned}f(T)(v) &= (T - \lambda_k I)(T - \lambda_{k-1} I) \cdots (T - \lambda_1 I)(v) \\ &= a_0' v + a_1' T(v) + a_2' T^2(v) + \cdots + a_{k-1}' T^{k-1}(v) + T^k(v) \\ &= 0.\end{aligned}$$

Let j be the smallest integer such that

$$(T - \lambda_j I)(T - \lambda_{j-1} I) \cdots (T - \lambda_1 I)(v) = 0$$

and let $w = v$ if $j = 0$ and

$$w = (T - \lambda_{j-1}I)\cdots(T - \lambda_1 I)(v)$$

if $j \geq 1$. It follows that $w \neq 0$ and $(T - \lambda_j I)(w) = 0$, that is,

$$T(w) = \lambda_j w.$$

Therefore, λ_j is an eigenvalue of T with eigenvector w. This completes the proof.

Exercises

1. Prove

5.2 Invariant subspaces

Let $T : V \to V$ be a linear operator. A subspace W of V is *invariant* with respect to T if $T(W) \subseteq W$, that is, if $w \in W$ implies that $T(w) \in W$. Equivalently, W is an invariant subspace of T if the restriction of T to W is a linear operator on W.

For example, let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be the linear operator defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix} \tag{5.1}$$

and let

$$W = \left\{ \begin{pmatrix} x \\ x \end{pmatrix} : x \in \mathbf{R} \right\}$$

be the one-dimensional subspace of $\mathbf{R}^2$ spanned by the vector $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. We have $T\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and so W is invariant with respect to T.

Let $T : V \to V$ be a linear operator, and let W be a subspace of V that is invariant with respect to T. Suppose that $\dim(V) = n$, and that $\dim(W) = r$. Choose a basis $\{e_1, \ldots, e_r\}$ for W, and extend to a basis for V, that is, choose vectors $\{e_{r+1}, \ldots, e_n\}$ such that $\mathscr{B} = \{e_1, \ldots, e_n\}$ is a basis for V. For $j = 1, \ldots, r$ we have $T(e_j) = \sum_{i=1}^{r} a_{i,j} e_i$, and for $j = r+1, \ldots, n$ we have $T(e_j) = \sum_{i=1}^{n} a_{i,j} e_i$. It follows that the matrix $A = (a_{i,j})$ of T with respect to the basis $\mathscr{B}$ consists of an $r \times r$ square sub matrix in the upper left corner, and beneath this square is an $(n-r) \times r$ rectangular matrix of 0s.

For example, let $e_1 = (1,1)$ and $e_2 = (1,0)$ in $\mathbf{R}^2$. If $T : \mathbf{R}^2 \to \mathbf{R}^2$ is the linear operator (5.1), then $\{e_1\}$ is a basis for W, and $\mathscr{B} = \{e_1, e_2\}$ is a basis for $\mathbf{R}^2$. Then $T(e_1) = e_1$, $T(e_2) = e_1 - e_2$, and the matrix for T with respect to $\mathscr{B}$ is

$$[T]_{\mathscr{B}} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Let $T : V \to V$ be a linear operator, and let W_1 and W_2 be invariant subspaces of T such that $V = W_1 \oplus W_2$. If $\dim(V) = n$ and $\dim(W_1) = r_1$, then $\dim(W_2) = n - r_2$. Let $\{e_1, \ldots, e_{r_1}\}$ be a basis for W_1 and $\{e_{r_1+1}, \ldots, e_n\}$ be a basis for W_2. Then $\mathscr{B} = \{e_1, \ldots, e_n\}$ is a basis for V, $T(e_j) = \sum_{i=1}^{r_1} a_{i,j} e_i$ for $j = 1, \ldots, r_1$, and $T(e_j) = \sum_{i=r_1+1}^{n} a_{i,j} e_i$ for $j = r_1 + 1, \ldots, n$. It follows that $A = [T]_{\mathscr{B}}$, the matrix for T with respect to $\mathscr{B}$, is a block matrix, that is, an $n \times n$ matrix such that the upper left corner is an $r_1 \times r_1$ matrix, the lower right corner is a $r_2 \times r_2$ matrix, the lower left corner is an $r_2 \times r_1$ matrix of 0s, and the upper right corner is an $r_2 \times r_1$ matrix of 0s.

For example, let $T : \mathbf{R}^4 \to \mathbf{R}^4$ be the linear operator such that

$$T \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 3x_1 - 5x_2 \\ 2x_1 + 7x_2 \\ x_3 - 8x_4 \\ 4x_3 - x_4 \end{pmatrix}.$$

The subspaces

$$W_1 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ 0 \\ 0 \end{pmatrix} : x_1, x_2 \in \mathbf{R} \right\}$$

and

$$W_2 = \left\{ \begin{pmatrix} 0 \\ 0 \\ x_3 \\ x_4 \end{pmatrix} : x_3, x_4 \in \mathbf{R} \right\}$$

are invariant with respect to T, and $\mathbf{R}^r = W_1 \oplus W_2$. A basis for W_1 is $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}$ and a basis for W_2 is $\left\{ \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$ Their union is the standard basis $\mathscr{E}$. The matrix for T with respect to the standard basis $\mathscr{E}$ is the block matrix

$$[T]_{\mathscr{E}} = \begin{pmatrix} 3 & -5 & 0 & 0 \\ 2 & 7 & 0 & 0 \\ 0 & 0 & 1 & -8 \\ 0 & 0 & 4 & -1 \end{pmatrix}.$$

Exercises

1. A linear operator $T : V \to V$ is an *involution* if $T^2 = I$. Prove that the linear operator defined by (5.1) is an involution.

5.3 Eigenvalues and eigenvectors in $\mathbf{R}^2$

Let V be a vector space over the field K, and let $T : V \to V$ be a linear operator. An *eigenvector* of T is a nonzero vector v such that $T(v) = \lambda v$ for some $\lambda \in K$. A scalar $\lambda \in K$ is an *eigenvalue* of T if there exists a nonzero vector $v \in V$ such that $T(v) = \lambda v$. The *spectrum* of the linear operator T, denoted $\mathrm{Spec}(T)$, is the set of eigenvalues of T, that is,

$$\mathrm{Spec}(T) = \{\lambda \in K : T(v) = \lambda v \text{ for some nonzero vector } v \in V\}.$$

We shall consider only linear operators $T : \mathbf{R}^2 \to \mathbf{R}^2$. In this case, we have $\lambda \in \mathrm{Spec}(T)$ if and only if there exists $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2$ such that $\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ and

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}. \tag{5.2}$$

We begin with some examples.

Consider the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x \\ 3y \end{pmatrix}.$$

Comparing this with (5.2), we have $\lambda \in \mathrm{Spec}(T)$ if and only if $\begin{pmatrix} 2x \\ 3y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}$ if and only if $\lambda x = 2x$ and $\lambda y = 3y$ for some $\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. If $x \neq 0$, then $\lambda = 2$ and $y = 0$. If $y \neq 0$, then $\lambda = 3$ and $x = 0$. Thus, $\mathrm{Spec}(T) = \{2, 3\}$, and $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is an eigenvector associated with the eigenvalue 2, and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is an eigenvector associated with the eigenvalue 3.

Consider the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -y \\ x \end{pmatrix}.$$

Comparing this with (5.2), we have $\lambda \in \mathrm{Spec}(T)$ if and only if $\lambda x = -y$ and $\lambda y = x$ for some $\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. These equations imply that

$$x = \lambda y = \lambda(-\lambda x) = -\lambda^2 x$$

and so

$$(\lambda^2 + 1)x = 0.$$

Because $\lambda^2 + 1 \neq 0$ for all $\lambda \in \mathbf{R}$, it follows that $x = 0$ and $y = 0$. Thus, the operator T has no eigenvalue, and $\mathrm{Spec}(T) = \emptyset$.

Consider the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3x + 2y \\ x + 4y \end{pmatrix}.$$

The real number λ is an eigenvalue of T if and only if there exists a nonzero vector $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2$ such that

$$\begin{pmatrix} 3x + 2y \\ x + 4y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}.$$

This is equivalent to the existence of a nonzero solution of the homogeneous system of linear equations

$$\begin{cases} (\lambda - 3)x - 2y = 0 \\ -x + (\lambda - 4)y = 0 \end{cases} \tag{5.3}$$

and this happens if and only

$$\det \begin{pmatrix} \lambda - 3 & -2 \\ -1 & \lambda - 4 \end{pmatrix} = \lambda^2 - 7\lambda + 10 = (\lambda - 2)(\lambda - 5) = 0.$$

It follows that $\mathrm{Spec}(T) = \{2, 5\}$.

If $\lambda = 2$, then equations (5.3) reduce to

$$-x - 2y = 0$$

and so $x = -2y$. Thus, the vector $\begin{pmatrix} -2 \\ 1 \end{pmatrix}$ is an eigenvector with eigenvalue 2.

If $\lambda = 5$, then equations (5.3) reduce to

$$2x - 2y = 0$$

and so $x = y$. It follows that the vector $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ is an eigenvector with eigenvalue 5.

We check this directly as follows:

$$\begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} -2 \\ 1 \end{pmatrix} = \begin{pmatrix} -4 \\ 2 \end{pmatrix} = 2 \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ 5 \end{pmatrix} = 5 \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

The general case is a linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by the 2×2 matrix $[T] = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Thus,

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}, \tag{5.4}$$

The real number λ is an eigenvalue of T if and only if there exists a nonzero vector $\begin{pmatrix} x \\ y \end{pmatrix}$ such that

$$\begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} = T \begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}$$

if and only if the system of homogeneous linear equations

$$\begin{aligned} (\lambda - a)x - by &= 0 \\ -cx + (\lambda - d)y &= 0 \end{aligned}$$

has a nonzero solution. This is equivalent to

$$\det \begin{pmatrix} \lambda - a & -b \\ -c & \lambda - d \end{pmatrix} = \lambda^2 - (a+d)\lambda + (ad - bc) = 0.$$

If $b \neq 0$, then $\begin{pmatrix} b \\ \lambda - a \end{pmatrix}$ is an eigenvector with eigenvalue λ. If $c \neq 0$, then $\begin{pmatrix} \lambda - d \\ c \end{pmatrix}$ is an eigenvector with eigenvalue λ. If $b = c = 0$, then $\mathrm{Spec}(T) = \{a, d\}$ and the vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are eigenvectors with eigenvalues a and d, respectively.

We observe that

$$[\lambda I - T] = \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda - a & -b \\ -c & \lambda - d \end{pmatrix}$$

and so $\lambda \in \mathrm{Spec}(T)$ if and only if $\det(\lambda I - T) = 0$.

We define the eigenvalues and eigenvectors of a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{R})$ as the eigenvalues and eigenvectors of the linear operator defined by (5.4).

Exercises

1. Consider the linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$T\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}117x+80y\\-168x-115y\end{pmatrix}.$$

Compute the eigenvalues of this operator, and an eigenvector for each eigenvalue.

2. Consider the linear operator $T:\mathbf{R}^2\to\mathbf{R}^2$ defined by

$$T\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}8x-6y\\5x-3y\end{pmatrix}.$$

Compute $\operatorname{Spec}(T)$, and construct an eigenvector for each eigenvalue $\lambda\in\operatorname{Spec}(T)$.

3. Compute the eigenvalues and eigenvectors for the following matrices:

$$\begin{pmatrix}1&1\\0&1\end{pmatrix},\qquad\begin{pmatrix}1&-1\\1&1\end{pmatrix},\qquad\begin{pmatrix}0&1\\1&0\end{pmatrix}.$$

4. The function $R_\alpha:\mathbf{R}^2\to\mathbf{R}^2$ that rotates every vector by the angle α is the linear operator with matrix

$$[R_\alpha]=\begin{pmatrix}\cos\alpha&-\sin\alpha\\\sin\alpha&\cos\alpha\end{pmatrix}$$

Prove that the rotation R_α has an eigenvalue if and only if $\alpha=n\pi$ for some $n\in\mathbf{Z}$, and that $\operatorname{Spec}(R_{n\pi})=\{(-1)^n\}$. Compute an eigenvector for this eigenvalue.

5. Let $-\pi/2<\alpha\le\pi/2$, and let ℓ_α be the line through the origin with slope $\tan\alpha$. Equivalently, ℓ_α is the one-dimensional subspace spanned by the vector $\begin{pmatrix}\cos\alpha\\\sin\alpha\end{pmatrix}$. The function $S_\alpha:\mathbf{R}^2\to\mathbf{R}^2$ that reflects every vector through the line ℓ_α is the linear operator with matrix

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

Prove that $\operatorname{Spec}(S_\alpha)=\{1,-1\}$. Compute an eigenvector for each of these eigenvalues.

Solutions

1. $\operatorname{Spec}(T)=\{-3,5\}$. Eigenvector -3 has eigenvalue $\begin{pmatrix}2\\-3\end{pmatrix}$. Eigenvector 5 has eigenvalue $\begin{pmatrix}5\\-7\end{pmatrix}$.
2. $\operatorname{Spec}(T)=\{2,3\}$. Eigenvector 2 has eigenvalue $\begin{pmatrix}1\\1\end{pmatrix}$. Eigenvector 3 has eigenvalue $\begin{pmatrix}6\\5\end{pmatrix}$.
3. Left to reader.

4. The real number λ is an eigenvalue of R_α if and only if λ is a solution of the quadratic equation

$$\begin{aligned}\det(\lambda I - [R_\alpha]) &= \det\begin{pmatrix}\lambda - \cos\alpha & \sin\alpha \\ -\sin\alpha & \lambda - \cos\alpha\end{pmatrix} \\ &= \lambda^2 - 2\cos\alpha\lambda + 1 \\ &= 0.\end{aligned}$$

By the quadratic formula,

$$\lambda = \cos\alpha \pm \sqrt{\cos^2\alpha - 1}$$

and λ is real if and only if $\cos\alpha = \pm 1$ if and only if $\alpha = n\pi$ for some $n \in \mathbf{Z}$. In this case, $\mathrm{Spec}(R_\alpha) = \{\cos n\pi\} = \{(-1)^n\}$.

5. The real number λ is an eigenvalue of S_α if and only if λ is a solution of the quadratic equation

$$\begin{aligned}\det(\lambda I - S_\alpha) &= \det\begin{pmatrix}\lambda - \cos 2\alpha & -\sin 2\alpha \\ -\sin 2\alpha & \lambda + \cos 2\alpha\end{pmatrix} \\ &= \lambda^2 - 1 \\ &= 0\end{aligned}$$

and so $\mathrm{Spec}(S_\alpha) = \{1, -1\}$. If $\alpha \neq 0, \pi/2$, then $\sin 2\alpha \neq 0$ and $\sin\alpha \neq 0$. An eigenvector with eigenvalue 1 is

$$\begin{aligned}\begin{pmatrix}\sin 2\alpha \\ 1 - \cos 2\alpha\end{pmatrix} = \begin{pmatrix}2\sin\alpha\cos\alpha \\ 1 - \cos^2\alpha + \sin^2\alpha\end{pmatrix} &= \begin{pmatrix}2\sin\alpha\cos\alpha \\ 2\sin^2\alpha\end{pmatrix} \\ &= 2\sin\alpha\begin{pmatrix}\cos\alpha \\ \sin\alpha\end{pmatrix}.\end{aligned}$$

Thus, every nonzero vector on the line ℓ_α is an eigenvector with eigenvalue 1 for reflection through ℓ_α.

An eigenvector with eigenvalue -1 is

$$\begin{aligned}\begin{pmatrix}\sin 2\alpha \\ -1 - \cos 2\alpha\end{pmatrix} &= \begin{pmatrix}2\sin\alpha\cos\alpha \\ -1 - \cos^2\alpha + \sin^2\alpha\end{pmatrix} \\ &= \begin{pmatrix}2\sin\alpha\cos\alpha \\ -2\cos^2\alpha\end{pmatrix} = -2\cos\alpha\begin{pmatrix}-\sin\alpha \\ \cos\alpha\end{pmatrix} \\ &= -2\cos\alpha\begin{pmatrix}\cos(\alpha + \pi/2) \\ \sin(\alpha + \pi/2)\end{pmatrix}.\end{aligned}$$

Thus, every nonzero vector on the line perpendicular to ℓ_α is an eigenvector with eigenvalue -1 for reflection through ℓ_α.

The case $\alpha \in \{0, \pi/2\}$ is left to the reader.

Lemma 5.2. *Let V be a vector space over the field K, and let $T : V \to V$ be a linear operator. For each $\lambda \in K$, let*

$$E_T(\lambda) = \{v \in V : T(v) = \lambda v\}.$$

Then $E_T(\lambda)$ is a subspace of V, and λ is an eigenvalue of T if and only if $\dim(E_T(\lambda)) \geq 1$. *If $p(t)$ is a polynomial with coefficients in K and if $v \in E_T(\lambda)$, then $p(T)(v) = p(\lambda)v$.*

We call $E_T(\lambda)$ the *eigenspace* associated with the eigenvalue λ.

Proof. Because $T(0) = 0 = \lambda 0$ for all $\lambda \in K$, we have $0 \in E_T(\lambda)$ for all $\lambda \in K$. If $v, v' \in E_T(\lambda)$ and $c \in K$, then

$$T(v + v') = T(v) + T(v') = \lambda v + \lambda v' = \lambda(v + v')$$

and so $v + v' \in E_T(\lambda)$. Similarly,

$$T(cv) = cT(v) = c(\lambda v) = (c\lambda)v = (\lambda c)v = \lambda(cv)$$

and so $cv \in E_T(\lambda)$. This proves that $E_T(\lambda)$ is a subspace of V. Moreover, $\dim(E_T(\lambda)) \geq 1$ if and only if $E_T(\lambda)$ contains a nonzero vector if and only if λ is an eigenvalue of T.

Let $T : V \to V$ be a linear operator, and let $p(t) = \sum_{i=0}^{d} a_i t^i$ be a polynomial with coefficients in K. We define the operator $p(T) : V \to V$ by

$$p(T) = \sum_{i=0}^{d} a_i T^i$$

where T^0 is the identity operator I.

Lemma 5.3. *Let V be a vector space over the field K, and let $T : V \to V$ be a linear operator with eigenvalue λ and associated eigenspace $E_T(\lambda)$. If $p(t)$ is a polynomial with coefficients in K and if $v \in E_T(\lambda)$, then $p(T)(v) = p(\lambda)v$.*

Equivalently, if $\lambda \in \mathrm{Spec}(T)$ and $v \in E_T(\lambda)$, then $p(\lambda) \in \mathrm{Spec}(p(T))$ and $p(T)(v) \in E_{p(T)}(p(\lambda))$ for all polynomials $p(t) \in K[t]$.

Lemma 5.4. *Let V be a vector space over the field K, and let $T : V \to V$ be a linear operator. If $\lambda_1, \ldots, \lambda_s$ are distinct eigenvalues of T, and if $v_i \in E_T(\lambda_i)$ for $i = 1, \ldots, s$, then $\{v_1, \ldots, v_s\}$ is a linearly independent set of vectors.*

Proof. The proof is by induction on s. If $s = 1$, then the eigenvector v_1 is nonzero and so $\{v_1\}$ is a linearly independent set.

Let $s \geq 2$, and assume that the Lemma holds for any set of $s - 1$ distinct eigenvalues and eigenvectors. Suppose that $c_1, \ldots, c_s \in K$ and $\sum_{i=1}^{s} c_i v_i = 0$. Then

$$0 = T(0) = T\left(\sum_{i=1}^{s} c_i v_i\right) = \sum_{i=1}^{s} c_i T(v_i) = \sum_{i=1}^{s} c_i \lambda_i v_i.$$

We also have

$$0 = \lambda_s \sum_{i=1}^{s} c_i v_i = \sum_{i=1}^{s} c_i \lambda_s v_i.$$

Subtracting, we obtain

$$0 = \sum_{i=1}^{s-1} c_i(\lambda_s - \lambda_i) v_i.$$

By the induction hypothesis, the set $\{v_1, \ldots, v_{s-1}\}$ is linearly independent. It follows that, for $i = 1, \ldots, s-1$, we have $c_i(\lambda_s - \lambda_i) = 0$ and so $c_i = 0$ because $\lambda_i \neq \lambda_s$. Therfore, $c_s v_s = 0$, and so $c_s = 0$. This completes the proof.

Lemma 5.5. *Let V be a vector space over the field K, let $T : V \to V$ be a linear operator, and let $\lambda_1, \ldots, \lambda_s$ be distinct eigenvalues of T. For $i = 1, \ldots, s$, let $E_T(\lambda_i)$ be the eigenspace associated with λ_i, let $\dim(E(\lambda_i)) = d_i$, and let $\mathscr{B}_i = \{w_{i,j} : j = 1, \ldots, d_i\}$ be a basis for the eigenspace $E(\lambda_i)$. Then $\mathscr{B} = \mathscr{B}_1 \cup \cdots \cup \mathscr{B}_s$ is a linearly independent subset of V.*

Proof. Let $\{c_{i,j} : i = 1, \ldots, s \text{ and } j = 1, \ldots, d_i\}$ be a set of scalars in K such that

$$\sum_{i=1}^{s} \sum_{j=1}^{d_i} c_{i,j} w_{i,j} = 0.$$

For $i = 1, \ldots, s$ we have

$$v_i = \sum_{j=1}^{d_i} c_{i,j} w_{i,j} \in E_T(\lambda_i)$$

and

$$\sum_{i=1}^{s} v_i = 0.$$

It follows from Lemma 5.4 that

$$v_i = \sum_{j=1}^{d_i} c_{i,j} w_{i,j} = 0$$

for $i = 1, \ldots, s$. Because the set $\mathscr{B}_i = \{w_{i,j} : j = 1, \ldots, d_i\}$ is linearly independent, it follows that $c_{i,j} = 0$ for all $i = 1, \ldots, s$ and $j = 1, \ldots, d_i\}$. This completes the proof.

For example, let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be the linear transformation defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 8x - 6y \\ 5x - 3y \end{pmatrix}.$$

Then

$$T\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}2\\2\end{pmatrix} = 2\begin{pmatrix}1\\1\end{pmatrix} \quad \text{and} \quad T\begin{pmatrix}6\\5\end{pmatrix} = \begin{pmatrix}18\\15\end{pmatrix} = 3\begin{pmatrix}6\\5\end{pmatrix}$$

and so $f_1 = \begin{pmatrix}1\\1\end{pmatrix}$ and $f_2 = \begin{pmatrix}6\\5\end{pmatrix}$ are eigenvectors of T with eigenvalues 2 and 3, respectively. By Lemma 5.4, the set $\mathscr{F} = \{f_1, f_2\}$ is an orthogonal basis for $\mathbf{R}^2$. Let $\mathscr{E} = \{e_1, e_2\}$ be the standard basis for $\mathbf{R}^2$. The matrix P that changes coordinates from basis $\mathscr{F}$ to basis $\mathscr{E}$ is

$$P = \begin{pmatrix}1 & 6\\1 & 5\end{pmatrix}.$$

The matrix of T with respect to the basis $\mathscr{E}$ is

$$A = [T]_{\mathscr{E}} = \begin{pmatrix}8 & -6\\5 & -3\end{pmatrix}$$

and so the matrix of T with respect to the basis $\mathscr{B}$ is

$$\begin{aligned} B = [T]_{\mathscr{B}} &= P^{-1}AP \\ &= \begin{pmatrix}-5 & 6\\1 & -1\end{pmatrix}\begin{pmatrix}8 & -6\\5 & -3\end{pmatrix}\begin{pmatrix}1 & 6\\1 & 5\end{pmatrix} \\ &= \begin{pmatrix}2 & 0\\0 & 3\end{pmatrix}. \end{aligned}$$

Thus, the matrix of the linear transformation T with respect to the eigenvector basis $\mathscr{F}$ is a diagonal matrix with the eigenvalues on the main diagonal.

Another example: Consider the symmetric 2×2 matrix

$$A = \begin{pmatrix}5 & 2\\2 & -1\end{pmatrix}$$

and the associated linear operator $T : \mathbf{R}^2 \to \mathbf{R}^2$ such that $[T]_{\mathscr{E}} = A$. The characteristic polynomial of T is

$$\det(tI - A) = \det\begin{pmatrix}t-5 & -2\\-2 & t+1\end{pmatrix} = t^2 - 4t - 9$$

with roots $\lambda_1 = 2 + \sqrt{13}$ and $\lambda_2 = 2 - \sqrt{13}$. Solving the vector equation

$$A\begin{pmatrix}x\\y\end{pmatrix} = \lambda_1\begin{pmatrix}x\\y\end{pmatrix}$$

or, equivalently,

$$\begin{pmatrix}5 & 2\\2 & -1\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = (2+\sqrt{13})\begin{pmatrix}x\\y\end{pmatrix}$$

we obtain

$$\begin{pmatrix} x \\ y \end{pmatrix} = t \begin{pmatrix} 3+\sqrt{13} \\ 2 \end{pmatrix}.$$

Solving the vector equation

$$\begin{pmatrix} 5 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} = \lambda_2 \begin{pmatrix} x \\ y \end{pmatrix} = (2-\sqrt{13}) \begin{pmatrix} x \\ y \end{pmatrix}$$

we obtain

$$\begin{pmatrix} x \\ y \end{pmatrix} = t \begin{pmatrix} 3-\sqrt{13} \\ 2 \end{pmatrix}.$$

Note that

$$\begin{pmatrix} 5 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 3+\sqrt{13} \\ 2 \end{pmatrix} = \begin{pmatrix} 19+5\sqrt{13} \\ 4+2\sqrt{13} \end{pmatrix} = (2+\sqrt{13}) \begin{pmatrix} 3+\sqrt{13} \\ 2 \end{pmatrix}$$

and

$$\begin{pmatrix} 5 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 3-\sqrt{13} \\ 2 \end{pmatrix} = \begin{pmatrix} 19-5\sqrt{13} \\ 4-2\sqrt{13} \end{pmatrix} = (2-\sqrt{13}) \begin{pmatrix} 3-\sqrt{13} \\ 2 \end{pmatrix}.$$

Let $\mathscr{B} = \{f_1, f_2\}$, where $f_1 = \begin{pmatrix} 3+\sqrt{13} \\ 2 \end{pmatrix}$ and $f_2 = \begin{pmatrix} 3-\sqrt{13} \\ 2 \end{pmatrix}$ are eigenvectors of the eigenvalues $\lambda_1 = 2+\sqrt{13}$ and $\lambda_2 = 2-\sqrt{13}$, respectively. Then $\mathscr{F}$ is a basis for $\mathbf{R}^2$. The change of basis matrix from $\mathscr{E}$ to $\mathscr{F}$ is

$$P = \begin{pmatrix} 3+\sqrt{13} & 3-\sqrt{13} \\ 2 & 2 \end{pmatrix}.$$

Then

$$P^{-1} = \frac{1}{4\sqrt{13}} \begin{pmatrix} 2 & -3+\sqrt{13} \\ -2 & 3+\sqrt{13} \end{pmatrix}.$$

and the matrix of T with respect to the basis $\mathscr{F}$ is

$$[T]_{\mathscr{F}} = P^{-1}[T]_{\mathscr{E}}P = \begin{pmatrix} 5 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 3+\sqrt{13} & 3-\sqrt{13} \\ 2 & 2 \end{pmatrix}$$

Let $C^\infty(\mathbf{R})$ be the vector space of real-valued infinitely differentiable functions on the real line, and let $D : C^\infty(\mathbf{R}) \to C^\infty(\mathbf{R})$ be the linear transformation defined by differentiation. Thus, if $f \in C^\infty(\mathbf{R})$, then $D(f)$ is the derivative of f. For example, if $f = t^2$, then $D(f) = 2t$. Here is an eigenvalue problem from calculus: For $\lambda \in \mathbf{R}$, find the eigenspace associated with the eigenvalue λ. The function f is an eigenvector of D with eigenvalue $\lambda \in \mathbf{R}$ if and only if

$$D(f) = \lambda f$$

The solution space of this differentiable equation, that is, the eigenspace associated with the λ, is the one-dimensional subspace of $C^\infty(\mathbf{R})$ generated by the function $f(t) = e^{\lambda t}$.

Theorem 5.3. *Let V be a finite dimensional vector space over the field K, and let $T : V \to V$ be a linear operator. The scalar $\lambda \in K$ is an eigenvalue of T if and only if* $\det(\lambda I - A) = 0$.

Proof. If λ is an eigenvalue of T with associated eigenvector v, then $T(v) = \lambda v = \lambda I(v)$, or, equivalently,
$$(\lambda I - T)(v) = 0.$$
Thus, the linear operator $\lambda I - T$ has a nonzero kernel. Conversely, if the kernel of $\lambda I - T$ is nonzero, then λ is an eigenvalue of T. Equivalently, λ is an eigenvalue of T if and only if $\det(\lambda I - T) \neq 0$.

Theorem 5.4. *If V is an n-dimensional vector space over the field K, then every linear operator on V has at most n eigenvalues.*

Proof. Let T be a linear operator on V, let $\mathscr{B}$ be an ordered basis for T, and let $A = [T]_{\mathscr{B}}$ be the $n \times n$ matrix of T with respect to the basis $\mathscr{B}$. Consider the $n \times n$ matrix
$$xI - A = \begin{pmatrix} x - a_{1,1} & -a_{1,2} & -a_{1,3} & \cdots & -a_{1,n-1} & -a_{1,n} \\ -a_{2,1} & x - a_{2,2} & -a_{2,3} & \cdots & -a_{2,n-1} & -a_{2,n} \\ -a_{3,1} & -a_{3,2} & x - a_{3,3} & \cdots & -a_{3,n-1} & -a_{3,n} \\ \vdots & & & \vdots & & \\ -a_{n-1,1} & -a_{n-1,2} & -a_{n-1,3} & \cdots & x - a_{n-1,n-1} & -a_{n-1,n} \\ -a_{n,1} & -a_{n,2} & -a_{n,3} & \cdots & -a_{n,n-1} & x - a_{n,n} \end{pmatrix}.$$

Then $f(x) = \det(xI - A)$ is a polynomial in x of degree n. A polynomial of degree n with coefficients in a field has at most n roots, and so T has at most n eigenvalues.

Exercises

1. Find the eigenvalues of the linear transformation $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by $T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}$. Find an orthonormal basis of eigenvectors of $\mathbf{R}^2$.
2. Find the eigenvalues of the linear transformation $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by $T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 8y \\ 2x \end{pmatrix}$, or, equivalently,
$$[T]_{\mathscr{E}} = \begin{pmatrix} 0 & 8 \\ 2 & 0 \end{pmatrix}.$$

   Find an orthonormal basis of eigenvectors of $\mathbf{R}^2$.

3. Find the eigenvalues of the linear transformation $T : \mathbf{C}^2 \to \mathbf{C}^2$ defined by $T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} y \\ 2z \\ 3x \end{pmatrix}$, or, equivalently,
$$[T]_{\mathscr{E}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 3 & 0 & 0 \end{pmatrix}.$$
Find an orthonormal basis of eigenvectors of $\mathbf{C}^3$.
4. Let $(c_n)_{n=1}^{\infty}$ be a sequence of complex numbers, and let $A_n = (a_{i,j})$ be the $n \times n$ matrix such that
$$a_{i,j} = \begin{cases} c_i & \text{if } i \in \{1, \ldots, n-1\} \text{ and } j = i+1 \\ c_n & \text{if } i = n \text{ and } j = 1 \\ 0 & \text{otherwise.} \end{cases}$$
Prove that A_n is diagonalizable, and that the spectrum of A_n is the set of nth roots of $c_1 c_2 \cdots c_n$.

5.4 Diagonalization of symmetric matrices

Let V be a finite-dimensional real inner product space. Let $T : V \to V$ be a linear operator. For every vector $w \in V$ we define the function $\alpha_w : V \to \mathbf{R}$ by
$$\alpha_w(v) = (T(v), w).$$
For all vectors $v, v' \in V$ and all scalars $c \in \mathbf{R}$ we have
$$\begin{aligned} \alpha_w(cv + v') &= (T(cv + v'), w) \\ &= (cT(v) + T(v'), w) \\ &= c(T(v), w) + (T(v'), w) \\ &= c\alpha_w(v) + \alpha_w(v') \end{aligned}$$
and so α_w is a linear functional. Thus, $\alpha \in V^*$, the dual space of V. By Theorem **??**, there exists a vector $w^* \in V$ such that
$$\alpha_w(v) = (v, w^*)$$
for all $v \in V$. We define the function $T^* : V \to V$ by
$$T^*(w) = w^*.$$
With this definition we have

$$(T(v),w) = \alpha_w(v) = (v,w^*) = (v,T^*(w))$$

for all $v,w \in V$.

We shall prove that $T^* : V \to V$ is a linear operator. Let $w,w' \in V$ and $c \in \mathbf{R}$. For all $v \in V$ we have

$$\begin{aligned}(v,T^*(cw+w')) &= \alpha_{cw+w'}(v)\\ &= (v,cw+w')\\ &= c(v,w)+(v,w')\\ &= c\alpha_w(v)+\alpha_{w'}(v)\\ &= c(v,T^*(w))+(v,T^*(w'))\\ &= (v,cT^*(w)+T^*(w')).\end{aligned}$$

It follows from Lemma **??** that $T^*(cw+w')) = cT^*(w)+T^*(w')$, and so T^* is a linear operator on V. This linear operator is called the *adjoint* of T.

An operator $T : V \to V$ on a real or complex inner product space is *self-adjoint* if $T = T^*$. Equivalently, T is self-adjoint if

$$(T(v),w) = (v,T(w))$$

for all vectors $v,w \in V$.

A self-adjoint operator on a complex vector space is called *Hermitian* if $T = T^*$. Equivalently, T is Hermitian if

$$(T(v),w) = (v,T(w))$$

for all vectors $v,w \in V$. An $n \times n$ matrix $A = (a_{i,j})$ is Hermitian if $a_{i,j} = \overline{a_{j,i}}$ for all $i,j = 1,\ldots,n$.

A self-adjoint operator on a real vector space is called *symmetric* if $T = T^*$. Equivalently, T is symmetric if

$$(T(v),w) = (v,T(w))$$

for all vectors $v,w \in V$. An $n \times n$ matrix $A = (a_{i,j})$ is symmetric if $a_{i,j} = a_{j,i}$ for all $i,j = 1,\ldots,n$.

An operator $T : V \to V$ is Hermitian (resp. symmetric) if and only if its matrix with respect to any orthonormal basis is a Hermitian (resp. symmetric) matrix.

Lemma 5.6. *Let V be a finite-dimensional real inner product space,* $\dim(V) = n$*, and let $\mathscr{E} = \{e_1,\ldots,e_n\}$ be an orthonormal basis for V. The linear operator $T : V \to V$ is symmetric if and only if the $n \times n$ matrix $[T]_{\mathscr{E}}$ is symmetric.*

Proof. Let $[T]_{\mathscr{E}} = A = (a_{i,j})$ and $[T^*]_{\mathscr{E}} = A^* = (a^*_{i,j})$. Then $T(e_i) = \sum_{r=1}^n a_{r,i}e_r$ and $T^*(e_j) = \sum_{s=1}^n a^*_{s,j}e_s$. For all $i,j = 1,\ldots,n$, we have

$$(e_i, T^*(e_j)) = \left(e_i, \sum_{s=1}^{n} a^*_{s,j} e_s\right) = \sum_{s=1}^{n} a^*_{s,j} (e_i, e_s) = \sum_{s=1}^{n} a^*_{s,j} \delta_{i,s} = a^*_{i,j}$$

and

$$(T(e_i), e_j) = \left(\sum_{r=1}^{n} a_{r,i} e_r, e_j\right) = \sum_{r=1}^{n} a_{r,i} (e_r, e_j) = \sum_{r=1}^{n} a_{r,i} \delta_{r,j} = a_{j,i}.$$

Therefore, $(T(e_i), e_j) = (e_i, T^*(e_j))$ if and only if

$$a^*_{i,j} = a_{j,i}$$

for all $i, j = 1, \ldots, n$, and so the matrix A^* is the transpose of the matrix A. It follows that T is symmetric if and only if $T = T^*$ if and only if $A = A^*$ if and only if $a_{i,j} = a^*_{i,j} = a_{j,i}$ for all $i, j = 1, \ldots, n$, that is, if and only if the matrix $A = [T]_{\mathscr{E}}$ is symmetric. This completes the proof.

Lemma 5.7. *Let T be an operator on a finite dimensional complex vector space V. If T is self-adjoint, then every eigenvalue of T is real.*

Proof. Let λ be an eigenvalue of T. If v is an eigenvector with eigenvalue λ, then $v \neq 0$ and

$$\lambda(v, v) = (\lambda v, v) = (T(v), v) = (v, T(v)) = (v, \lambda v) = \overline{\lambda}(v, v).$$

It follows that

$$(\lambda - \overline{\lambda})(v, v) = 0$$

and so $\lambda = \overline{\lambda}$, that is, λ is a real number. This completes the proof.

Theorem 5.5. *Let V be a finite-dimensional real inner product space. Every symmetric linear operator $T : V \to V$ has a real eigenvalue.*

Proof. Let $\dim(V) = n$. Let $\mathscr{E}$ be an ordered basis for V, and let $A = [T]_{\mathscr{E}}$ be the matrix for T with respect to $\mathscr{E}$. Note that A is an $n \times n$ matrix with real coefficients. Consider the n-dimensional vector space $\mathbf{C}^n$, and use the matrix A to define a linear operator S on $\mathbf{C}^n$ by

$$S \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = A \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}.$$

By Theorem **??**, the linear operator S has an eigenvector with eigenvalue λ. Because every real symmetric matrix is self-adjoint, it follows from Lemma 5.7 that λ is a real number. Let w be an eigenvector with eigenvalue λ. Then $w \in \mathbf{C}^n$ and so there are complex numbers $w_j = u_j + iv_j$ for $j = 1, \ldots, n$ such that

$$w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} u_1 + iv_1 \\ \vdots \\ u_n + iv_n \end{pmatrix} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} + i \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = u + iv$$

where

$$u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in \mathbf{R}^n \quad \text{and} \quad v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbf{R}^n.$$

We have the vector equation

$$\lambda u + i\lambda v = \lambda(u+iv) = \lambda w = A(w) = A(u+iv) = A(u) + iA(v).$$

Because the vectors λu, λv, $A(u)$, and $A(v)$ are real, it follows that

$$A(u) = \lambda u \quad \text{and} \quad A(v) = \lambda v.$$

If $u = v = 0$, then $w = u + iv = 0$, which is false. Therefore, at least one of the real vectors u and v is nonzero, and so at least one of the vectors u and v in $\mathbf{R}^n$ is an eigenvector with eigenvalue λ. This completes the proof.

5.5 Adjoint of a linear operator

Let V be a vector space over the field K. A *linear functional* on the vector space V is a linear transformation from V into K. Let $\mathscr{E} = \{e_1, \ldots, e_n\}$ be an ordered basis for V. Let α be a linear functional on V. If $v = \sum_{i=1}^n x_i e_i \in V$, then

$$\alpha(v) = \alpha\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n x_i \alpha(e_i)$$

and so α is determined by the n-tuple

$$\begin{pmatrix} \alpha(e_1) \\ \vdots \\ \alpha(e_n) \end{pmatrix} \in K^n.$$

Define the linear functional Let V be a finite-dimensional vector space, and let V^* be the dual space of V, that is, the vector space of linear

Let V be a finite-dimensional real or complex inner product space, and let $T : V \to V$ be a linear operator. There exists a unique linear operator $T^* : V \to V$ such that

$$(T(v), v') = (v, T^*(v'))$$

for all vectors $v, v' \in V$. If T_1, T_2 are linear operators on V and if c is a scalar, then

$$\begin{aligned}((cT_1+T_2)(v),v') &= c(T_1(v),v')+(T_2(v),v') \\ &= c(v,T_1^*(v'))+(v,T_2^*(v')) \\ &= (v,\bar{c}T_1^*(v'))+(v,T_2^*(v')) \\ &= (v,(\bar{c}T_1^*+T_2^*)(v')) \\ &= (v,(cT_1+T_2)^*(v'))\end{aligned}$$

and so

$$(cT_1+T_2)^* = \bar{c}T_1^*+T_2^*.$$

Let $T^{**}=(T^*)^*$ denote the adjoint of the adjoint of T. It follows that

$$(T(v),v') = (v,T^*(v')) = \overline{(T^*(v'),v)} = \overline{(v',T^{**}(v))} = (T^{**}(v),v')$$

and so

$$((T-T^{**})(v),v') = (T(v)-T^{**}(v),v') = 0.$$

It follows that $T-T^{**}=0$, or, equivalently,

$$T = T^{**}.$$

5.6 Normal operators

Let V be a finite-dimensional complex vector space. A linear operator $T:V\to V$ is *normal* if it commutes with its adjoint, that is, if

$$TT^* = T^*T.$$

Lemma 5.8. *Let V be a finite-dimensional complex vector space, and let $T:V\to V$ be a normal operator. If w is an eigenvector of T with eigenvalue λ, then w is an eigenvector of T^* with eigenvalue $\overline{\lambda}$.*

Proof. If S is a normal operator on V, then for all $v\in V$ we have

$$\begin{aligned}\|S(v)\|^2 &= (S(v),S(v)) = (v,S^*S(v)) \\ &= (v,SS^*(v)) = (v,S^{**}S^*(v)) \\ &= (S^*(v),S^*(v)) \\ &= \|S^*(v)\|^2.\end{aligned}$$

We shall prove that the operator

$$S = \lambda I - T$$

is normal. We have

$$S^* = \overline{\lambda}I - T^*$$

and

$$\begin{aligned} SS^* &= (\lambda I - T)(\overline{\lambda} I - T^*) \\ &= \lambda\overline{\lambda} I - \lambda T^* - \overline{\lambda} T + TT^* \\ &= \overline{\lambda}\lambda I - \lambda T^* - \overline{\lambda} T + T^*T \\ &= (\overline{\lambda} I - T^*)(\lambda I - T) \\ &= S^*S. \end{aligned}$$

Thus, the operator S is normal, and so

$$\begin{aligned} \|T^*(w) - \overline{\lambda} w\|^2 &= \|S^*(w)\|^2 \\ &= \|S(w)\|^2 \\ &= \|T(w) - \lambda w\|^2 \\ &= 0. \end{aligned}$$

Thus, w is an eigenvector of T^* with eigenvalue $\overline{\lambda}$. This completes the proof.

Theorem 5.6. *Let V be a finite-dimensional complex inner product space, and let $T : V \to V$ be a linear operator. There exists an orthonormal basis $\mathscr{E}$ for V such that the matrix of T with respect to $\mathscr{B}$ is upper triangular.*

Proof. The proof is by induction on $n = \dim(V)$. Every 1×1 matrix is upper diagonal. If $n = 1$, then every unit vector e_1 in V is an eigenvector, and $\mathscr{E} = \{e_1\}$ is an orthonormal basis for V such that $[T]_{\mathscr{B}}$ is diagonal.

Let $n \geq 2$, and assume the theorem is true for linear operators on inner product spaces of dimension $n-1$. Every operator on a finite-dimensional complex inner product space has an eigenvector. Let e_n be a unit eigenvector of T^*, and let V' be the orthogonal complement of the one-dimensional subspace spanned by e_1. By Theorem **??**, the subspace V' is invariant with respect to operator $T^{**} = T$. Let T' be the restriction of T to V'. Because $\dim(V') = n-1$, the induction hypothesis implies that there is an orthonormal basis $\mathscr{E}' = \{e_1, \ldots, e_{n-1}\}$ for V' such that the matrix of T' is upper diagonal. Thus, for $j = 1, \ldots, n-1$ and $i = 1, \ldots, j$ there are complex numbers $a_{i,j}$ such that $T(e_j) = \sum_{i=1}^{j} a_{i,j} e_i$. Because V' is orthogonal to the subspace spanned by $\{e_n\}$, the set $\mathscr{E} = \mathscr{E}' \cup \{e_n\} = \{e_1, \ldots, e_{n-1}, e_n\}$ is an orthonormal basis for V. There are complex numbers $a_{i,n}$ such that $T(e_n) = \sum_{i=1}^{n} a_{i,n} e_i$. Let $a_{i,j} = 0$ for $1 \leq j < i \leq n$. The $n \times n$ matrix $A = [T]_{\mathscr{B}}$ is upper triangular. This completes the proof.

Theorem 5.7. *Let V be a finite-dimensional complex inner product space, and let $\mathscr{E}$ be an orthonormal basis for V. Let T be a linear operator on V such that $A = [T]_{\mathscr{E}}$, the matrix for T with respect to $\mathscr{E}$, is upper diagonal. Then T is a normal operator if and only if A is diagonal.*

Proof. Let $\dim(V) = n$ and let $\mathscr{E} = \{e_1, \ldots, e_n\}$. If $A = (a_{i,j})$ is diagonal, then every basis vector i_i is an eigenvector with eigenvalue $\lambda_i = a_{i,i}$ for $i = 1, \ldots, n$. By Theorem **??**, the vector e_i is also an eigenvector of T^* with eigenvalue $\overline{\lambda_i}$. It follows that

$$T^*T(e_i) = T^*(\lambda_i e_i) = \lambda_i T^*(e_i) = \lambda_i \overline{\lambda_i} e_i = |\lambda_i|^2 e_i.$$

Similarly,

$$TT^*(e_i) = T(\overline{\lambda_i} ie_i) = \overline{\lambda_i} T(e_i) = \overline{\lambda_i} \lambda_i e_i = |\lambda_i|^2 e_i$$

It follows that $T^*T(e_i) = TT^*(e_i)$ for all $e_i \in \mathscr{E}$, and so $T^*T(v) = TT^*(v)$ for all $v \in V$. Thus, T is a normal operator.

Conversely, suppose that T is a normal operator whose matrix $A = (a_{i,j}) = [T]_{\mathscr{E}}$ is upper diagonal. The matrix for T^* is the conjugate transpose of A, that is,

$$[T^*] = (\overline{a_{j,i}}) = [T^*]_{\mathscr{E}}.$$

The upper diagonally of A implies that $T(e_1) = a_{1,1}e_1$, a nd so e_1 is an eigenvector of T with eigenvalue $a_{1,1}$. By Theorem **??** the vector e_1 is an eigenvector of T^* with eigenvalue $\overline{a_{1,1}}$, and so

$$T^*(e_1) = \overline{a_{1,1}} e_1 = \sum_{i=1}^{n} a^*_{i,1} e_i = \sum_{i=1}^{n} \overline{a_{1,i}} e_i.$$

The unique representation of a vector as a linear combination of basis vectors implies that $\overline{a_{1,i}} = 0$ for $i = 2, \ldots, n$.

5.7 Unitary and orthogonal operators

Let V be a finite-dimensional complex vector space. An operator $U : V \to V$ is *unitary* if $U^{-1} = U^*$. A complex $n \times n$ matrix is *unitary* if the inverse of U is the conjugate transpose of U.

Let V be a finite-dimensional complex vector space. An operator $U : V \to V$ is *orthogonal*
indexlinear transformation!orthogonal if $U^{-1} = U^*$. A complex $n \times n$ matrix is *orthogonal* if the inverse of U is the transpose of U.

Lemma 5.9. *Let V be a finite-dimensional complex or real inner product space, and let S and T be orthonormal bases for V. Let P be the change of basis matrix from T to S, and let $Q = P^{-1}$ be the change of basis matrix from S to T. If V is a complex vector space, then P and Q are unitary matrices. If V is a real vector space, then P and Q are orthogonal matrices.*

Proof. Let $S = \{s_1, \ldots, s_n\}$ and $T = \{t_1, \ldots, t_n\}$. The matrices $P = (p_{i,j})$ and $Q = (q_{i,j})$ are defined by the change of basis equations

$$t_j = \sum_{i=1}^{n} p_{i,j} s_i \qquad \text{and} \qquad s_j = \sum_{i=1}^{n} q_{i,j} t_i.$$

We have

$$\begin{aligned}
(s_i, t_j) &= \left(\sum_{k=1}^{n} q_{k,i} t_k, t_j \right) \\
&= \sum_{k=1}^{n} q_{k,i} \, (t_k, t_j) \\
&= \sum_{k=1}^{n} q_{k,i} \delta_{k,j} \\
&= q_{j,i}
\end{aligned}$$

and

$$\begin{aligned}
(s_i, t_j) &= \left(s_i, \sum_{k=1}^{n} p_{k,j} s_k \right) \\
&= \sum_{k=1}^{n} \overline{p_{k,j}} \, (s_i, s_k) \\
&= \sum_{k=1}^{n} \overline{p_{k,j}} \delta_{i,k} \\
&= \overline{p_{i,j}}.
\end{aligned}$$

Therefore,

$$q_{j,i} = \overline{p_{i,j}}$$

for all $i, j = 1, \ldots, n$, and so

$$P^{-1} = Q = \overline{P}^t = P^*.$$

Thus, P is unitary if V is complex and P is orthogonal if V is real. This completes the proof.

5.8 Spectral theory - added March 16, 2014

Let V be a real or complex inner product space, and let $T : V \to V$ be a linear operator. Let W be a T-invariant subspace of V, and let $W^\perp$ be the orthogonal complement of W. Thus,

$$T(w) \in W \qquad \text{for all } w \in W,$$

$$W^\perp = \{ v \in V : (w, v) = 0 \text{ for all } w \in W \},$$

and

$$V = W \oplus W^\perp.$$

Let T^* be the adjoint of T, that is,

$$(T(v), v') = (v, T^*(v')) \qquad \text{for all } v, v' \in V.$$

Let $w' \in W^\perp$. For all $w \in W$, we have $T(w) \in W$ and so

$$(w, T^*(w')) = (T(w), w') = 0.$$

Therefore, $T(w') \in W^\perp$, and $W^\perp$ is a T^*-invariant subspace of V. This proves the following Lemma.

Lemma 5.10. *Let V be a real or complex inner product space, and let $T : V \to V$ be a self-adjoint linear operator. If W is a T-invariant subspace of V, then $W^\perp$ is a T-invariant subspace of V.*

A spectral theorem on an inner product space asserts that a set of linear operators has a basis of eigenvectors. If $T : V \to V$ is an operator in this set, then there exists a basis for V such that the matrix of T with respect to this basis is diagonal. The eigenvalues of T are the numbers on the diagonal of the matrix, and the set of eigenvalues is called the *spectrum* of T.

Here is the *spectral theorem* for Hermitian operators.

Lemma 5.11. *Let V be a complex vector space, and let $T : V \to V$ be a Hermitian operator. Every eigenvalue of T is real.*

Proof. Let λ be an eigenvalue of T, and let $v \in V$ be an eigenvector with eigenvalue λ. Then $v \neq 0$, and

$$\lambda(v, v) = (\lambda v, v) = (T(v), v) = (v, T(v)) = (v, \lambda v) = \overline{\lambda}(v, v).$$

Dividing by $(v, v) \neq 0$, we obtain $\lambda = \overline{\lambda}$, and so λ is real. This completes the proof.

Theorem 5.8. *Let V be a finite-dimensional complex inner product space, and let T : $V \to V$ be a Hermitian operator. Then V has an orthonormal basis of eigenvectors.*

Proof. The proof is by induction on $n = \dim(V)$. If $n = 1$, then V is generated by a nonzero vector v, and $T(v) = \lambda_1 v$ for some complex number λ_1. Let $v_1 = v/\|v\|$. Then $\|v_1\| = 1$ and $T(v_1) = \lambda_1 v_1$, and so $\{v_1\}$ is an orthonormal basis of eigenvectors for V.

Let $n \geq 2$, and assume that the spectral theorem is true for Hermitian operators on vector spaces of dimension $n - 1$.

Let V be a vector space of dimension n, and let T be a Hermitian operator on V. Let $\mathscr{B}$ be a basis for V, let A be the matrix of T with respect to $\mathscr{B}$, and let $f(t) = \det(tI_n - A)$ be the characteristic polynomial of A. The Fundamental Theorem of Algebra states that every non-constant polynomial with complex coefficients has a root in $\mathbf{C}$, and so there is a complex number λ_1 such that $f(\lambda_1) = 0$. This means that λ_1 is an eigenvalue of V, and there is a nonzero vector v such that $T(v) = \lambda_1 v$. Dividing v by $\|v\|$, we obtain an eigenvector v_1 with eigenvalue λ_1 and $\|v_1\| = 1$.

Let W be the one-dimensional subspace of V that is spanned by $\{v_1\}$. Then W is a T-invariant subspace. Let $W^\perp$ be the orthogonal complement of W. Because T is

Hermitian, Lemma 5.10 implies that $W^{\perp}$ is T-invariant. Let $T^{\perp}$ be the restriction of the operator T to the $(n-1)$-dimensional vector space $W^{\perp}$. For all vectors $v, v' \in W^{\perp}$ we have

$$(T^{\perp}(v), v') = (T(v), v') = (v, T(v')) = (v, T^{\perp}(v'))$$

and so $T^{\perp}$ is a Hermitian operator on $V^{\perp}$. By the induction hypothesis, there is an orthonormal basis $\{v_2, \ldots, v_n\}$ of eigenvectors for the vector space $W^{\perp}$. Moreover, $v_1 \in W$ and $v_i \in W^{\perp}$ imply that $(v_1, v_i) = 0$ for $i = 2, \ldots, n$. Therefore, $\{v_1, v_2, \ldots, v_n\}$ is an orthonormal basis of eigenvectors for V. This completes the proof.

Theorem 5.9. *If A is a Hermitian matrix, then there exists a unitary matrix P such that $P^{-1}AP$ is diagonal.*

Proof. Let V be a complex inner product space with an orthonormal basis $\mathscr{B}$, and let T be the linear operator on V defined by the matrix A. Then T is a Hermitian operator. By the spectral theorem for Hermitian operators (Theorem 5.8), there V has an orthonormal basis $\mathscr{B}'$ of eigenvectors of T. The matrix for T with respect the basis $\mathscr{B}'$ is a diagonal matrix D. By Lemma 5.9, there is a unitary matrix P such that $D = P^{-1}DP$. This completes the proof.

Here is the *spectral theorem* for real symmetric operators.

Theorem 5.10. *Let V be a finite-dimensional real inner product space, and let $T : V \to V$ be a symmetric operator. Then V has an orthonormal basis of eigenvectors.*

Proof. Let $\dim(V) = n$, and let $\mathscr{B}$ be an orthonormal basis for V. For every vector $v \in V$, let $[v]_{\mathscr{B}}$ be the coordinate vector of v with respect to $\mathscr{B}$, and let $A = [T]_{\mathscr{B}}$ be the matrix of T with respect to $\mathscr{B}$. Then A is a real $n \times n$ matrix.

Let V' be an n-dimensional complex vector space with orthonormal basis $\mathscr{B}'$, and let T' be the linear operator whose matrix with respect to $\mathscr{B}'$ is A. The matrix A is real and symmetric, and so T' is a Hermitian operator on V'. By the Fundamental Theorem of Algebra, there exists an eigenvalue λ_1 for T'. By Lemma 5.11, the eigenvalue λ_1 is real. Let $v'_1 \in V'$ be an eigenvector for λ_1, that is, $T'(v'_1) = \lambda_1 v'_1$. The coordinate vector of v'_1 with respect to $\mathscr{B}'$ is

$$[v'_1]_{\mathscr{B}'} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}.$$

For $j = 1, \ldots, n$, we write the complex number z_j in the form $z_j = x_j + iy_j$ with $x_j, y_j \in \mathbf{R}$, and obtain

$$[v'_1]_{\mathscr{B}'} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + i \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Moreover, $v'_1 \neq 0$ implies that

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{5.5}$$

We have

$$\lambda_1 [v_1']_{\mathscr{B}'} = \lambda_1 \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \lambda_1 \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + i\lambda_1 \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

and

$$A[v_1']_{\mathscr{B}'} = A \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + iA \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Because $A[v_1']_{\mathscr{B}'} = \lambda [v_1']_{\mathscr{B}'}$, it follows that

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \lambda_1 \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad \text{and} \qquad A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \lambda_1 \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

By (5.5), at least one of the column vectors $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ is nonzero, say, $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

Consider the vector $\tilde{v_1} \in V$ defined by $[\tilde{v_1}]_{\mathscr{B}} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Then

$$[T(\tilde{v_1})]_{\mathscr{B}} = A[v]_{\mathscr{B}} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \lambda_1 \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \lambda_1 [\tilde{v_1}]_{\mathscr{B}}$$

and so $T(\tilde{v_1}) = \lambda_1 \tilde{v_1}$, that is, $\tilde{v_1}$ is an eigenvector in V with eigenvalue λ_1. It follow that $v_1 = \tilde{v_1}/\|\tilde{v_1}\|$ is an eigenvector of length 1 with eigenvalue λ_1.

Let W be the one-dimensional subspace of V spanned by $\{v_1\}$, and let $W^\perp$ be the orthogonal complement of W in V. The linear transformation T restricted to $W^\perp$ is a symmetric linear operator on $W^\perp$, and $\dim(W^\perp = n-1$. The induction hypothesis implies that $W^\perp$ has an orthonormal basis $\{v_2, \ldots, v_n\}$, and so $\{v_1, v_2, \ldots, v_n\}$ is an orthonormal basis of eigenvectors for V. The change of basis matrix P from the original orthonormal basis for V to the orthonormal basis of eigenvectors is an orthogonal matrix such that $P^{-1}AP$ is diagonal. This completes the proof.

Here is the spectral theorem for real symmetric matrices.

Theorem 5.11. *Let A be an $n \times n$ real symmetric matrix. There is an orthogonal matrix P such that $P^{-1}AP$ is diagonal.*

Proof. By induction on n.

Let T be the linear operator on $\mathbf{R}^n$ whose matrix with respect to the standard basis is A, and let T' be the linear operator on $\mathbf{C}^n$ whose matrix with respect to the standard basis is also A. By the Fundamental Theorem of Algebra, the operator T' has a eigenvalue λ with nonzero eigenvector $z = (z_1, \ldots, z_n)$. Moreover, the eigenvalue λ is real because T' is Hermitian (Lemma 5.11). For $j = 1, \ldots, n$, we write the complex number z_j in the form $z_j = x_j + iy_j$, with $x_j, y_j \in \mathbf{R}$, and so

$$\begin{aligned} z &= (z_1, \ldots, z_n) = (x_1 + iy_1, \ldots, x_n + iy_n) \\ &= (x_1, \ldots, x_n) + i(y_1, \ldots, y_n) = x + iy \end{aligned}$$

where

$$x = (x_1, \ldots, x_n) \in \mathbf{R}^n \quad \text{and} \quad y = (y_1, \ldots, y_n) \in \mathbf{R}^n.$$

Then

$$T'(x) + iT'(y) = T'(x+iy) = T'(z) = \lambda z = \lambda(x+iy) = \lambda x + i\lambda y.$$

Because $\lambda \in \mathbf{R}$, equating the real and complex parts of the vectors in the equation above gives

$$T(x) = T'(x) = \lambda x \quad \text{and} \quad T(y) = T'(y) = \lambda y.$$

Because $z \neq 0$, it follows that either $x \neq 0$ or $y \neq 0$, and so λ is an eigenvalue of the linear operator T on $\mathbf{R}^n$. Let $v_1 \in \mathbf{R}^n$ be an eigenvector for λ with $\|v_1\| = 1$, and let W be the one-dimensional subspace of $\mathbf{R}^n$ spanned by $\{v_1\}$. Let $W^\perp$ be the orthogonal complement of W. By Lemma 5.9, $W^\perp$ is invariant under T. Because $\dim(W^\perp) = n-1$, the induction hypothesis implies that there exists an orthonormal basis $\{v_2, \ldots, v_n\}$ of eigenvectors for $W^\perp$, and so $\{v_1, v_2, \ldots, v_n\}$ is an orthonormal basis of eigenvectors for V. If P is the change of basis matrix, then P is orthogonal and $P^{-1}AP$ is a diagonal matrix. This completes the proof.

5.9 Move somewhere

Lemma 5.12. *Let V be a complex inner product space. If $T : V \to V$ is a self-adjoint linear operator, then every eigenvalue of T is real.*

Proof. Let $w \in V$ be an eigenvector with eigenvalue λ. Then $\langle w, w \rangle > 0$, and

$$\lambda \langle w, w \rangle = \langle \lambda w, w \rangle = \langle T(w), w \rangle = \langle w, T(w) \rangle = \langle w, \lambda w \rangle = \overline{\lambda} \langle w, w \rangle.$$

Dividing by $\langle w, w \rangle$, we obtain $\lambda = \overline{\lambda}$, and so λ is real.

Note that this proof does not assume that V is finite-dimensional.

5.10 Rayleigh quotients and the min-max theorem

Let $T : V \to V$ be a linear operator on the vector space V. For every nonzero vector $v \in V$, we define the *Rayleigh quotient*

$$R_T(v) = \frac{\langle T(v), v\rangle}{\langle v, v\rangle}.$$

For every nonzero complex number c, we have

$$\begin{aligned} R_T(cv) &= \frac{\langle T(cv), cv\rangle}{\langle cv, cv\rangle} = \frac{\langle cT(v), cv\rangle}{\langle cv, cv\rangle} \\ &= \frac{c\bar{c}\langle T(v), v\rangle}{c\bar{c}\langle v, v\rangle} = \frac{\langle v, T(v)\rangle}{\langle v, v\rangle} \\ &= R_T(v) \end{aligned}$$

and so the Rayleigh quotient is homogeneous of degree 0.

(A real or complex-valued function $f(v)$ is homogeneous of degree k if $f(cv) = c^k f(v)$ for all $c \neq 0$.)

If $w \in V$ is an eigenvector with eigenvalue λ, then

$$R_T(w) = \frac{\langle T(w), w\rangle}{\langle w, w\rangle} = \frac{\langle \lambda w, w\rangle}{\langle w, w\rangle} = \frac{\lambda \langle w, w\rangle}{\langle w, w\rangle} = \lambda. \tag{5.6}$$

Lemma 5.13. *Let V be a finite-dimensional real or complex inner product space, $\dim(V) = n$, let $T : V \to V$ be a self-adjoint linear operator with real eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$, and let $\mathscr{B} = \{w_1, \ldots, w_n\}$ be an orthonormal basis of eigenvectors for V such that $T(w_i) = \lambda_i w_i$ for $i = 1, \ldots, n$. Let I be a nonempty subset of $\{1, \ldots, k\}$, and let W_I be the subspace of V spanned by $\{w_i : i \in I\}$. If $a = \min(I)$ and $b = \max(I)$, then*

$$\lambda_b \leq R_T(v) \leq \lambda_a$$

for all $v \in U_I \setminus \{0\}$. Moreover,

$$\max\{R_T(v) : v \in W_I \setminus \{0\}\} = \lambda_a$$

and

$$\min\{R_T(v) : v \in W_I \setminus \{0\}\} = \lambda_b.$$

Proof. Writing $v \in V \setminus \{0\}$ as a linear combination of the eigenvectors in $\{w_i : i \in I\}$, we have

$$v = \sum_{i \in I} x_i w_i$$

and

$$T(v) = \sum_{i \in I} x_i T(w_i) = \sum_{i \in I} \lambda_i x_i w_i.$$

Because

$$\langle v,v\rangle = \sum_{i\in I} x_i^2$$

and

$$\langle T(v),v\rangle = \sum_{i\in I} \lambda_i x_i^2$$

It follows that

$$\lambda_b\langle v,v\rangle = \lambda_b \sum_{i\in I} x_i^2 \leq \langle T(v),v\rangle \leq \lambda_a \sum_{i\in I} x_i^2 = \lambda_a \langle v,v\rangle$$

and so

$$\lambda_b \leq R_T(v) = \frac{\langle T(v),v\rangle}{\langle v,v\rangle} \leq \lambda_a.$$

Because $w_a, w_b \in W_I \setminus \{0\}$, identity (5.6) implies that $R_T(w_a) = \lambda_a$ and $R_T(w_b) = \lambda_b$. This completes the proof.

Corollary 5.1. *Let V be a finite-dimensional real or complex inner product space, $\dim(V) = n$, and let $T : V \to V$ be a self-adjoint linear operator with real eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Let $\mathscr{B} = \{w_1,\ldots,w_n\}$ be an orthonormal basis of eigenvectors for V such that $T(w_i) = \lambda_i w_i$ for $i = 1,\ldots,n$. If $v \in V$ and $v \neq 0$, then*

$$\lambda_n \leq R_T(v) \leq \lambda_1. \tag{5.7}$$

Moreover,

$$\sup\{R_T(v) : v \in V \setminus \{0\}\} = \lambda_1 \tag{5.8}$$

and

$$\inf\{R_T(v) : v \in V \setminus \{0\}\} = \lambda_n. \tag{5.9}$$

Proof. Inequality (5.7) follows immediately from Lemma 5.13 with $I = \{1,2,\ldots,k\}$. Identities (5.8) and (5.9) follow from the observation that $R(w_i) = \lambda_i$ for all $i \in \{1,2,\ldots,k\}$. This completes the proof.

The following result is called the *min-max theorem* or the *Courant-Fischer-Weyl theorem*.

Theorem 5.12. *Let V be a finite-dimensional real or complex inner product space, $\dim(V) = n$, and let $T : V \to V$ be a self-adjoint linear operator with real eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. For $k = 1,\ldots,n$, let $\mathscr{U}_k$ be the set of k-dimensional subspaces of V. Then*

$$\begin{aligned}\lambda_k &= \max_{U\in\mathscr{U}_k} \left(\min\left(R_T(v) : v \in U \setminus \{0\}\right)\right)\\ &= \min_{U\in\mathscr{U}_{n-k+1}} \left(\max\left(R_T(v) : v \in U \setminus \{0\}\right)\right).\end{aligned}$$

Proof. Let $\{w_1,w_2,\ldots,w_n\}$ be an orthonormal basis of eigenvectors for V such that $T(w_i) = \lambda_i w_i$ for $i = 1,\ldots,n$. For $k = 1,\ldots,n$, let $W_k \in \mathscr{U}_k$ be the subspace of V

spanned by the set $\{w_1, w_2, \ldots, w_k\}$ and let $W'_{n-k+1} \in \mathscr{U}_{n-k+1}$ be the subspace of V spanned by the set $\{w_k, w_{k+1}, \ldots, w_n\}$. Lemma 5.13 implies that

$$\min\{R_T(v) : v \in W_k \setminus \{0\}\} = \max\{R_T(v) : v \in W'_{n-k+1} \setminus \{0\}\} = \lambda_k. \tag{5.10}$$

It follows that

$$\max_{U \in \mathscr{U}_k} \left(\min\left(R_T(v) : v \in U \setminus \{0\}\right)\right) \geq \lambda_k \tag{5.11}$$

and

$$\min_{U \in \mathscr{U}_{n-k+1}} \left(\max\left(R_T(v) : v \in U \setminus \{0\}\right)\right) \leq \lambda_k. \tag{5.12}$$

If $U \in \mathscr{U}_k$, then $\dim(U) = k$ and

$$\begin{aligned}
\dim(U \cap W'_{n-k+1}) &= \dim(U) + \dim(W'_{n-k+1}) - \dim(U + W'_{n-k+1}) \\
&= k + (n-k+1) - \dim(U + W'_{n-k+1}) \\
&\geq n + 1 - n \\
&= 1
\end{aligned}$$

and so there exists a nonzero vector $v \in U \cap W'_{n-k+1}$. Identity (5.10) implies that

$$R_T(v) \leq \lambda_k$$

and so, for every subspace $U \in \mathscr{U}_k$, we have

$$\min\left(R_T(v) : v \in U \setminus \{0\}\right) \leq \lambda_k$$

and

$$\max_{U \in \mathscr{U}_k} \left(\min\left(R_T(v) : v \in U \setminus \{0\}\right)\right) \leq \lambda_k.$$

Combining this inequality with inequality (5.11) proves that

$$\max_{U \in \mathscr{U}_k} \left(\min\left(R_T(v) : v \in U \setminus \{0\}\right)\right) = \lambda_k.$$

Similarly, if $U \in \mathscr{U}_{n-k+1}$, then $\dim(U) = n - k + 1$ and

$$\begin{aligned}
\dim(U \cap W_k) &= \dim(U) + \dim(W_k) - \dim(U + W_k) \\
&= (n-k+1) + k - \dim(U + W_k) \\
&\geq n + 1 - n \\
&= 1
\end{aligned}$$

and so there exists a nonzero vector $v \in U \cap W_k$. Identity (5.10) implies that

$$R_T(v) \geq \lambda_k$$

and so, for every subspace $U \in \mathscr{U}_{n-k+1}$, we have

$$\max\left(R_T(v) : v \in U \setminus \{0\}\right) \geq \lambda_k$$

and

$$\min_{U \in \mathscr{U}_{n-k+1}} \left(\max\left(R_T(v) : v \in U \setminus \{0\}\right)\right) \geq \lambda_k.$$

Combining this inequality with inequality (5.12) proves that

$$\min_{U \in \mathscr{U}_{n-k+1}} \left(\max\left(R_T(v) : v \in U \setminus \{0\}\right)\right) = \lambda_k.$$

This completes the proof.

Exercises

1. Let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be the linear operator whose matrix with respect to the standard basis is $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.
   a. Prove that T is not self-adjoint.
   b. Prove that 0 is the only eigenvalue of T.
   c. Prove that
   $$\min(R_T(v) : v \in \mathbf{R}^2 \setminus \{0\}) = -\frac{1}{2}$$
   and
   $$\max(R_T(v) : v \in \mathbf{R}^2 \setminus \{0\}) = \frac{1}{2}.$$

   Thus, Theorem 5.12 fails for operators that are not self-adjoint.

5.11 Calculus proof of the spectral theorem for self-adjoint operators.

Let V be a finite-dimensional real or complex vector space, and let $T : V \to V$ be a self-adjoint linear operator. Because T is self-adjoint and the inner product on V is skew-symmetric, for every vector $v \in V$ we have

$$\langle T(v), v\rangle = \langle v, T(v)\rangle = \overline{\langle T(v), v\rangle}$$

and so $\langle T(v), v\rangle$ is a real-valued function of v. It follows that the Rayleigh quotient

$$R_T(v) = \frac{\langle T(v), v\rangle}{\langle v, v\rangle}$$

is also a real-valued function of v. The Rayleigh quotient is also continuous a function on $V \setminus \{0\}$. Because $R_T(v)$ is homogeneous of degree 0, for every nonzero vector v we have

$$R_T(v) = R_T\left(\frac{v}{\|v\|}\right)$$

where $v/\|v\|$ is a vector of length 1, that is, an element of the sphere S of radius 1 with center at 0. Because S is compact and a continuous real-valued function on a compact set has a minimum value, the Rayleigh quotient has a minimum value λ_1 on the unit sphere, and there exists a unit vector w_1 such that

$$\lambda_1 = R_T(w_1) = \frac{\langle T(w_1), w_1\rangle}{\langle w_1, w_1\rangle} = \langle T(w_1), w_1\rangle.$$

We shall prove that $T(w_1) = \lambda_1 w_1$, that is, we shall prove that λ_1 is an eigenvalue of T and that w_1 is an eigenvector with eigenvalue λ_1.

Let w be a nonzero vector in V. Because $w_1 \neq 0$, there exists $\delta > 0$ such that $w_1 + tw \neq 0$ for $-\delta < t < \delta$. Thus, the function

$$f(t) = R_T(w_1 + tw)$$

is defined on the open interval $-\delta < t < \delta$. Because T is self-adjoint, we have

$$\langle T(w), w_1\rangle = \langle w, T(w_1)\rangle = \overline{\langle T(w_1), w\rangle}.$$

Expanding the inner products, we obtain

$$\begin{aligned}
f(t) &= R_T(w_1 + tw) \\
&= \frac{\langle T(w_1 + tw), w_1 + tw\rangle}{\langle w_1 + tw, w_1 + tw\rangle} \\
&= \frac{\langle T(w_1), w_1\rangle + \langle T(w_1), tw\rangle + \langle T(tw), w_1\rangle + \langle T(tw), tw\rangle}{\langle w_1, w_1\rangle + \langle w_1, tw\rangle + \langle tw, w_1\rangle + \langle tw, tw\rangle} \\
&= \frac{\langle T(w_1), w_1\rangle + t(\langle T(w_1), w\rangle + \langle T(w), w_1\rangle) + t^2\langle T(w), w\rangle}{\langle w_1, w_1\rangle + t(\langle w_1, w\rangle + \langle w, w_1\rangle) + t^2\langle w, w\rangle} \\
&= \frac{\langle T(w_1), w_1\rangle + t(\langle T(w_1), w\rangle + \overline{\langle T(w_1), w\rangle}) + t^2\langle T(w), w\rangle}{\langle w_1, w_1\rangle + t(\langle w_1, w\rangle + \overline{\langle w_1, w\rangle}) + t^2\langle w, w\rangle} \\
&= \frac{\langle T(w_1), w_1\rangle + 2t\Re(\langle T(w_1), w\rangle) + t^2\langle T(w), w\rangle}{\langle w_1, w_1\rangle + 2t\Re(\langle w_1, w\rangle) + t^2\langle w, w\rangle}.
\end{aligned}$$

Thus, $f(t)$ is a quotient of quadratic polynomials. Because $f(t)$ is differentiable and has a minimum at $t = 0$, we have

$$f'(t) = 0.$$

Let $p(t)$ denote the numerator of $f(t)$ and let $q(t)$ denote the denominator of $f(t)$. By the quotient rule,

$$f'(t) = \frac{p'(t)q(t) - p(t)q'(t)}{q(t)^2}$$

We have

$$\begin{aligned}
q(t) &= \langle w_1, w_1 \rangle + 2t\Re(\langle w_1, w \rangle) + t^2 \langle w, w \rangle \\
q'(t) &= 2\Re(\langle w_1, w \rangle) + 2t\langle w, w \rangle \\
q(0) &= \langle w_1, w_1 \rangle = \|w_1\|^2 = 1 \\
q'(0) &= 2\Re(\langle w_1, w \rangle)
\end{aligned}$$

and

$$\begin{aligned}
p(t) &= \langle T(w_1), w_1 \rangle + 2t\Re(\langle T(w_1), w \rangle) + t^2 \langle T(w), w \rangle \\
p'(t) &= 2\Re(\langle T(w_1), w \rangle) + 2t\langle T(w), w \rangle \\
p(0) &= \langle T(w_1), w_1 \rangle \\
p'(0) &= 2\Re(\langle T(w_1), w \rangle).
\end{aligned}$$

Therefore,

$$\begin{aligned}
f'(0) &= \frac{p'(0)q(0) - p(0)q'(0)}{q(0)^2} \\
&= 2\Re(\langle T(w_1), w \rangle) - 2\langle T(w_1), w_1 \rangle \Re(\langle w_1, w \rangle) \\
&= 2\Re(\langle T(w_1), w \rangle) - 2\lambda_1 \Re(\langle w_1, w \rangle) \\
&= 2\Re(\langle T(w_1), w \rangle - \lambda_1 \langle w_1, w \rangle) \\
&= 2\Re(\langle T(w_1) - \lambda_1 w_1, w \rangle) \\
&= 0.
\end{aligned}$$

Because $f'(0) = 0$, we have

$$\Re(\langle T(w_1) - \lambda_1 w_1, w \rangle) = 0$$

for every vector $w \in V$. Replacing $w = u + iv$ with $iw = -v + iu$, we obtain

$$\Re(\langle T(w_1) - \lambda_1 w_1, iw \rangle) = 0$$

It follows from Lemma 5.14 that

$$\langle T(w_1) - \lambda_1 w_1, w \rangle = 0$$

for all $w \in V$, and so $T(w_1) - \lambda_1 w_1 = 0$. Thus, w_1 is an eigevector of T with eigenvalue λ_1. This completes the proof.

Lemma 5.14. *Let V be a complex inner product space, and let $w, z \in V$. If $\Re\langle z, w\rangle = \Re\langle z, iw\rangle = 0$, then $\langle z, w\rangle = 0$.*

Proof. If $\langle z, w\rangle = a + bi$, then $\langle z, iw\rangle = -i\langle z, w\rangle = b - ai$. Therefore, if $a = \Re\langle z, w\rangle = 0$ and $b = \Re\langle z, iw\rangle = 0$, then $\langle z, w\rangle = 0$.

Appendix A
Sets

A.1 Sets

In the beginning there is the primitive, undefined notion of a *set*. We must have an intuition about a "set" as a "collection" or "class" of objects that contains elements, like a vase contains flowers or a suitcase contains clothes or a piggy bank contains coins. We can axiomatize the properties of sets and their members, but we shall not define a set. We start with sets.

The set of all positive integers is $\mathbf{N} = \{1,2,3,4,\ldots\}$. We denote by $\{1,2,3,\ldots,n\}$ the set consisting of the first n positive integers, The set of nonnegative integers is $\mathbf{N}_0 = \{0,1,2,3,4,\ldots\}$. We denote by $\mathbf{Z}$ denotes the set of all integers (positive, negative, and zero), and by $\mathbf{Q}$ the set of rational numbers. The real numbers and complex numbers are denoted $\mathbf{R}$ and $\mathbf{C}$, respectively.

If S is a set, then we write $x \in S$ if x is an element of S, and we write $x \notin S$ if x is not an element of S. If $x \in S$, we also write "x is a member of the set S" or "x belongs to S." It is fundamental that a set is completely determined by its elements. Sets S and T are equal if and only if every element of S is an element of T, and every element of T is an element of S.

If every element of S is an element of T, that is, if $x \in S$ implies that $x \in T$, then S is a *subset* of T, denoted $S \subseteq T$. The set S is a *proper subset* of T is S is a subset of T and $S \neq T$. Equivalently, S is a proper subset of T if S is a subset of T and there exists an element $y \in T$ with $y \notin S$.

If S is a subset of T, then we also write that T is a *superset* of S, denoted $T \supseteq S$.

Equality of sets can be restated as follows: For any sets S and T, we have $S = T$ if and only if $S \subseteq T$ and $T \subseteq S$.

The *empty set*, denoted $\emptyset$, is the set that contains no elements. The empty set is a subset of every set, and every set is a superset of the empty set.

If S and T are sets, then the *union* of the sets S and T is the set

$$S \cup T = \{x : x \in S \text{ or } x \in T\}$$

and the *intersection* of the sets S and T is the set

$$S \cap T = \{x : x \in S \text{ and } x \in T\}.$$

Sets S and T are called *disjoint* if $S \cap T = \emptyset$.

For example, if

$$R = \{1,4,7,10\}, \quad S = \{1,3,5,7\}, \quad T = \{2,4,6,8\}$$

then

$$S \cup T = \{1,2,3,4,5,6,7,8\}$$
$$S \cap T = \emptyset$$
$$R \cap S = \{1,7\}$$
$$R \cap T = \{4\}$$
$$R \cap (S \cup T) = \{1,4,7\}$$
$$(R \cap S) \cup (R \cap T) = \{1,4,7\}$$

Theorem A.1. *If R, S, and T are sets, then*

$$R \cap (S \cup T) = (R \cap S) \cup (R \cap T) \tag{A.1}$$

and

$$R \cup (S \cap T) = (R \cup S) \cap (R \cup T). \tag{A.2}$$

Equations (A.1) and (A.2) are called the *distributive laws* of union and intersection of sets.

Proof. If $x \in R \cap (S \cup T)$, then $x \in R$ and $x \in S \cup T$. The latter inclusion implies that $x \in S$ or $x \in T$, and so $x \in R \cap S$ or $x \in R \cap T$. It follows that $x \in (R \cap S) \cup (R \cap T)$, and so

$$R \cup (S \cap T) \subseteq (R \cup S) \cap (R \cup T). \tag{A.3}$$

Conversely, if $x \in (R \cup S) \cap (R \cup T)$, then $x \in R \cup S$ and $x \in R \cup T$. If $x \notin R$, then $x \in S$ and $x \in T$, hence $x \in S \cap T$. Therefore, $x \in R \cup (S \cap T)$. Equivalently,

$$(R \cup S) \cap (R \cup T) \subseteq R \cup (S \cap T). \tag{A.4}$$

By definition of equality of sets, the set inclusions (A.3) and (A.4) imply the set identity (A.1).

The proof of (A.4) is Exercise 3.

The *complement* of the set S in T, denoted $T \setminus S$, is the set of all elements of T that do not belong to S, that is,

$$T \setminus S = \{x \in T : x \notin S\}.$$

Thus,

$$S = (S \cap T) \cup (S \setminus T)$$

and

$$(S \cap T) \cap (S \setminus T) = \emptyset.$$

A subset S of T is proper if and only if $T \setminus S \neq \emptyset$.

Let Ω be a set. If we are considering only subsets of Ω, and if $S \subseteq \Omega$, then we often denote the complement of a subset S of Ω by S^c.

Theorem A.2. *If S and T are subsets of Ω, then*

$$(S \cup T)^c = S^c \cap T^c \tag{A.5}$$

and

$$(S \cap T)^c = S^c \cup T^c. \tag{A.6}$$

Equations (A.5) and (A.6) are called *de Morgan's laws*.

Proof. We have $x \in (S \cup T)^c$ if and only if $x \notin S \cup T$ if and only if $x \notin S$ and $x \notin T$ if and only if $x \in S^c$ and $x \in T^c$ if and only if $x \in S^c \cap T^c$. This proves (A.5).

The proof of (A.6) is Exercise 4.

The *symmetric difference* of the sets A and B is the set

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

We have $x \in A \Delta B$ if and only if $x \in A \cup B$ and $x \notin A \cap B$, and so

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

Let I be a set. For each $i \in I$, let S_i be a set. We call these sets a *family* of sets indexed by I, and denote the family by $(S_i)_{i \in I}$. We define the union and intersection of the sets in $(S_i)_{i \in I}$ as follows:

$$\bigcup_{i \in I} S_i = \{s : s \in S_i \text{ for some } i \in I\}$$

and

$$\bigcap_{i \in I} S_i = \{s : s \in S_i \text{ for all } i \in I\}.$$

We adopt the convention that if $I = \emptyset$, then $\bigcup_{i \in I} S_i = \emptyset$ and $\bigcap_{i \in I} S_i = X$.

If X is a set and if S_i is a subset of X for every $i \in I$, then we call $(S_i)_{i \in I}$ a family of subsets of X, indexed by I.

Exercises

1. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 3, 5, 7, 9\}$, and $C = \{2, 6, 10, 14\}$.

a. Compute the following sets:

$$A \cup B, \quad A \cap B, \quad B \cup C, \quad B \cap C, \quad A \setminus B, \quad B \setminus A.$$

b. Compute the following sets:

$$A \cap (B \cup C), \quad (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C), \quad (A \cup B) \cap (A \cup C).$$

2. Prove that union and intersection are associative operations on sets. Thus, for any sets A, B, and C, prove that

$$(A \cup B) \cup C = A \cup (B \cup C)$$

and

$$(A \cap B) \cap C = A \cap (B \cap C)$$

3. Prove that, for any sets A, B, and C,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

4. Prove that, for any sets S and T,

$$(S \cap T)^c = S^c \cup T^c.$$

5. Prove that

$$A \subseteq (A \cap B \cap C) \cup (A \setminus B) \cup (A \setminus C).$$

6. Let A, B, C be sets. Prove the following properties of the symmetric difference:

a.

$$A \Delta A = \emptyset$$

b.

$$A \Delta B = B \Delta A$$

c.

$$(C \setminus A) \Delta (C \setminus B) = A \Delta B$$

d.

$$(A \Delta B) \Delta C = A \Delta (B \Delta C)$$

e.

$$(A \Delta C) \Delta (B \Delta C) = A \Delta B$$

A.2 The minimum principle and mathematical induction

There are two equivalent principles that we use to prove theorems in algebra and number theory. They are the minimum principle and the principle of mathematical induction.

Let X be a set of integers. This set is *bounded below* if there is an integer L such that $L \leq n$ for all $n \in X$. The set X *contains a smallest element* if there exists an integer $n_0 \in X$ such that $n_0 \leq n$ for all $n \in X$. A smallest element is unique. The *minimum principle* states: Every nonempty set of integers that is bounded below contains a smallest element. In particular, every nonempty set of nonnegative integers contains a smallest element.

Note that the minimum principle is not true for sets of rational numbers. For example, the set $\{x \in \mathbf{Q} : 0 < x < 1\}$ is nonempty and bounded below by 0, but does not contain a smallest element.

The *principle of mathematical induction* states: Let X be a set of integers. If $n_0 \in X$ and if $n \in X$ implies that $n+1 \in X$, then X contains all integers $n \geq n_0$.

We often use the principle of mathematical induction in the following form: Let $S(n)$ be a statement about the integer n. If $S(n_0)$ is true and if, for each integer $n \geq n_0$, the truth of $S(n)$ implies the truth of $S(n+1)$, then $S(n)$ is true for all integers $n \geq n_0$

Theorem A.3. *The minimum principle and the principle of mathematical induction are equivalent.*

Proof. Assume the minimum principle. Let X be a set of integers such that (i) $n_0 \in X$, and (ii) if $n \in X$ then $n+1 \in X$. Let X' be the set of all integers $n \geq n_0$ such that $n \notin X$. We must prove that $X' = \emptyset$. If $X' \neq \emptyset$, then X' is a nonempty set of integers that is bounded below by n_0. By the minimum principle, X' contains a smallest element n_1. By (i), $n_0 \in X$, and so $n_1 \neq n_0$. Therefore, $n_1 > n_0$. It follows that $n_1 - 1 \notin X'$, and so $n_1 - 1 \in X$. Because $n_0 \leq n_1 - 1 < n_1$, condition (ii) implies that $n_1 \in X$, and this contradicts $n_1 \in X'$. This contradiction implies that the set X' is empty. Thus, the minimum principle implies the principle of mathematical induction.

Conversely, assume the principle of mathematical induction. Let X be a nonempty set of integers that is bounded below. Then there exists an integer n_0 such that $n_0 < x$ for all $x \in X$. Suppose that X does not contain a smallest element. Let X' be the set of all integers $n \geq n_0$ such that $n < x$ for all $x \in X$. By the discreteness property of $\mathbf{Z}$, we have $n+1 \leq x$ for all $x \in X$. If $n+1 \in X$, then $n+1$ is the smallest element in X. If X does not contain a smallest element, then $n+1 \in X'$. It follows that if X does not contain a smallest element, then $n \geq n_0$ and $n \in X'$ imply that $n+1 \in X'$. By the principle of mathematical induction, X' contains all integers $n \geq n_0$. Because the sets X and X' are disjoint, it follows that X is empty, which contradicts the hypothesis that X is nonempty. Therefore, X must contain a smallest element. This completes the proof.

Here are examples of the use of mathematical induction.

The nth odd positive integer is $2n-1$. Consider sums of the first n odd positive integers. For $n = 1$, the first odd positive integer is 1 and

$$1 = 1^2.$$

For $n = 2$, the first two odd positive integers are 1 and 3, and

$$1 + 3 = 4 = 2^2.$$

For $n = 3$, the first three odd positive integers are 1, 3, and 5, and

$$1 + 3 + 5 = 9 = 3^2.$$

For $n = 4$, the first three odd positive integers are 1, 3, 5, and 7, and

$$1 + 3 + 5 + 7 = 16 = 4^2.$$

We can use mathematical induction to generalize this "experimental data."

Theorem A.4. *The sum of the first n odd positive integers is n^2.*

Proof. The proof is by induction on n. Let $n \geq 1$, and assume that the Theorem is true for the sum of the first n odd positive integers. This means that

$$1 + 3 + \cdots + (2n - 1) = n^2$$

and so the sum of the first $n+1$ odd positive integers is

$$1 + 3 + \cdots + (2n - 1) + (2(n + 1) - 1) = n^2 + (2n + 1) = (n + 1)^2.$$

This completes the induction.

Let X be a finite set, $\mathrm{card}(X) = n$, and let $\mathscr{P}(X)$ be the power set of X. If $n = 0$, then $X = \emptyset$ is the empty set, and the only subset of the empty set is the empty set, that is, $\mathscr{P}(\emptyset) = \{\emptyset\}$ and $\mathrm{card}(\mathscr{P}(X)) = 1 = 2^0$. If $n = 1$ and $X = \{x_1\}$, then

$$\mathscr{P}(X) = \{\emptyset, \{x_1\}\} \quad \text{and} \quad \mathrm{card}(\mathscr{P}(X)) = 2 = 2^1.$$

If $n = 2$ and $X = \{x_1, x_2\}$, then

$$\mathscr{P}(X) = \{\emptyset, \{x_1\}, \{x_2\}, X\} \quad \text{and} \quad \mathrm{card}(\mathscr{P}(X)) = 4 = 2^2.$$

If $n = 3$ and $X = \{x_1, x_2, x_3\}$, then

$$\mathscr{P}(X) = \{\emptyset, \{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}, X\}$$

and

$$\mathrm{card}(\mathscr{P}(X)) = 8 = 2^3.$$

We use mathematical induction to extend these observations.

Theorem A.5. *If $\mathrm{card}(X) = n$, then $\mathrm{card}(\mathscr{P}(X)) = 2^n$.*

Proof. We have already proved this for $n = 0, 1, 2$, and 3. Assume the Theorem holds for the nonnegative integer n, and let X be a finite set with $\mathrm{card}(X) = n+1$. Then $X \neq \emptyset$. Choose an element $x^* \in X$, and let $X' = X \setminus \{x^*\}$.

If A is a subset of X, then either $x^* \notin A$ or $x^* \in A$. If $x^* \notin A$, then A is a subset of X'. Because $\mathrm{card}(X') = \mathrm{card}(X) - 1 = n$, the induction hypothesis implies that $\mathrm{card}(\mathscr{P}(X')) = 2^n$. If $x^* \in A$, then $A' = A \setminus \{x^*\}$ is a subset of X'. Moreover, if A' and A'' are distinct subsets of X', then $A' \cup \{x^*\}$ and $A'' \cup \{x^*\}$ are distinct subsets of X that contain x^*. It follows that there are exactly $\mathscr{P}(X') = 2^n$ subsets of X that contain x^*, and so $\mathscr{P}(X) = 2^n + 2^n = 2^{n+1}$. This completes the proof.

Here is another example of a proof that uses mathematical induction. A *semigroup* is a nonempty set with an associative binary operation. Let X be a semigroup, and denote the binary operation on X by multiplication. For every $x \in X$ and for every positive integer k, we define the powers of x inductively:

$$
\begin{aligned}
x^1 &= x \\
x^2 &= xx \\
x^3 &= x^2x = (xx)x \\
x^4 &= x^3x = (x^2x)x = ((xx)x)x.
\end{aligned}
$$

and, for all integers $k \geq 4$

$$x^{k+1} = x^k x. \tag{A.7}$$

Because multiplication is associative, we have

$$xx^2 = x(xx) = (xx)x = x^2x = x^3$$

and

$$x^2x^2 = x^2(xx) = (x^2x)x = x^3x = x^4.$$

The following theorem extends these observations.

Lemma A.1. *Let X be a semigroup, and let $x \in X$. If $k, \ell \in \mathbf{N}$, then*

$$x^k x^\ell = x^{k+\ell}.$$

Proof. By induction on ℓ. If $\ell = 1$, then

$$x^k x^1 = x^{k+1}$$

by definition (A.7). If $\ell \geq 2$ and the Theorem holds for $\ell - 1$, then

$$x^k x^\ell = x^k \left(x^{\ell-1} x\right) = \left(x^k x^{\ell-1}\right) x = \left(x^{k+\ell-1}\right) x = x^{k+\ell}.$$

This completes the proof.

Exercises

1. Use mathematical induction to prove that
$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$
2. Use mathematical induction to prove that
$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$
3. Use mathematical induction to prove that
$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2.$$
4. Let X be a finite set with $\mathrm{card}(X) = n$. Prove that there are 2^{n-1} subsets of X that contain an even number of elements.
5. Let n and k be nonnegative integers, and let $C(n,k)$ denote the number of subsets of cardinality k contained in a set of cardinality n. The integer $C(n,k)$ is called the *binomial coefficient*. We also refer to the binomial coefficient $C(n,k)$ as "n choose k". Note that $C(n,k) = 0$ if $k > n$, and $C(n,0) = 1$ for all $n \geq 0$.

   a. Prove that $C(n,1) = n$ and $C(n,n) = 1$.
   b. Prove that $C(n,2) = n(n-1)/2$.
   c. Prove that if $1 \leq k \leq n$, then
   $$C(n,k) = C(n-1,k-1) + C(n-1,k).$$
   d. Prove that if k_1, k_2, n_1, and n_2 are nonnegative integers such that $k_1 + k_2 = k$ and $n_1 + n_2 = n$, then
   $$C(n,k) = \sum_{k_1+k_2=n} C(n_1,k_1)C(n_2,k_2).$$
   e. Let $r \geq 2$. Prove that if $k_1,\ldots,k_r$ and $n_1,\ldots,n_r$ are nonnegative integers such that $k_1 + \cdots + k_r = k$ and $n_1 + \cdots + n_r = n$, then
   $$C(n,k) = \prod_{i=1}^{r} C(n_i,k_i).$$
   f. Prove that
   $$\sum_{k=0}^{n} C(n,k) = 2^n.$$

6. Apply the minimum principle to prove that every positive integer is interesting.
   Hint: Consider the set of uninteresting positive integers. If this set is nonempty, then its smallest element is interesting because it is the smallest uninteresting number.

A.3 Functions

A function from the set X to the set Y is a relation $f \subseteq X \times Y$ such that for every element $x \in X$ there is one and only one element $y \in Y$ with $(x,y) \in f$. We write $f(x) = y$ if $(x,y) \in f$, and denote the function by $f : X \to Y$.

For example, if X is a set, then the *identity function* is the function $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$ for all $x \in X$.

The set X is called the *domain* of the function f, and the set Y is called the *range* of f. The *image* of f is the set

$$f(X) = \{f(x) : x \in X\} = \{y \in Y : y = f(x) \text{ for some } x \in X\}.$$

Let X' be a subset of X. The image of X' in Y with respect to the function f is the set

$$f(X') = \{y \in Y : y = f(x') \text{ for some } x' \in X'\}.$$

Let Y' be a subset of Y. The *inverse image* of Y' in X with respect to the function f is the set

$$f^{-1}(Y') = \{x \in X : f(x) \in Y'\}.$$

The function $f : X \to Y$ is *one-to-one* if, for all $x_1, x_2 \in X$, the condition $f(x_1) = f(x_2)$ implies that $x_1 = x_2$. A one-to-one function is also called an *injection* or a *monomorphism*.

The function $f : X \to Y$ is *onto* if for every $y \in Y$ there exists $x \in X$ such that $f(x) = y$. An onto function is also called a *surjection* or an *epimorphism*.

The function $f : X \to Y$ is *one-to-one and onto* if it is both one-to-one and onto. A one-to-one and onto function is also called a *bijection* and a *set isomorphism*.

For example, the identity function $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$ for all $x \in X$ is a one-to-one and onto function.

If $f : X \to Y$ is one-to-one and onto, then for each $y \in Y$ there is a unique $x \in X$ such that $f(x) = y$. We define the function $g : Y \to X$ by $g(y) = x$, where x is the unique element of X such that $f(x) = y$. Then $gf = \mathrm{id}_X$ and $fg = \mathrm{id}_Y$. We call g the *inverse function* of f, and denote it by f^{-1}.

Let X, Y, and Z be sets, and let $f : X \to Y$ and $g : Y \to Z$ be functions. We define the composite function $g \circ f : X \to Z$ by

$$(g \circ f)(x) = g(f(x))$$

for all $x \in X$.

If the functions $f : X \to Y$ and $g : Y \to Z$ are one-to-one, then the composite function $gf : X \to Z$ is one-to-one (Exercise 6a). If the functions $f : X \to Y$ and $g : Y \to Z$ are onto, then the composite function $gf : X \to Z$ is onto (Exercise 6b). It follows that if $f : X \to Y$ and $g : Y \to Z$ are one-to-one and onto functions, then the composite function $gf : X \to Z$ is also one-to-one and onto.

A *permutation* of a nonempty set X is a one-to-one and onto function form X to itself. For example, the identity function $\mathrm{id}_X : X \to X$ is a permutation. If $\sigma : X \to X$ is a permutation, then σ is invertible and $\sigma^{-1} : X \to X$ is a permutation. If $\sigma : X \to X$ and $\tau : X \to X$ are permutations, then their composition $\sigma\tau : X \to X$ is a permutation. We denote by the set of all permutations of X $\mathrm{Perm}(X)$ or $\mathrm{Sym}(X)$. A permutation of X is also called an *automorphism* of X.

We say the sets X and Y *have the same cardinality* or *have the same number of elements* if there exists a function $f : X \to Y$ that is one-to-one and onto. We denote this by $|X| = |Y|$.

Theorem A.6. *Let X, Y, Z, and W be sets, and let $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$ be functions. Then $(h \circ g) \circ f$ and $h \circ (g \circ f)$ are functions from X to W, and*

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Equivalently, composition of functions is associative.

Proof. We have $f : X \to Y$ and $h \circ g : Y \to Z$, hence $(h \circ g) \circ f$ is a function from X to W. Similarly, $h \circ (g \circ f)$ is a function from X to W. Moreover,

$$\begin{aligned} ((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) = h(g(f(x))) \\ &= h((g \circ f)(x)) = (h \circ (g \circ f))(x). \end{aligned}$$

This completes the proof.

Consider functions $f : X \to Y$ and $g : Y \to X$. The function g is the *inverse* of the function f if $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. Note that if g is the inverse of f, then f is the inverse of g. We denote the inverse of f by f^{-1}.

The function $f : X \to Y$ is called *invertible* if there exists a function $g : Y \to X$ such that $g = f^{-1}$.

Theorem A.7. *The function $f : X \to Y$ is invertible if and only if f is one-to-one and onto.*

Proof. Let $f : X \to Y$ be a function that is one-to-one and onto. Define a function $g : Y \to X$ as follows: Let $y \in Y$. Because f is onto, there exists $x \in X$ such that $f(x) = y$. If $x_1, x_2 \in X$ satisfy $f(x_1) = y$ and $f(x_2) = y$, then $f(x_1) = f(x_2)$. Because f is one-to-one, it follows that $x_1 = x_2$, and so there exists a unique $x \in X$ such that $f(x) = y$. We define $g(y) = x$. Then $g : Y \to X$ is a function that satisfies $f \circ g(y) = f(g(y)) = y$ and $g \circ f(x) = g(f(x)) = x$, that is, f is invertible and $f^{-1} = g$.

Conversely, suppose that f is invertible and $g = f^{-1}$. If $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$, then

$$x_1 = \mathrm{id}_X(x_1) = g \circ f(x_1) = g(f(x_1)) = g(f(x_2)) = g \circ f(x_2) = \mathrm{id}_X(x_2) = x_2$$

and so f is one-to-one. Similarly, if $y \in Y$, then

$$y = \mathrm{id}_Y(y) = f \circ g(y) = f(g(y))$$

and so f is onto. This completes the proof.

Let $f : X \to Y$ be a function and let W be a subset of X. The function $f|_W : W \to Y$ defined by

$$f|_W(w) = f(w)$$

for all $w \in W$ is called the *restriction* of f to W.

The set X is *finite* if $X = \emptyset$ or if, for some positive integer n, there exists a one-to-one and onto function $f : X \to \{1, 2, \ldots, n\}$. The *cardinality* of a finite set X, denoted $|X|$, is n if there exists a bijection $f : X \to \{1, 2, \ldots, n\}$. The cardinality of the empty set is 0.

The set X is *infinite* if there exist a subset X' of X and a one-to-one and onto function $f : X' \to \mathbf{N}$. We write $|X| = \infty$ is X is an infinite set.

The *power set* of the set X is the set $\mathscr{P}(X)$ whose elements are the subsets of X. For example, if $X = \{a, b, c\}$, then

$$\mathscr{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, X\}.$$

and $\mathscr{P}(X) = 8$. In general, if X is a finite set with cardinality n, then $|\mathscr{P}(X)| = 2^n$ (Exercise 1).

Exercises

1. Prove that if X is a finite set with $|X| = n$, then $|\mathscr{P}(X)| = 2^n$.
2. Define the functions $f, g, h : \mathbf{R} \to \mathbf{R}$ by

$$f(t) = \frac{2t+1}{3t+2}$$

$$g(t) = \frac{5t-6}{-4t+5}$$

$$h(t) = \frac{t+2}{t+3}$$

   a. Compute the composite functions

$$f \circ g \qquad \text{and} \qquad g \circ f.$$

   Does $f \circ g = g \circ f$?

   b. Compute the composite functions

$$(f \circ g) \circ h, \qquad \text{and} \qquad f \circ (g \circ h)$$

Does $(f \circ g) \circ h = f \circ (g \circ h)$?

3. Prove that the inverse of an invertible function is unique. Equivalently, prove that if the functions $f : X \to Y$, $g : Y \to X$, and $h : Y \to X$ satisfy $g \circ f = h \circ f = \mathrm{id}_X$ and $f \circ g = f \circ h = \mathrm{id}_Y$, then $g = h$.
4. Prove that the function $f : X \to Y$ is one-to-one if and only if there exists a function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$.
5. Prove that the function $f : X \to Y$ is onto if and only if there exists a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$.
6. a. Prove that if the functions $f : X \to Y$ and $g : Y \to Z$ are one-to-one, then the composite function $gf : X \to Z$ is one-to-one.
   b. Prove that if the functions $f : X \to Y$ and $g : Y \to Z$ are onto, then the composite function $gf : X \to Z$ is onto.
7. Prove that if $f : X \to Y$ is onto, then there exists a subset W of X such that f_W is one-to-one and onto.
8. Let X be a nonempty set, and let $f : X \to X$ be a function. For every nonnegative integer n, the *nth-iterate* of f is the function $f^n : X \to X$ defined inductively as follows: For all $x \in X$,

$$\begin{aligned} f^0(x) &= \mathrm{id}_X(x) = x \\ f^1(x) &= f(x) \\ f^2(x) &= f \circ f(x) \\ f^{n+1}(x) &= f \circ f^n(x) \qquad \text{for all } n \geq 2. \end{aligned}$$

   a. Prove that $f^m \circ f^n = f^{m+n}$ for all nonnegative integers m and n.
   b. Prove that if $f^n = \mathrm{id}_X$ for some positive integer n, then f is a bijection, and $f^{-1} = f^{n-1}$.
   c. The function $f : X \to X$ is an *involution* if $f^2 = \mathrm{id}_X$. Prove that the function $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = -x$ is an involution.
   d. A *rational function* with real coefficients is a quotient of polynomials with real coefficients. If $F(t)$ is a rational function, then there exist polynomials $R(t)$ and $S(t)$ with $S(t) \neq 0$ such that $F(t) = R(t)/S(t)$. Let X be the set of nonzero rational functions. Prove that the function $\Phi : X \to X$ defined by

$$\Phi(F(t)) = \frac{1}{F\left(\frac{1}{t}\right)}$$

   is an involution.

9. The function $f : X \to X$ has *order* k if $f^k = \mathrm{id}_X$ and $f^i \neq \mathrm{id}_X$ for $i = 1, \ldots, k-1$. Compute the orders of the following functions:

   a. $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = -x$.
   b. $f : \mathbf{R}^* \to \mathbf{R}^*$ defined by $f(x) = 1/x$.

c. $f : \mathbf{C} \to \mathbf{C}$ defined by $f(z) = \zeta z$, where $\zeta = \cos 2\pi/3 + i \sin 2\pi/3$..

10. Let $\mathbf{Z}^5 = \{(x_1, x_2, x_3, x_4, x_5) : x_1, x_2, x_3, x_4, x_5) \in \mathbf{Z}\}$.

    a. Define $f : \mathbf{Z}^5 \to \mathbf{Z}^5$ by $f(x_1, x_2, x_3, x_4, x_5) = (-x_2, x_{1,3}, x_4, x_5)$.
    b. Define $f : \mathbf{Z}^5 \to \mathbf{Z}^5$ by $f(x_1, x_2, x_3, x_4, x_5) = (x_3, x_1, x_2, x_4, x_5)$.
    c. Define $f : \mathbf{Z}^5 \to \mathbf{Z}^5$ by $f(x_1, x_2, x_3, x_4, x_5) = (x_4, x_1, x_2, x_3, x_5)$.
    d. Define $f : \mathbf{Z}^5 \to \mathbf{Z}^5$ by $f(x_1, x_2, x_3, x_4, x_5) = (x_5, x_1, x_2, x_3, x_4)$.
    e. Define $f : \mathbf{Z}^5 \to \mathbf{Z}^5$ by $f(x_3, x_1, x_2, x_5, x_4)$.

11. Let $f : \mathbf{R}^2 \to \mathbf{R}$ be a function such that $f(x,y) = f(y,x) = f(-x,y)$ for all $x, y \in \mathbf{R}$. Prove that $f(x,y) = f(x,-y) = f(-x,-y)$ for all $x, y \in \mathbf{R}$.
12. Define the function $f : \mathbf{R}^2 \to \mathbf{R}$ by

$$f(x,y) = \max(|x|, |y|).$$

    a. Prove that $f(x,y) = f(y,x) = f(-x,y)$ for all $x, y \in \mathbf{R}$.
    b. Prove that $f(x,y) \geq 0$ for all $x, y \in \mathbf{R}$.
    c. Prove that $f(x,y) = 0$ if and only if $x = y = 0$.
    d. Prove that

$$f(x,y) \leq \max(f(x,z), f(y,z)) \leq f(x,z) + f(z,y)$$

    for all $x, y, z \in \mathbf{R}$.

13. Define the function $f : \mathbf{R}^2 \to \mathbf{R}$ by

$$f(x,y) = |x| + |y| - |x - y|.$$

    a. Prove that

$$f(x,y) = \begin{cases} 2\min(|x|, |y|) & \text{if } xy > 0 \\ 0 & \text{if } xy \leq 0. \end{cases}$$

    b. Prove that

$$f(x,y) \geq \min(f(x,z), f(y,z))$$

    for all $x, y, z \in \mathbf{R}$.

A.4 Equivalence relations and partitions of sets

Let S and T be sets. The *product* of S and T is the set

$$S \times T = \{(s,t) : s \in S \text{ and } t \in T\}.$$

Thus, $S \times T$ is the set of ordered pairs whose first coordinate is in S and whose second coordinate is in T. The set $S \times T$ is sometimes called the *Cartesian product* of the sets S and T. Note that $S \times T$ is nonempty if and only if both S and T are nonempty sets.

The product of a finite family of sets $(S_i)_{i=1}^n$ is the set

$$S_1 \times \cdots \times S_n = \{(s_1, \ldots, s_n) : s_i \in S_i \text{ for all } i = 1, \ldots, n\}.$$

Thus, the product is the set of all n-tuples whose ith coordinate belongs to S_i for all $i = 1, \ldots, n$. We also denote the product by $\prod_{i \in I} S_i$.

If $S = T$, then we write

$$S^2 = S \times S = \{(s_1, s_2) : s_1, s_2 \in S\}.$$

For example, if $\mathbf{R}$ is the set of real numbers, then $\mathbf{R}^2$ is the ordinary Euclidean plane.

A *relation* on sets X and Y is a subset $\mathscr{R}$ of $X \times Y$. A *relation* on X is is a subset $\mathscr{R}$ of X^2. For example, if $X = \mathbf{R}$, then

$$\mathscr{R}_< = \{(x, y) \in \mathbf{R}^2 : x < y\}$$

is the relation "less than" between real numbers, and

$$\mathscr{R}_\leq = \{(x, y) \in \mathbf{R}^2 : x \leq y\}$$

is the relation "less than or equal to" between real numbers

If $\mathscr{R}$ is a relation on the set X and $x, y \in S$, then we often write $x \sim_R y$ or, simply, $x \sim y$ to indicate that $(x, y) \in \mathscr{R}$.

Let S be a set. A family $(S_i)_{i \in I}$ of subsets of S is *pairwise disjoint* if $S_i \cap S_j = \emptyset$ for all $i, j \in I$ with $i \neq j$. A *partition* of a set S is a family $(S_i)_{i \in I}$ of pairwise disjoint subsets of S such that $\bigcup_{i \in I} S_i = S$.

If $f : S \to T$ is a function, and if $f(S)$ is the image of S, then

$$f^{-1}(t) = \{s \in S : f(s) = t\}$$

is a nonempty subset of S. If $t_1, t_2 \in f(S)$ and $t_1 \neq t_2$, then $f^{-1}(t_1) \cap f^{-1}(t_2) = \emptyset$. Moreover, if $s \in S$ and $t = f(s)$, then $s \in f^{-1}(t)$. It follows that $\{f^{-1}(t) : t \in f(S)\}$ is a partition of S into pairwise disjoint nonempty sets.

Let S be a set and let $s_1, s_2, s_3 \in S$. A relation on S is *reflexive* if $s \sim s$ for all $s \in S$. A relation on S is *symmetric* if $s_1 \sim s_2$ implies that $s_2 \sim s_1$. A relation on S is *transitive* if $s_1 \sim s_2$ and $s_2 \sim s_3$ imply that $s_1 \sim s_3$.

An *equivalence relation* on the set S is a relation that is reflexive, symmetric, and transitive.

The simplest example of an equivalence relation is equality. On any set X, define the relation $x \sim y$ if and only if $x = y$. Equality is reflexive, symmetric, and transitive.

By contrast, on the set of real numbers, the relation $\mathscr{R}_<$ is transitive but neither reflexive not symmetric, and the relation $\mathscr{R}_\leq$ is reflexive and transitive but not symmetric.

In plane geometry, congruence of triangles is an equivalence relation, and similarity of triangles is an equivalence relation.

Let $\mathbf{Z}$ be the set of integers. Consider the relation

$$\mathscr{R}_2 = \{(a,b) \in \mathbf{Z}^2 : a-b \text{ is divisible by } 2\}.$$

Let $a,b,c \in \mathbf{Z}$. The integer 0 is divisible by 2 (because $0 = 2 \cdot 0$), and so $0 = a-a$ is divisible by 2. Thus, $a \sim a$ and $\mathscr{R}_2$ is a reflexive relation. If $a \sim b$, then $a-b$ is divisible by 2, that is, $a-b = 2x$ for some $x \in \mathbf{Z}$, and so $b-a = 2(-x)$ and $b \sim a$. Thus, the relation $\mathscr{R}_2$ is symmetric. If $a \sim b$ and $b \sim c$, then there exist integers x and y such that

$$a-b = 2x$$

and

$$b-c = 2y.$$

Adding these equations, we obtain

$$a-c = 2(x+y)$$

and so $\mathscr{R}_2$ is transitive. It follows that $\mathscr{R}_2$ is an equivalence relation.

More generally, for every positive integer m, the relation

$$\mathscr{R}_m = \{(a,b) \in \mathbf{Z}^2 : a-b \text{ is divisible by } m\}$$

is an equivalence relation. (Exercise 1).

Let $W = \{(a,b) \in \mathbf{Z}^2 : b \neq 0\}$. We define a relation $\mathscr{F}$ on W as follows: If $(a,b),(c,d) \in W$, then $(a,b) \sim (c,d)$ if

$$ad = bc.$$

Thus,

$$\mathscr{F} = \{((a,b),(c,d))\} \in W^2 : ad = bc\}.$$

Let $(a,b),(c,d),(e,f) \in W$. Because $ab = ba$, it follows that $((a,b),(a,b))\} \in \mathscr{F}$ and so $\mathscr{F}$ is reflexive.

If $(a,b) \sim (c,d)$, then $ad = bc$ and so $cb = da$. Therefore, $(c,d) \sim (a,b)$ and the relation $\mathscr{F}$ is symmetric. If $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$, then $ad = bc$ and $cf = de$. Multiplying the first equation by f and the second equation by b, we obtain

$$adf = bcf = bde.$$

Therefore,

$$0 = adf - bde = (af - be)d$$

Because $d \neq 0$, we can divide by d and obtain

$$af = be.$$

Therefore, $(a,b) \sim (e,f)$ and the relation $\mathscr{F}$ is transitive. Thus, $\mathscr{F}$ is an equivalence relation. Note that the proof uses only the simplest properties of addition and multiplication, and the fact that the product of two integers is 0 if and only if at least one of the factors is 0.

Let K denote either the set $\mathbf{Q}$ of rational numbers or the set $\mathbf{R}$ of real numbers, and let

$$L = K^3 \setminus \{(0,0,0)\}$$

be the set of all nonzero triples of elements of K. Because the product of two nonzero numbers in K is nonzero, it follows that if $(x,y,z) \in L$ and $t \in K \setminus \{0\}$, then

$$t(x,y,z) = (tx,ty,tz) \in L.$$

We define a relation $\mathscr{P}^2(K)$ on L as follows: $(x_1,y_1,z_1) \sim (x_2,y_2,z_2)$ if there is a nonzero number t in K such that

$$(x_2,y_2,z_2) = t(x_1,y_1,z_1).$$

Thus,

$$\mathscr{P}^2(K) = \big\{((x_1,y_1,z_1),(x_2,y_2,z_2)) \in L^2 : (x_2,y_2,z_2) = t(x_1,y_1,z_1) \\ \text{for some } t \in K \setminus \{0\}\big\}.$$

Let $(x_1,y_1,z_1),(x_2,y_2,z_2),(x_3,y_3,z_3) \in \mathscr{P}^2(K)$. Because $(x_1,y_1,z_1) = 1 \cdot (x_1,y_1,z_1)$ and $1 \neq 0$, it follows that $(x_1,y_1,z_1) \sim (x_1,y_1,z_1)$ and the relation $\mathscr{P}^2(K)$ is reflexive.

If $t \in K$ is nonzero, then $t^{-1} \in K$ is also nonzero. Thus, if $(x_1,y_1,z_1) \sim (x_2,y_2,z_2)$, then $(x_2,y_2,z_2) = t(x_1,y_1,z_1)$ for some $t \in K \setminus \{0\}$, and so $(x_1,y_1,z_1) = t^{-1}(x_2,y_2,z_2)$. Therefore, $(x_2,y_2,z_2) \sim (x_1,y_1,z_1)$ and $\mathscr{P}^2(K)$ is symmetric.

Suppose that $(x_1,y_1,z_1) \sim (x_2,y_2,z_2)$ and $(x_2,y_2,z_2) \sim (x_3,y_3,z_3)$. There exist nonzero numbers $t,u \in K \setminus \{0\}$ such that $(x_2,y_2,z_2) = t(x_1,y_1,z_1)$ and $(x_3,y_3,z_3) = u(x_2,y_2,z_2)$. It follows that

$$(x_3,y_3,z_3) = u(x_2,y_2,z_2) = ut(x_1,y_1,z_1)$$

and ut is nonzero (because the product of nonzero numbers is nonzero). This proves the transitivity of the relation $\mathscr{P}^2(K)$, and so $\mathscr{P}^2(K)$ is an equivalence relation.

Here is an example of a geometrical equivalence relation. Let T be the set of triangles in the plane. The relation $\Delta_1 \sim \Delta_2$ if Δ_1 and Δ_2 are congruent triangles is an equivalence relation

Let $(S_i)_{i \in I}$ be a partition of the set S. Associated with this partition is the relation

$$\mathscr{R} = \{(s_1,s_2) \in S^2 : \text{there exists } i \in I \text{ such that } s_1,s_2 \in S_i\}.$$

This is an equivalence relation (Exercise 2).

Conversely, associated with every equivalence relation on a set S is a partition of S. Let $\mathscr{R}$ be an equivalence relation on S. For every $s \in S$, the *equivalence class* of s is the set

$$\bar{s} = \{s' \in s : s \sim s'\}.$$

Because an equivalence relation is reflexive, we have $s \sim s$ and so $s \in \overline{s}$. Thus, $\overline{s} \neq \emptyset$ for all $s \in S$.

Suppose that $s_1, s_2 \in S$ and $\overline{s_1} \cap \overline{s_2} \neq \emptyset$. Then there exists $t \in S$ such that $s_1 \sim t$ and $s_2 \sim t$. Because an equivalence relation is symmetric, we have $t \sim s_2$. Because an equivalence relation is transitive, the conditions $s_1 \sim t$ and $t \sim s_2$ imply that $s_1 \sim s_2$. If $s \in \overline{s_2}$, then $s_2 \sim s$ and, by transitivity, $s_1 \sim s$. Therefore, $\overline{s_2} \subseteq \overline{s_1}$. Similarly, $\overline{s_1} \subseteq \overline{s_2}$. It follows that if $s_1, s_2 \in S$ and $\overline{s_1} \cap \overline{s_2} \neq \emptyset$, then $\overline{s_1} = \overline{s_2}$. Equivalently, distinct equivalence classes are disjoint. Let $\{s_i\}_{i \in I}$ be a complete set of representatives of the set of equivalence classes of elements of S. Then

$$S = \bigcup_{i \in I} \overline{s_i}$$

is a partition of S.

For example, let **Even** be the set of even integers and let **Odd** be the set of odd integers. Then $\mathbf{Z} = \mathbf{Even} \cup \mathbf{Odd}$ is a partition of $\mathbf{Z}$, and $\mathscr{R}_2$ is the associated equivalence relation on $\mathbf{Z}$. Conversely, $\mathbf{Z} = \mathbf{Even} \cup \mathbf{Odd}$ is the partition associated with the equivalence relation $\mathscr{R}_2$.

Let X be a set with an equivalence relation $\mathscr{R}$. Let $\overline{x}$ denote the equivalence class of x, and let $X/\mathscr{R}$ denote the set of equivalence classes of this relation. We define the *canonical function* $\pi : X \to X/\mathscr{R}$ by $\pi(x) = \overline{x}$ for all $x \in X$.

Theorem A.8. *Let X and Y be sets, let $\mathscr{R}$ be an equivalence relation on X, and let $X/\mathscr{R}$ be the set of equivalence classes of $\mathscr{R}$. Let $f : X \to Y$ be a function. There exists a function $\tilde{f} : X/\mathscr{R} \to Y$ such that $\tilde{f}\pi = f$ if and only if $f(x) = f(x')$ for all $x, x' \in X$ with $(x, x') \in \mathscr{R}$.*

The equation $\tilde{f}\pi = f$ is equivalent to the statement that the following diagram commutes:

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\pi"'] & & Y \\ & X/\mathscr{R} \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

Theorem A.9. *Let X be a nonempty set. There is a one-to-one correspondence between the number of equivalence relations on X and the number of partitions of X.*

The *Bell number* $B(n)$ is the number of partitions of a set of cardinality n.

Exercises

1. Let
$$X = \{(a,b) :\in \mathbf{Z}_{\text{and}} b \in \mathbf{Z} \setminus \{0\}\}.$$
For $(a,b$ and (c,d) in X, define $(a,b) \sim (c,d)$ if $ad = bc$.

a. Prove that this is an equivalence relation.

b. Show that the equivalence classes of this relation are the rational numbers.

A.5 Binary operations

Let S be a nonempty set. A *binary relation* is a function f from $S \times S$ into S. Thus, if $s_1, s_2 \in S$, then $f(s_1, s_2) \in S$. We usually denote the binary operation f by multiplication or by addition. Using multiplicative notation, we write

$$f(s_1, s_2) = s_1 \cdot s_2 \quad \text{or} \quad s_1 s_2.$$

Using additive notation, we write

$$f(s_1, s_2) = s_1 + s_2.$$

For example, multiplication of real numbers is a binary relation, and addition of integers is a binary relation.

A binary operation on the set S is *associative* if

$$f(f(s_1, s_2), s_3) = f(s_1, f(s_2, s_3))$$

for all $s_1, s_2, s_3 \in S$. Written in multiplicative notation, associativity is

$$(s_1 s_2) s_3 = s_1 (s_2 s_3).$$

Written in additive notation, associativity is

$$(s_1 + s_2) + s_3 = s_1 + (s_2 + s_3).$$

A *semigroup* is a nonempty set with an associative binary operation.

An element e in the semigroup S is an *identity* if

$$f(e, s) = f(s, e) = s$$

for all $s \in S$. If e, e' are identities in S, then

$$e = f(e, e') = e'$$

and so, if a semigroup S has an identity, then it has a unique identity. In multiplicative notation, the identity is often denoted 1, and

$$1 \cdot s = s \cdot 1 = s.$$

In additive notation, the identity is often denoted 0, and

$$0+s=s+0=s.$$

A *monoid* is a semigroup with an identity.

Addition and multiplication of integers and rational, real, and complex numbers are associative binary operations with identities 0 and 1, respectively, and so **Z**, **Q**, **R**, and **C** are monoids with respect to both addition and multiplication.

A.6 Semigroups and monoids

A *binary operation* on a set S is a function $\mu : S\times S\to S$. We often denote a binary operation multiplicatively:

$$\mu(x,y)=x\cdot y$$

or additively:

$$\mu(x,y)=x+y.$$

The binary operation μ is *commutative* if $\mu(x,y)=\mu(y,x)$ for all $x,y\in S$. Commutativity is expressed multiplicatively as $x\cdot y=y\cdot x$ and additively as $x+y=y+x$.

A commutative binary operation is also called *abelian*. Usually, if a binary operation is written additively, then the operation is commutative. A multiplicative operation may be commutative or not commutative. Also, we often write $x\cdot y$ as xy.

The binary operation μ is *associative* if, for all $x,y,z\in S$ we have

$$\mu(\mu(x,y),z)=\mu(x,\mu(y,z)).$$

Associativity is expressed multiplicatively as

$$(x\cdot y)\cdot z=x\cdot(y\cdot z)$$

and additively as

$$(x+y)+z=x+(y+z).$$

A *semigroup* is a set with an associative binary operation. An *abelian semigroup* (or *commutative semigroup*) is a semigroup whose binary operation is commutative. For example, for every nonnegative integer n, the set $\{x\in\mathbf{Z}:x\geq n\}$ is an abelian additive semigroup, that is, a semigroup with the binary operation of addition. The set $\{x\in\mathbf{Z}:x\geq n\}$ is also an abelian multiplicative semigroup, that is, a semigroup with the binary operation of multiplication.

An element e in a semigroup S is an *identity* if $e\cdot x=x\cdot e=x$ for all $x\in S$. A *monoid* is a semigroup with an identity. If e_1 and e_2 are identity elements in a semigroup S, then

$$e_1=e_1e_2=e_2$$

and so the identity element in a monoid is unique.

For example, the set $\mathbf{N}_0$ of nonnegative integers is an abelian monoid under addition, and also an abelian monoid under multiplication. If S is an additive monoid, then we often denote the identity element by 0.

Let S be a multiplicative monoid with identity element e, and let $x \in S$. An element $y \in S$ is an *inverse* of x if $x \cdot y = y \cdot x = e$. If y_1 and y_2 are inverses of x in S, then

$$y_1 = y_1 e = y_1(xy_2) = (y_1 x)y_2 = ey_2 = y_2$$

and so the inverse of an element is unique. We denote the multiplicative inverse of x by x^{-1}.

If S is an additive monoid with identity element 0, then $y \in S$ is an *inverse* of x if $x + y = 0$. We denote the additive inverse of x by $-x$.

A monoid G is a *group* if every element of G has an inverse. Equivalently, a set G with a binary operation, written multiplicatively, is a group if

1. Multiplication is associative: $(xy)z = x(yz)$ for all $x,y,z \in G$.
2. There is element $e \in G$ such that $ex = xe = x$ for all $x \in G$.
3. For every $x \in G$ there exists $y \in G$ such that $xy = yx = e$.

The group G is *commutative* or *abelian* if $xy = yx$ for all $x,y \in G$.

Similarly, a set G with a binary operation, written additively, is a group if

1. Addition is associative: $(x+y)+z = x+(y+z)$ for all $x,y,z \in G$.
2. There is element $0 \in G$ such that $0+x = x+0 = x$ for all $x \in G$.
3. For every $x \in G$ there exists $y \in G$ such that $x+y = y+x = 0$.

The group G is *commutative* or *abelian* if $x+y = y+x$ for all $x,y \in G$.

For example, the set $\mathbf{Q}$ of rational numbers is an additive group. The set $\mathbf{Q}^*$ of nonzero rational numbers is a multiplicative group.

Let G be a group with identity e. A subset H of G is a *subgroup* of G if

1. $e \in H$.
2. If $x,y \in H$, then $xy \in H$.
3. If $x \in H$, then $x^{-1} \in H$.

For example, the set of even integers is a subgroup of the additive group $\mathbf{Z}$. The set of nonzero rational numbers whose denominators are powers of 2 is a multiplicative subgroup of $\mathbf{Q}$ (Exercise 2).

Let X be a semigroup with an associative multiplication. Let $k \geq 3$, and let $(x_1, x_2, \ldots, x_k)$ be a sequence of k not necessarily distinct elements of X. Multiplication is a binary operation. For $k \geq 3$, we define iterated products by induction: Let

$$x_1 x_2 x_3 = (x_1 x_2)x_3$$

If $k \geq 3$ and if the k-fold product $x_1 x_2 \cdots x_k$ has been defined, then we define the $(k+1)$-fold product

$$x_1 x_2 \cdots x_k x_{k+1} = (x_1 x_2 \cdots x_k)x_{k+1}. \tag{A.8}$$

For example,

$$x_1x_2x_3x_4x_5 = (x_1x_2x_3x_4)x_5 = ((x_1x_2x_3)x_4)x_5 = (((x_1x_2)x_3)x_4)x_5.$$

Lemma A.2. *Let X be a multiplicative semigroup, and let $(x_1,\ldots,x_{k+\ell})$ be a sequence of $k+\ell$ not necessarily distinct elements of X. For $k \geq 1$ and $\ell \geq 1$,*

$$(x_1x_2\cdots x_k)(x_{k+1}x_{k+2}\cdots x_{k+\ell}) = x_1x_2\cdots x_kx_{k+1}x_{k+2}\cdots x_{k+\ell}.$$

If $x_i = x$ for $i = 1,\ldots,k+\ell$, then

$$x^kx^\ell = x^{k+\ell}.$$

We note that if X is an additive semigroup, then the Lemma asserts that

$$(x_1+\cdots+x_k)+(x_{k+1}+\cdots+x_{k+\ell}) = x_1+\cdots+x_k+x_{k+1}+\cdots+x_{k+\ell}.$$

and

$$kx+\ell x = (k+\ell)x.$$

Proof. The proof is my induction on ℓ. For $\ell = 1$, the identity

$$(x_1x_2\cdots x_k)x_{k+1} = x_1x_2\cdots x_kx_{k+1}$$

is the definition of the iterated product in a semigroup. Let $\ell \geq 2$, and assume that the Lemma holds for $\ell - 1$. Applying definition (A.8) and associativity, we obtain

$$\begin{aligned}(x_1\cdots x_k)(x_{k+1}\cdots x_{k+\ell-1}x_{k+\ell}) &= (x_1\cdots x_k)((x_{k+1}\cdots x_{k+\ell-1})x_{k+\ell})\\ &= ((x_1\cdots x_k)(x_{k+1}\cdots x_{k+\ell-1}))x_{k+\ell}\\ &= (x_1\cdots x_kx_{k+1}\cdots x_{k+\ell-1})x_{k+\ell}\\ &= x_1\cdots x_{k+\ell-1}x_{k+\ell}.\end{aligned}$$

This completes the induction. If $x_i = x$ for $i = 1,\ldots,k+\ell$, then

$$x^kx^\ell = x^{k+\ell}.$$

This completes the proof.

Let A and B be subsets of a group G. We define the *product set*

$$AB = \{ab : a \in A \text{ and } b \in B\}.$$

We have $AB = \emptyset$ if and only if $A = \emptyset$ or $B = \emptyset$. Let A and B be subsets of a group G. We define the *product set*

$$AB = \{ab : a \in A \text{ and } b \in B\}.$$

We have $AB = \emptyset$ if and only if $A = \emptyset$ or $B = \emptyset$.

If $x \in G$ and $A \subseteq X$, we define the *left translation*

$$x = \{x\}A = \{xa : a \in A\}$$

and the *right translation*

$$Ax = A\{x\} = \{ax : a \in A\}.$$

If X is a set, then the *power set* of X is the set $\mathscr{P}(X)$ consisting of all subsets of X. If X is a semigroup, then *set multiplication* is the binary operation μ on $\mathscr{P}(X)$ such that $\mu(A,B)$ is the product set AB for every ordered pair (A,B) of subsets of X.

Lemma A.3. *If G is a semigroup, then $\mathscr{P}(G)$ is a semigroup with the binary operation of set multiplication. If G is a monoid with identity e, then $\mathscr{P}(G)$ is a monoid with identity $\{e\}$.*

Proof. If $A,B,C \in \mathscr{P}(G)$, then

$$\begin{aligned}(AB)C &= \{ab : a \in A, b \in B\}C \\ &= \{(ab)c : a \in A, b \in B, c \in C\} \\ &= \{a(bc) : a \in A, b \in B, c \in C\} \\ &= A\{bc : b \in B, c \in C\} \\ &= A(BC).\end{aligned}$$

If G is a monoid with identity e, then $\{e\}A = A\{e\} = A$ for all $A \in \mathscr{P}(G)$, and so $\mathscr{P}(G)$ is a monoid with identity $\{e\}$. This completes the proof.

Exercises

1. Let A be a subset of a semigroup G, and let $x, y \in G$. Prove that $(xA)y = x(Ay)$.
2. Prove that the set of nonzero rational numbers whose denominators are powers of 2 is a multiplicative subgroup of $\mathbf{Q}$.
3. Prove that the set of rational numbers whose denominators are divisors of 12 is an additive subgroup of $\mathbf{Q}$.
4. Let $\mathbf{T} = \{x \in \mathbf{R} : 0 \le x < 1\}$, and define a binary operation $(x,y) \mapsto x \oplus y$ in $\mathbf{T}$ as follows:
$$x \oplus y = \begin{cases} x+y & \text{if } x+y < 1 \\ x+y-1 & \text{if } x+y \ge 1. \end{cases}$$
   Prove that $\mathbf{T}$ is an additive abelian group.

A.7 Combinations and the binomial theorem

Let n and k be integers such that $0 \le k \le n$. We denote by $C(n,k)$ the number of k-element subsets of a set of size n.

Theorem A.10. *Let n and k be integers such that $0 \leq k \leq n$. Then*

$$C(n,k) = C(n,n-k) \tag{A.9}$$

and

$$C(n+1,k+1) = C(n,k) + C(n,k+1). \tag{A.10}$$

Proof. Let X be a set of cardinality n, and let $0 \leq k \leq n$. Let $\mathscr{P}_k(X)$ denote the set of subsets of X of cardinality k. If A is a subset of X of cardinality k, then the complementary set $X \setminus A$ is a subset of X of cardinality $n-k$. The function $A \mapsto X \setminus A$ is a one-to-one correspondence between between $\mathscr{P}_k(X)$ and $\mathscr{P}_{n-k}(X)$. This establishes the symmetry (A.9).

Let X^* be a set of cardinality $n+1$, let $x^* \in X^*$, and let $X = X^* \setminus \{x^*\}$. Then X is a set of cardinality n. We can partition the set of subsets of X^* of cardinality $k+1$ into two disjoint sets: Those subsets that contain x^* and those that do not. There is a one-to-one correspondence between subsets of X^* of size $k+1$ that contain x^* and subsets of X of size k. Similarly, there is a one-to-one correspondence between subsets of X^* of size $k+1$ that do not contain x^* and subsets of X of size $k+1$. Formula (A.10) follows from the observation from that the number of sets of the first kind is $C(n,k)$ and the number of sets of the second kind is $C(n,k+1)$. This completes the proof.

For every nonnegative integer n, we define the positive integer $n!$ (called *n factorial*) as follows:

$$0! = 1 \quad \text{and} \quad n! = 1 \cdot 2 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

Theorem A.11. *Let n and k be integers such that $0 \leq k \leq n$. Then*

$$C(n,k) = \frac{n!}{k!(n-k)!}. \tag{A.11}$$

Proof. The proof is by induction on n. For $n = 0$ and $n = 1$ we have

$$\begin{aligned} C(0,0) &= 1 = \frac{0!}{0!0!} \\ C(1,0) &= 1 = \frac{1!}{0!1!} \\ C(1,1) &= 1 = \frac{1!}{1!0!}. \end{aligned}$$

Assume that formula (A.11) holds for n. If $0 \leq k \leq n$, then

$$\begin{aligned}C(n+1,k+1) &= C(n,k+1)+C(n,k)\\ &= \frac{n!}{(k+1)!(n-(k+1))!}+\frac{n!}{k!(n-k)!}\\ &= \frac{n!}{k!(n-k-1)!}\left(\frac{1}{k+1}+\frac{1}{n-k}\right)\\ &= \frac{n!}{k!(n-k-1)!}\left(\frac{n+1}{(k+1)(n-k)}\right)\\ &= \frac{(n+1)!}{(k+1)!((n+1)-(k+1))!}.\end{aligned}$$

This completes the proof.

For nonnegative integers n and k we define the *binomial coefficient*

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{if } 0 \le k \le n \\ 0 & \text{if } k > n. \end{cases}$$

We often read $C(n,k) = \binom{n}{k}$ as "n choose k" and call it the number of *combinations* of k elements chosen from a set of size n. Theorem A.11 implies that $\binom{n}{k}$ is an integer for all nonnegative integers n and k. With the notation of binomial coefficients, Theorem A.10 states that

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

for all positive integers n and k.

We can arrange the binomial coefficients in a center-justified triangular array as follows: For $n = 0,1,2,\ldots$, the nth row of the triangle consists go the $n+1$ numbers $\binom{n}{0}$, $\binom{n}{1}$, $\binom{n}{2}$, ... , $\binom{n}{n}$. The first seven rows are as follows:

$$\begin{array}{ccccccccccccc} &&&&&&1&&&&&& \\ &&&&&1&&1&&&&& \\ &&&&1&&2&&1&&&& \\ &&&1&&3&&3&&1&&& \\ &&1&&4&&6&&4&&1&& \\ &1&&5&&10&&10&&5&&1& \\ 1&&6&&15&&20&&15&&6&&1 \end{array}$$

This array is called *Pascal's triangle*. Notice that each number in the triangle is the sum of the two numbers to its right and left in the previous row. Equivalently, the $(k+1)$st number in row $n+1$ is the sum of the kth and $(k+1)$st numbers in row n. This is exactly the recursion formula (A.10).

Theorem A.12. *For every nonnegative integer n,*

$$2^n = \sum_{k=0}^{n} \binom{n}{k}.$$

Proof. A set X of size n contains exactly 2^n subsets, that is, the cardinality of $\mathscr{P}(X)$ is 2^n. Partitioning the subsets of X according to their cardinalities, we obtain

$$\mathscr{P}(X) = \bigcup_{k=0}^{n} \mathscr{P}_k(X)$$

and so

$$2^n = |\mathscr{P}(X)| = \sum_{k=0}^{n} |\mathscr{P}_k(X)| = \sum_{k=0}^{n} C(n,k) = \sum_{k=0}^{n} \binom{n}{k}.$$

This completes the proof.

Theorem A.13 (Binomial theorem). *For every positive integer n,*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Proof. By induction on n. If $n = 1$, then

$$(x+y)^1 = x+y = \binom{1}{0}x + \binom{1}{1}y = \sum_{k=0}^{1} \binom{n}{k} x^{n-k} y^k.$$

Let $n \geq 1$, and assume the Theorem holds for n. Then

$$
\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n \\
&= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \\
&= \sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1} \\
&= \sum_{k=0}^{n}\binom{n}{k}x^{n+1-k}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{(n+1)-(k+1)}y^{k+1} \\
&= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n+1-k}y^k + \sum_{k=0}^{n-1}\binom{n}{k}x^{(n+1)-(k+1)}y^{k+1} + y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n+1-k}y^k + \sum_{k=1}^{n}\binom{n}{k-1}x^{(n+1)-k}y^{k} + y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^{n}\left(\binom{n}{k}+\binom{n}{k-1}\right)x^{(n+1)-k}y^k + y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}x^{(n+1)-k}y^k + y^{n+1} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^{(n+1)-k}y^k.
\end{aligned}
$$

This completes the induction.

Exercises

1. Let m be a positive integer. Prove that the relation

$$\mathscr{R}_m = \{(a,b) \in \mathbf{Z}^2 : a-b \text{ is divisible by } m\}$$

   is an equivalence relation.
2. Prove that the relation associated with a partition of a set S is an equivalence relation on S.
3. Let $S = \{1,2,3,4\}$.

   a. Consider the relation $\mathscr{R}$ on S defined by

$$\mathscr{R} = \{(1,1),(1,3),(1,4),(2,2),(3,1),(3,3),(4,1),(4,4)\}.$$

   Prove that this relation is symmetric and reflexive, but not transitive.

   b. Construct a relation on S that is reflexive and transitive but not symmetric.

   c. Construct a relation on S that is symmetric and transitive but not reflexive.

4. Prove that if n is a positive integer, then $\frac{1}{n+1}\binom{2n}{n}$ is a positive integer.
   Hint: Consider $\binom{2n}{n} - \binom{2n}{n+1}$.
5. Let n and k be integers with $0 \leq k \leq n$. Prove that

$$\binom{n}{k-1} < \binom{n}{k} \quad \text{and} \quad \text{if } 0 < k \leq n/2$$

   and

$$\binom{n}{k} > \binom{n}{k+1} \quad \text{and} \quad \text{if } n/2 \leq k < n.$$

   Prove that $\binom{n}{k} = \binom{n}{\ell}$ if and only if n is odd and $k = (n-1)/2$ and $\ell = (n+1)/2$.

A.8 Binomial coefficients and the binomial theorem

For every positive integer n, the integer *n factorial*, denoted $n!$, is the product of the first n positive integers, that is,

$$n! = 1 \cdot 2 \cdots (n-1) \cdot n.$$

We define

$$0! = 1.$$

We shall use mathematical induction to construct a positive integer $C(n,k)$ for every pair of nonnegative integers n and k such that

$$0 \leq k \leq n.$$

Let $C(0,0) = 1$. Let $n \geq 1$, and suppose that we have constructed the numbers $C(n-1,k)$ for $k = 0,1,2,\ldots,n-1$. Let $C(n,0) = C(n,n) = 1$, and, for $k = 1,2,\ldots,n-1$, define

$$C(n,k) = C(n-1,k) + C(n-1,k-1).$$

The integers $C(n,k)$ are called the *binomial coefficients*. The binomial coefficient $C(n,k)$ is also denoted $\binom{n}{k}$.

Theorem A.14. *If n and k are nonnegative integers such that* $0 \leq k \leq n$*, then*

$$C(n,k) = \frac{n!}{k!(n-k)!}. \tag{A.12}$$

Proof. The proof is by induction on n. For $n = k = 0$ we have

$$\frac{n!}{k!(n-k)!} = \frac{0!}{0!0!} = \frac{1}{1 \cdot 1} = 1 = C(0,0).$$

For $n = 1$ and $k = 0$ or 1, we have

$$\frac{n!}{k!(n-k)!} = \frac{1!}{0!1!} = \frac{1}{1\cdot 1} = 1 = C(1,k).$$

Let $n \geq 2$, and assume that identity (A.12) holds for $n-1$ and all $k = 0,1,\ldots,n-1$. Then

$$\begin{aligned}
C(n,k) &= C(n-1,k) + C(n-1,k-1) \\
&= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} \\
&= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\
&= \frac{(n-1)!(n-k)}{k!(n-k)!} + \frac{(n-1)!k}{k!(n-k)!} \\
&= \frac{n!}{k!(n-k)!}.
\end{aligned}$$

This completes the proof.

Corollary A.1. *Let k be a positive integer. The product of any k consecutive integers is divisible by $k!$.*

Proof. Let $n \in \mathbf{Z}$, and let

$$a(n) = \prod_{i=0}^{k-1}(n-i) = n(n-1)(n-2)\cdots(n-k+1).$$

We must prove that $k!$ divides $a(n)$.

By Theorem A.14, the binomial coefficient $C(n,k) = a(n)/k!$ is an integer for every $n \geq k$. If $0 \leq n \leq k-1$, then $a(n) = 0$ is divisible by $k!$. If $n \leq -1$, then $n = -m$ for the positive integer $m = |n|$, and $m+k-1 \geq k$. It follows that $a(m-k+1)$ is divisible by $k!$. We have

$$\begin{aligned}
a(n) &= (-m)(-m-1)\cdots(-m-k+2)(-m-k+1) \\
&= (-1)^k(m+k-1)(m+k-2)\cdots(m+1)m \\
&= (-1)^k a(m+k-1).
\end{aligned}$$

and so $k!$ divides $a(n)$. This completes the proof.

The polynomial identities

$$\begin{aligned}
(x+y)^1 &= x+y \\
(x+y)^2 &= x^2+2xy+y^2 \\
(x+y)^3 &= x^3+3x^2y+3xy^2+y^3 \\
(x+y)^4 &= x^4+4x^3y+6x^2y^2+4xy^3+y^4
\end{aligned}$$

are special cases of the following result.

Theorem A.15 (Binomial theorem). *For every positive integer n, there is the polynomial identity*

$$(x+y)^n = \sum_{k=0}^{n} C(n,k)x^{n-k}y^k.$$

Proof. The proof is by induction on n. For $n = 1$ we have $C(1,0) = C(1,1) = 1$ and so

$$(x+y)^1 = \sum_{k=0}^{1} C(1,k)x^{n-k}y^k = C(1,0)x + C(1,1)y = x + y.$$

Let $n \geq 2$ and assume the binomial theorem holds for $n-1$. Then

$$\begin{aligned}
(x+y)^n &= (x+y)(x+y)^{n-1} \\
&= (x+y)\sum_{k=0}^{n-1} C(n-1,k)x^{n-1-k}y^k \\
&= x\sum_{k=0}^{n-1} C(n-1,k)x^{n-1-k}y^k + y\sum_{k=0}^{n-1} C(n-1,k)x^{n-1-k}y^k \\
&= \sum_{k=0}^{n-1} C(n-1,k)x^{n-k}y^k + \sum_{k=0}^{n-1} C(n-1,k)x^{n-1-k}y^{k+1} \\
&= x^n + \sum_{k=1}^{n-1} C(n-1,k)x^{n-k}y^k + \sum_{k=0}^{n-2} C(n-1,k)x^{n-1-k}y^{k+1} + y^n \\
&= x^n + \sum_{k=1}^{n-1} C(n-1,k)x^{n-k}y^k + \sum_{k=1}^{n-1} C(n-1,k-1)x^{n-k}y^k + y^n \\
&= x^n + \sum_{k=1}^{n-1} \left(C(n-1,k) + C(n-1,k-1)\right)x^{n-k}y^k + y^n \\
&= x^n + \sum_{k=1}^{n-1} C(n,k)x^{n-k}y^k + y^n \\
&= \sum_{k=0}^{n} C(n,k)x^{n-k}y^k.
\end{aligned}$$

This completes the proof.

Exercises

1. Let $f(x,y) = (x+y)^n$. Apply the binomial theorem to compute $f(1,1)$. This gives another proof of Theorem A.12.
2. Prove that

$$0 = \sum_{k=0}^{n} (-1)^k C(n,k).$$

Hint: Let $f(x,y) = (x+y)^n$. Use the binomial theorem to evaluate $f(1,-1)$.

3. Let n and k be integers such that $n \geq 1$ and $0 \leq k \leq n$. Prove that

$$\sum_{i=0}^{k} (-1)^i \binom{n}{i} = (-1)^k \binom{n-1}{k}.$$

4. Prove that $n!$ is the number of bijections of a set of size n.
5. Prove that $C(n,k)$ is the number of subsets of size k in a set of size n.

A.9 The multinomial theorem

The binomial coefficients $\binom{n}{k}$ counts the number of k-element subsets of a set with k elements. Equivalently, it counts the number of ordered partitions of a set with n elements into two subsets, one of cardinality k and the the other of cardinality $n-k$. Let $k_1 = k$ and $k_2 = n-k$. Then $\binom{n}{k} = \frac{n!}{k_1!k_2!}$ counts the number of ordered pairs (X_1,X_2), where X_1 and X_2 are disjoint subsets of X such that $|X_1| = k_1$ and $|X_2| = k_2$.

A natural generalization is the following. Let n be a positive integer, and let $(k_1,\ldots,k_m)$ be an m-tuple of nonnegative integers such that $n = k_1 + k_2 + \cdots + k_m$. Let $C(n,k_1,k_2,\ldots,k_m)$ count the number of m-tuples of pairwise disjoint subsets $(X_1,X_2,\ldots,X_m)$ of X such that $|X_i| = k_i$ for $i = 1,2,\ldots,m$. We call the nonnegative integer $C(n,k_1,k_2,\ldots,k_m)$ the *multinomial coefficient*, and denote it by

$$C(n,k_1,k_2,\ldots,k_m) = \binom{n}{k_1,k_2,\ldots,k_m}$$

Theorem A.16. *Let m be a positive integer and let n be a nonnegative integer. If $(k_1,k_2,\ldots,k_m)$ is an m-tuple of nonnegative integers such that $n = k_1 + k_2 + \cdots + k_m$, then*

$$C(n,k_1,k_2,\ldots,k_m) = \frac{n!}{k_1!k_2!\cdots k_m!}. \tag{A.13}$$

If $n+1 = k_1 + k_2 + \cdots + k_m$, then

$$C(n+1,k_1,k_2,\ldots,k_m) = \sum_{j=1}^{m} C(n,k_1,\ldots,k_{j-1},k_j - 1,k_{j+1},\ldots,k_m). \tag{A.14}$$

Proof. By induction on n. If $n = 0$, then $(0,0,\ldots,0)$ is the unique m-tuple $(k_1,k_2,\ldots,k_m)$ satisfying $0 = k_1 + k_2 + \cdots + k_m$, and

$$\begin{aligned} C(n, k_1, k_2, \ldots, k_m) &= C(0, 0, 0, \ldots, 0) \\ &= 1 = \frac{0!}{0!0!\cdots 0!} \\ &= \frac{n!}{k_1!k_2!\cdots k_m!}. \end{aligned}$$

If $n = 1$ and if the m-tuple $(k_1, k_2, \ldots, k_m) \in \mathbf{N}_0^m$ satisfies $n = k_1 + k_2 + \cdots + k_m$, then there exists $j \in \{1, 2, \ldots, m\}$ such that $k_j = 1$ and $k_i = 0$ for $i \in \{1, 2, \ldots, m\} \setminus \{j\}$. It follows that

$$\begin{aligned} C(n, k_1, k_2, \ldots, k_m) &= C(1, 0, 0, \ldots, 1, \ldots, 0) \\ &= 1 = \frac{0!}{0!0!\cdots 1!\cdots 0!} \\ &= \frac{n!}{k_1!k_2!\cdots k_m!}. \end{aligned}$$

Let $n \geq 1$, and assume that the Theorem holds for n. Let X be a set with $|X| = n+1$, let $(k_1, k_2, \ldots, k_m) \in \mathbf{N}_0^m$ satisfy $k_1 + k_2 + \cdots + k_m = n+1$, and let $a \in X$. If the sets $X_1, X_2, \ldots, X_m$ partition X, then there is a unique set X_j such that $a \in X_j$. We can partition the set of m-tuples $(X_1, X_2, \ldots, X_m)$ of pairwise disjoint subsets of X satisfying $|X_i| = k_i$ for $i = 1, \ldots, m$ into m sets $\mathscr{S}_1, \mathscr{S}_2, \ldots, \mathscr{S}_m$ as follows. The set $\mathscr{S}_i$ consists of all m-tuples $(X_1, X_2, \ldots, X_m)$ such that $a \in X_j$. The number of m-tuples $(X_1, X_2, \ldots, X_m)$ in $\mathscr{S}_j$ is exactly the number of m-tuples $(X_1', X_2', \ldots, X_m')$ such that, for $i = 1, \ldots, m$, the set X_i' is a subset of $X \setminus \{a\}$ with $|X_i'| = k_i$ for $i \neq j$ and $|X_j'| = k_j - 1$. Because $|X \setminus \{a\}| = n$, the induction hypothesis implies that

$$\begin{aligned} |\mathscr{S}_j| &= C(n, k_1, \ldots, k_{j-1}, k_j - 1, k_{j+1}, \ldots, k_m) \\ &= \frac{n!}{k_1!\cdots k_{j-1}!(k_j-1)!k_{j+1}!\cdots k_m!} \\ &= \frac{k_j n!}{k_1!\cdots k_{j-1}!k_j!k_{j+1}!\cdots k_m!} \end{aligned}$$

and so

$$
\begin{aligned}
C(n+1,k_1,\ldots,k_{j-1},k_j,k_{j+1},\ldots,k_m) &= \sum_{j=1}^{m} |\mathscr{S}_j| \\
&= \sum_{j=1}^{m} C(n,k_1,\ldots,k_{j-1},k_j-1,k_{j+1},\ldots,k_m) \\
&= \sum_{j=1}^{m} \frac{k_j n!}{k_1!\cdots k_{j-1}!k_j!k_{j+1}!\cdots k_m!} \\
&= \left(\sum_{j=1}^{m} k_j\right) \frac{n!}{k_1!\cdots k_{j-1}!k_j!k_{j+1}!\cdots k_m!} \\
&= \frac{(n+1)n!}{k_1!\cdots k_{j-1}!k_j!k_{j+1}!\cdots k_m!} \\
&= \frac{(n+1)!}{k_1!\cdots k_{j-1}!k_j!k_{j+1}!\cdots k_m!}.
\end{aligned}
$$

This completes the proof of (A.13) and (A.14).

Theorem A.17 (Multinomial theorem). *For all positive integers m and n,*

$$
(x_1+x_2+\cdots+x_m)^n = \sum_{\substack{(k_1,k_2,\ldots,k_m)\in\mathbf{N}_0^m \\ k_1+k_2+\cdots+k_m=n}} \frac{n!}{k_1!k_2!\cdots k_m!} x_1^{k_1}x_2^{k_2}\cdots x_m^{k_m}.
$$

Proof. By induction on m. The case $m=1$ is the statement that $x_1^n = x_1^n$ and the case $m=2$ is the binomial theorem. Let $m \geq 3$, and assume the multinomial theorem holds for $m-1$ variables. If $y = x_{m-1}+x_m$, then

$$
\begin{aligned}
&(x_1+\cdots+x_{m-2}+x_{m-1}+x_m)^n = (x_1+\cdots+x_{m-2}+y)^n \\
&\quad = \sum_{\substack{(k_1,\ldots,k_{m-2},\ell)\in\mathbf{N}_0^{m-1} \\ k_1+\cdots+k_{m-2}+\ell=n}} \frac{n!}{k_1!\cdots k_{m-2}!\ell!} x_1^{k_1}x_2^{k_2}\cdots x_{m-2}^{k_{m-2}}(x_{m-1}+x_m)^{\ell} \\
&\quad = \sum_{\substack{(k_1,\ldots,k_{m-2},\ell)\in\mathbf{N}_0^{m-1} \\ k_1+\cdots+k_{m-2}+\ell=n}} \frac{n!}{k_1!\cdots k_{m-2}!\ell!} x_1^{k_1}x_2^{k_2}\cdots x_{m-2}^{k_{m-2}} \sum_{\substack{(k_{m-1},k_m)\in\mathbf{N}_0^{2} \\ k_{m-1}+k_m=\ell}} \frac{\ell!}{k_{m-1}!k_m!} x_{m-1}^{k_{m-1}}x_m^{k_m} \\
&\quad = \sum_{\substack{(k_1,\ldots,k_{m-2},\ell)\in\mathbf{N}_0^{m-1} \\ k_1+\cdots+k_{m-2}+\ell=n}} \sum_{\substack{(k_{m-1},k_m)\in\mathbf{N}_0^{2} \\ k_{m-1}+k_m=\ell}} \frac{n!}{k_1!\cdots k_{m-2}!\ell!} \frac{\ell!}{k_{m-1}!k_m!} x_1^{k_1}x_2^{k_2}\cdots x_{m-2}^{k_{m-2}}x_{m-1}^{k_{m-1}}x_m^{k_m} \\
&\quad = \sum_{\substack{(k_1,\ldots,k_{m-2},k_{m-1},k_m)\in\mathbf{N}_0^{m} \\ k_1+\cdots+k_{m-2}+k_{m-1}+k_m=n}} \frac{n!}{k_1!\cdots k_{m-2}!k_{m-1}!k_m!} x_1^{k_1}x_2^{k_2}\cdots x_{m-2}^{k_{m-2}}x_{m-1}^{k_{m-1}}x_m^{k_m}.
\end{aligned}
$$

This completes the proof.

Exercises

1. Let $X = \{1,2,3,4,5\}$. Compute the number of triples (X_1,X_2,X_3) of pairwise disjoint subsets of X of such that $|X_1| = |X_2| = 2$ and $|X_3| = 1$. An example of this kind of subset triple is $(\{2,5\},\{1,4\},\{3\})$. List all such triples.
2. Let m and n be positive integers, and let $(k_1,\ldots,k_m) \in \mathbf{N}_0^m$ satisfy $k_1 + \cdots + k_m = n$.

   a. Let $\ell = k_{m-1} + k_m$. Prove that
   $$\binom{n}{k_1,\ldots,k_{m-2},k_{m-1},k_m} = \binom{n}{k_1,\ldots,k_{m-2},\ell}\binom{\ell}{k_{m-1},k_m}.$$
   b. Let $j \in \{1,2,\ldots,m-1\}$ and
   $$n_{j+1} = k_{j+1} + \cdots + k_m = n - k_1 - k_2 - \cdots - k_m.$$
   Prove that
   $$\binom{n}{k_1,\ldots,k_j,\ldots,k_m} = \binom{n}{k_1,\ldots,k_j,n_{j+1}}\binom{n_{j+1}}{k_{j+1},\ldots,k_m}.$$
3. Prove that
$$\sum_{\substack{(k_1,k_2,k_3)\in\mathbf{N}_0^3 \\ k_1+k_2+k_3=n}} \binom{n}{k_1,k_2,k_3} = 3^n.$$
4. Prove that, for every positive integer m,
$$\sum_{\substack{(k_1,k_2,\ldots,k_m)\in\mathbf{N}_0^m \\ k_1+k_2+\cdots+k_m=n}} \binom{n}{k_1,k_2,\ldots,k_m} = m^n.$$

A.10 Ordered sets

A relation $\sim$ on a set X is *anti-symmetric* if $x \sim y$ and $y \sim x$ imply $x = y$. A *partial order* on a set X is a relation that is reflexive, anti-symmetric, and transitive. We denote the relation by $\preceq$. Reflexivity means that $x \preceq x$ for all $x \in X$. Anti-symmetry means that if $x,y \in X$ and both $x \preceq y$ and $y \preceq x$, then $x = y$. Transitivity means that if $x \preceq y$ and $y \preceq z$, then $x \preceq z$.

For example, in the power set of a set X, the relation of set inclusion is a partial order (Exercise 1).

A partially ordered set X is *totally ordered* if, for all $x,y \in X$, either $x \preceq y$ or $y \preceq x$. For example, the relation $x \leq y$ in $\mathbf{Z}$ is a total order. The relation of subset inclusion is a partial order but not a total order. For example, $S = \{1,2\}$ and $T = \{1,3\}$ are subsets of $\mathbf{Z}$, but S is not a subset of T and T is not a subset of S.

Let S be a nonempty set, and let X_S be the set of all finite sequences of elements of S. An element $x = (s_i)_{i=1}^n \in X_S$ is a called a *word* in the *alphabet* S. We often write $x = s_1 s_2 \cdots s_n$, and we call n the *length* of x. If S is totally ordered, then there are several ways to construct a total order on the words in X_S. For example, if $x = s_1 s_2 \cdots s_m$ and $x' = s'_1 s'_2 \cdots s'_n$ are distinct words of lengths m and n, respectively, then there is a smallest positive integer j such that $s_i = s'_i$ for all $i = 1, \ldots, j-1$ and $s_j \neq s'_j$. We define $x \preceq_{\text{lex}} x'$ in X_S if $s_j \preceq s'_j$ in S. If $x = x'$, then we define $x \preceq_{\text{lex}} x'$. This total order on X_S is called the *lexicographical order*. For example, if we order the letters in the Latin alphabet $a \preceq b \preceq \cdots \preceq z$, then the words in a dictionary are ordered lexicographically.

Here is another total order on the set X_S. If x and x' are words of lengths m and n respectively, let $x \preceq_{\text{grlex}} x'$ if $m < n$ and let $x \preceq_{\text{grlex}} x'$ if $m =$ and $x \preceq_{\text{lex}} x'$ in the usual lexicographical order. This total order on X_S is called the *graded lexicographical order*.

Let A be a nonempty subset of a partially ordered set X. An element $x \in X$ is an *upper bound* for A if $a \preceq x$ for all $a \in A$. An element $x^* \in X$ is a *least upper bound* for A if x^* is an upper bound for A and if $x^* \preceq x$ for every upper bound for A. If A has a least upper bound, then the least upper bound is unique (Exercise 4).

Similarly, an element $x \in X$ is a *lower bound* for A if $x \preceq a$ for all $a \in A$. An element $x^* \in X$ is a *greatest lower bound* for A if x^* is an lower bound for A and if $x \preceq x^*$ for every lower bound for A. If A has a greatest lower bound, then the greatest lower bound is unique (Exercise 5).

A *lattice* is a partially ordered set in which every two elements have both a least upper bound and a greatest lower bound. For example, if $\mathscr{P}(X)$ is the power set of X, that is, the set consisting of all subsets of X, then X is partially ordered by inclusion, that is, if $A, B \in \mathscr{P}(X)$, then $A \preceq B$ if A is a subset of B. The least upper bound of a pair A and B of subsets of X is the union $A \cup B$, and the greatest lower bound of A and B is the intersection $A \cap B$. Thus, the partially ordered set $\mathscr{P}(X)$ is a lattice.

Another example: We can partially order the set $\mathbf{N}$ of positive integers by divisibility: For $a, b \in \mathbf{N}$, we write $b \preceq a$ if a divides b. This relation is reflexive, anti-symmetric, and transitive (Exercise 3). However, divisibility does not induce a total order on $\mathbf{N}$. For example, the numbers 5 and 7 are incomparable. However, for any two integers a and b, with greatest common divisor $d = (a,b)$ and least common multiple $m = [a,b]$, we have $m \preceq a \preceq d$ and $m \preceq b \preceq d$, so d is an upper bound for the set $\{a,b\}$ and m is a lower bound for the set $\{a,b\}$. Moreover, d and m are the least upper bound and greatest lower bound, respectively, for $\{a,b\}$, and so the set $\mathbf{N}$, partially ordered by divisibility, is a lattice.

Let S be a nonempty subset of a partially ordered set X. An element $x \in S$ is *maximal* if there does not exist an element $s \in S$ such that $x \preceq s$ and $x \neq s$. Equivalently, $x \in S$ is maximal if the conditions $s \in S$ and $x \preceq s$ imply that $x = s$. A maximal element in a set is not necessarily an upper bound for the set. For example, consider the set $\mathscr{P}(\{1,2,3\})$, partially ordered by inclusion, and the subset

$S = \{\{1\},\{1,2\},\{3\}\}$. The sets $\{1,2\}$ and $\{3\}$ are both maximal elements of S, but neither is an upper bound for S.

An element $x \in S$ is *minimal* if there does not exist an element $s \in S$ such that $s \preceq x$ and $x \neq s$.

A fundamental axiom of set theory, and a powerful tool in algebra, is *Zorn's lemma*: If X is a partially ordered set in which every totally ordered subset of X has an upper bound in X, then X contains a maximal element.

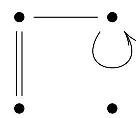
Exercises

1. Prove that if R, S, and T are subsets of a set X, then
   a. $S \subseteq S$
   b. If $S \subseteq T$ and $T \subseteq S$, then $S = T$
   c. If $R \subseteq S$ and $S \subseteq T$, then $R \subseteq T$.
2. Consider the $S = \{a,b,c\}$ with total order $a \preceq c \preceq b$, and consider the following set of words in the alphabet S:
   $$A = \{b, abc, babab, aacacac, cc, baa, aaa, bc\}.$$
   a. Order the set A using the lexicographical order.
   b. Order the set A using the graded lexicographical order.
3. For $a, b \in \mathbf{N}$, define $b \preceq a$ if a divides b. Prove that this relation is reflexive, anti-symmetric, and transitive.
4. Prove that the least upper bound of a nonempty subset of a partially ordered set is unique.
5. Prove that the greatest lower bound of a nonempty subset of a partially ordered set is unique.
6. Let X be a set with $|X| \geq 2$.
   a. Prove that the set of proper subsets of X contains maximal elements, but no upper bound. Prove that the set of nonempty subsets of X contains minimal elements, but no lower bound,

A.11 Graphs

An *undirected graph* $\Gamma = \Gamma(V,E)$ consists of a set V whose elements are called the *vertices* of the graph, and a set E whose elements are called the *edges* of the graph. Each edge $e \in E$ is a set consisting of one or two vertices. A edge $\{v\}$ consisting of one vertex v is called a *loop*. If $e = \{v, v'\} \in E$, then we say that e is an edge connecting the vertices v and v'. Conversely, we say that vertices v and v' in the graph Γ are *adjacent* if $\{v,v'\} \in E$. The graph Γ is *finite* if it has only finitely many vertices and finitely many edges.

For example, let $\Gamma = \Gamma(V,E)$ be the graph with vertex set $V = \{a,b,c,d\}$ and edge set $E = \{e_1,e_2,e_3,e_4\}$, where $e_1 = e_2 = \{a,c\}$, $e_3 = \{a,b\}$, and $e_4 = \{b\}$. Then e_1 and e_2 are multiple edges between vertices a and c, e_3 is a single edge between vertices a and b, and e_4 is a loop at vertex b. Vertex d is isolated; it is not adjacent to any other vertex. We can draw this graph as follows:



Let $\Gamma(V,E)$ be a graph. A path of length k between the vertices v and v' is a $(k+1)$-tuple of vertices $(v_0,v_1,\ldots,v_k)$ such that $v_0 = v$, $v_k = v'$, and $\{v_{i-1},v_i\}$ is an edge in Γ for all $i = 1,\ldots,k$. The number of paths of length 2 connecting vertices v and v' is exactly $|N(v) \cap N(v')|$.

Let $\Gamma = \Gamma(V,E)$ be a finite graph. The *degree* of a vertex v in the graph $\Gamma(V,E)$ is the number of edges that are contain the vertex, that is, if $v \in V$, then

$$\deg(v) = \sum_{\substack{e \in E \\ v \in E}} 1.$$

A set of vertices in Γ is *independent* if the set does not contain two adjacent vertices. Every subset of an independent set is independent. The *independence number* of a finite graph is the cardinality of the largest independent subset of V. If the graph contains a loop at v, then v is adjacent to itself and no set containing v is independent. We denote the independence number by $i(\Gamma)$.

The graph Γ is k-colorable if there exists a partition of the vertex set V into k independent sets. Equivalently, the graph Γ is k-colorable if it is possible to paint the vertices of Γ with k colors so that no two vertices with the same color are connected by an edge. For example, if Γ contains n vertices and each vertex is painted a different color, then we have an n-coloring of Γ. The *chromatic number* of a finite graph without loops is the smallest integer k such that Γ is k-colorable. We denote the chromatic number by $\chi(\Gamma)$.

Lemma A.4. *If $\Gamma = \Gamma(V,E)$ is a finite graph without loops, then*

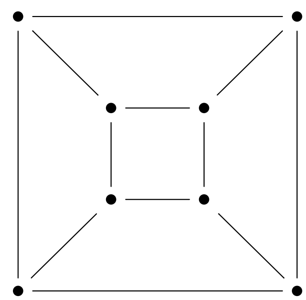
$$|V| \le \chi(\Gamma) i(\Gamma).$$

Proof. Let $\chi(\Gamma) = k$. Suppose that $c_1,\ldots,c_k$ are colors and that each vertex in the graph Γ has been painted one color. For each color c_i, let V_i be the set of vertices in V that have been painted color c_i. Because no two vertices of the same color are adjacent, the set V_i is independent, and so $|V_i| \le i(\Gamma)$ and

$$|V| = \sum_{i=1}^{k} |V_i| \le \sum_{i=1}^{k} i(\Gamma) = k i(\Gamma) = \chi(\Gamma) i(\Gamma).$$

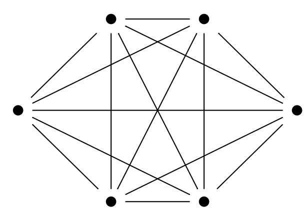
This completes the proof.

The undirected graph Γ is *simple* if it does not contain multiple edges or loops. The absence of multiple edges means that if $v, v' \in V$ and $v \neq v'$, then there is at most one edge in Γ that connects the vertices v and v'. Here are drawings of some simple graphs:



For example, a *complete graph* on n vertices is a graph $K_n = K_n(V,E)$, where the vertex set V has cardinality n and the edge set consists of the $\binom{n}{2}$ subsets of V of size 2.

Here is a drawing of K_6:



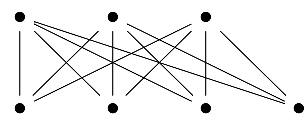
A *bipartite graph* is a simple undirected graph $\Gamma = \Gamma(V,E)$ whose vertex set is the union of disjoint sets V_1 and V_2, and whose edges are of the form $\{v_1, v_2\}$, where $v_1 \in V_1$ and $v_2 \in V_2$. We denote this bipartite graph by $\Gamma = \Gamma(V_1, V_2, E)$. Equivalently, the graph $\Gamma = \Gamma(V,E)$ is bipartite if there is a partition $V = V_1 \cup V_2$ such that $V_1 \cap V_2 = \emptyset$ and

$$E \subseteq \{\{v_1, v_2\} : v_1 \in V_1 \text{ and } v_2 \in V_2\}.$$

If Γ is bipartite graph with disjoint vertex sets V_1 and V_2, then the neighborhood sets satisfy $N(v_2) \subseteq V_1$ for all $v_2 \in V_2$ and $N(v_1) \subseteq V_2$ for all $v_1 \in V_1$.

A bipartite graph with disjoint vertex sets V_1 and V_2 is *complete* if $E = \{\{v_1, v_2\} : v_1 \in V_1 \text{ and } v_2 \in V_2\}$. If V_1 and V_2 are nonempty finite sets with $|V_1| = n_1$ and $|V_2| = n_2$, then we denote the complete bipartite graph by K_{n_1,n_2}. The number of edges in the complete bipartite graph K_{n_1,n_2} is $n_1 n_2$. Every path of length 2 in a bipartite graph is of the form (v_1, v_2, v_1') or (v_2, v_1, v_2'), where $v_1, v_1' \in V_1$ and $v_2, v_2' \in V_2$.

Here is a drawing of $K_{3,4}$:

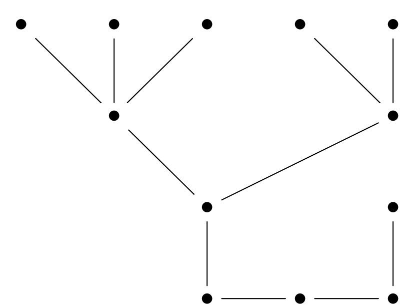


Let v and v' be vertices in the graph $\Gamma(V,E)$. A *path* of length n from v to v' is a finite sequence $(v_i)_{i=0}^n$ of vertices $v_i \in V$ such that $v_0 = v$, $v_n = v'$, and $\{v_{i-1}, v_i\}$ is an edge for all $i = 1, \ldots, n$. The path $(v_i)_{i=0}^n$ contains n edges. The *length* of a path is the number of edges in the path.

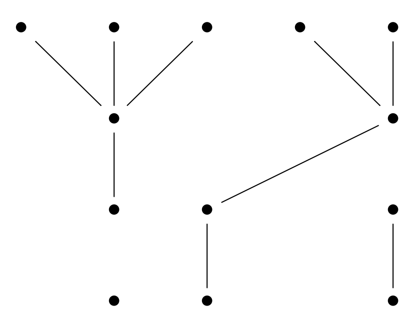
The path is *simple* or *non-intersecting* if $v_i \neq v_j$ for all $0 \leq i < j \leq n$. The path is *closed* if $v = v'$. A closed path is also called a *circuit*. A *simple closed path* in γ is a closed path $(v_i)_{i=0}^n$ such that $v_i \neq v_j$ for $1 \leq i < j \leq n$. The *girth* of a graph is the length of the shortest circuit in the graph of length at least 3.

Vertices v and v' are *connected* if there exists a path from v to v'. This defines a relation $\sim$ on V: $v \sim v'$ if there exists a path from v to v'. This is an equivalence relation (Exercise 1), and the equivalence classes of this relation are called the *connected components* of Γ. The graph Γ is *connected* if there exists a path from v to v' for every pair of distinct vertices $v, v' \in V$.

A graph with no circuits is called a *forest*. A connected graph with no circuits is called a *tree*. Thus, the connected components of a forest are trees. Here is a drawing of a tree:



Here is a drawing of a forest that contains four trees:



Exercises

Let $\Gamma = \gamma(V,E)$ be a graph.

1. Prove that the connected relation on the vertices of the graph Γ is reflexive, symmetric, and transitive, and so "being connected by a path" is an equivalence relation.
2. a. Prove that if $\Gamma(V,E)$ is a finite graph with no loops, then
$$|E| = \frac{1}{2}\sum_{v\in V}\deg(v).$$
   b. Prove that if $\Gamma(V,E)$ is a finite graph with exactly r loops, then
$$|E| = \frac{1}{2}\left(r + \sum_{v\in V}\deg(v)\right).$$
3. Let $V = V_1 \cup V_2$ and $V_1 \cap V_2 = \emptyset$. Prove that if Γ is a bipartite graph on the vertex sets V_1 and V_2, then $|E| \leq |V_1||V_2|$, and that Γ is the complete bipartite graph if and only if $|E| = |V_1||V_2|$.
4. The *neighborhood* $N(v)$ of a vertex $v \in V$ is the set of vertices adjacent to v, that is,
$$N(v) = \{v' \in V : \{v,v'\} \in E\}.$$
   a. Prove that $v \in N(v)$ if and only if Γ has a loop at v.
   b. The degree of the vertex v, denoted $\deg(v)$, is the number of edges that contain v. Prove that $\deg(v) = |N(v)|$ if and only if Γ has no multiple edges.
   c. Let $v, v' inV$. Prove that $N(v) \cap N(v') \neq \emptyset$ if and only if v and v' are connected by a path of length 2.
5. Prove that if there exists a closed path at the vertex v in Γ, then there exists a simple closed path at the vertex v.
6. Prove that the length of a circuit in a bipartite graph is even.
7. A *leaf* in a tree is a vertex of degree 1.
   a. Let Γ be the infinite graph with vertex set $V = \mathbf{Z}$ and edge set $E = \{\{n,n+1\} : n \in \mathbf{Z}\}$. Prove that this graph is a tree with no leaves. Prove that the distance from m to n is $|-n|$ for all $m,n \in \mathbf{Z}$.
   b. Prove that a finite tree with at least two vertices contains at least two leaves.

A.12 Metric spaces

A *metric space* is a set X together with a function that measures the "distance" between every pair of points of the set. Here is the formal definition: A *metric space* is a pair (X,d), where X is a set and d is a real-valued on X^2 that satisfies the following properties:

(i) $d(x,y) \geq 0$ for all $x,y \in X$, and $d(x,y) = 0$ if and only if $x = y$,
(ii) $d(x,y) = d(y,x)$ for all $x,y \in X$,
(iii) $d(x,y \leq d(x,z) + d(z,y)$ for all $x,y,z \in X$. This is called the *triangle inequality*.

The function d is called the *distance function* or the *metric* on the set X.

For example, $(\mathbf{Z}, |\ |)$ is a metric space, where $\mathbf{Z}$ is the set of integers and the metric is the absolute value: For all $x,y \in \mathbf{Z}$, the distance between x and y is $|x-y|$. Similarly,$(\mathbf{R}, |\ |)$ and $(\mathbf{C}, |\ |)$ are metric spaces, where $\mathbf{R}$ and $\mathbf{C}$ are the real and complex numbers, respectively, and the metric is the usual absolute value.

The *diameter* of a nonempty subset Y of a metric space X, denoted $\mathrm{diam}(Y)$, is the least upper bound of the set of distances between elements of Y, that is,

$$\mathrm{diam}(Y) = \sup\left(\{d(y,y') : y,y' \in Y\}\right).$$

Thus, $\mathrm{diam}(Y) = 0$ if and only if Y is a set with only one element. For example, in the metric space $\mathbf{R}$ with the usual absolute value, we have $\mathrm{diam}(\mathbf{R}) = \infty$. If $I = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$ and if $J = \{x \in \mathbf{R} : 0 < x < 1\}$, then $\mathrm{diam}(I) = \mathrm{diam}(J) = 1$.

Let (X,d) be a metric space and let $x_0 \in X$. The *open ball* of radius r with center x_0 is the set

$$B(r,x_0) = \{x \in X : d(x,x_0) < r\}.$$

The *closed ball* of radius r with center x_0 is the set

$$\overline{B}(r,x_0) = \{x \in X : d(x,x_0) \leq r\}.$$

The *sphere* of radius r with center x_0 is the set

$$S(r,x_0) = \{x \in X : d(x,x_0) = r\}.$$

Every connected graph $\Gamma(V,E)$ is a vector space. Because Γ is connected, there exists at least one path between every pair v, v' of distinct vertices in V. We define the *length* of a path as the number of edges in the path. Thus, the length of the path $(v_i)_{i=0}^n$ is n. We define the distance $d(v,v')$ as the length of the shortest path from v to v'. Thus, $d(v,v') \geq 1$ and $d(v,v') = 1$ if and only if v and v' a are adjacent vertices in Γ. We define $d(v,v) = 0$ for every vertex $v \in V$. Thus, for all $v,v' \in V$ we have $d(v,v') = 0$ if and only if $v = v'$.

If $(v_i)_{i=0}^n$ is a path in Γ from v to v', then the "reverse path" $(v_{n-i})_{i=0}^n$ is a path in Γ from v' to v. Thus, there is a path of length n from v to v' if and only if there is a path of length n from v' to v, and so the shortest paths from v to v' and from v' to v have the same length. This implies that $d(v,v') = d(v',v)$ for all vertices v and v'.

Let v, v', and v'' be vertices in V, with $d(v,v') = r$ and $d(v',v'') = s$. Thus, there exists a path $(v_i)_{i=0}^r$ of length r from v to v', and there exists a path $(v_i')_{i=0}^s$ of length s from v' to v''. We construct a path length $(w_i)_{i=0}^{r+s}$ from v to v'' as follows:

$$w_i = \begin{cases} v_i & \text{if } i = 0, \dots, r \\ v'_{i-r} & \text{if } i = r, \dots, s. \end{cases}$$

Because the distance from v to v'' is the minimum of the lengths of all paths from v to v'', it follows that

$$d(v, v'') \leq r + s = d(v, v') + d(v', v'').$$

The "path length" function d satisfies the triangle inequality, and so (V, d) is a metric space. Thus, every graph is a metric space.

In a graph, a path of minimum length is called a *geodesic*.

The *diameter* of a connected subset of a graph is the greatest distance between two vertices in the subset. The *diameter* of a connected graph Γ, denoted $\operatorname{diam}(\Gamma)$, is the greatest distance between two vertices in the graph, that is, the length of the longest geodesic in the graph.

Exercises

1. A subset Y of a metric space is *bounded* if there exists $z \in X$ and $c \in \mathbf{R}$ such that $d(y, z) \leq c$ for all $y \in Y$. Prove that if Y is a bounded set, then for every $x_0 \in X$ there exists $r \in \mathbf{R}$ such that $Y \subseteq B(r, x_0)$.

A.13 Pigeonhole principle

The pigeonhole principle states that if there are n pigeon holes and $n+1$ pigeons, and if each pigeon is put into a pigeonhole, then some pigeon hole contains at least two pigeons.

Here is an application of the pigeonhole principle. For every real number α, the *integer part* of α is greets integer k such that $k \leq \alpha$, that is, the unique integer k such that $k \leq \alpha < k+1$. If k is the integer part of α, then the *fractional part* of α is $\alpha - k$. We denote the integer part of α by $[\alpha]$ and the fractional part of α by (α). Thus,

$$\alpha = [\alpha] + (\alpha)$$

where $[\alpha] \in \mathbf{Z}$ and $0 \leq (\alpha) < 1$.

Theorem A.18. *Let α be an irrational number. For every positive integer Q there is a rational number p/q such that $q \leq Q$ and*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Proof. Consider the sequence of fractional parts

$$0, (\alpha), (2\alpha), \ldots, (Q\alpha).$$

These $Q+1$ numbers are in the interval $(0,1)$. Partition this interval into the Q subintervals

$$\left[\frac{i-1}{Q}, \frac{i}{Q}\right) \quad \text{for } i = 1, 2, \ldots, Q.$$

By the pigeonhole principle, at least one subinterval contains two terms of the sequence, that is, there exist integers j, r, and s with $j \in \{1, 2, \ldots, Q\}$ and $0 \leq r < s \leq Q$ such that

$$\{(r\alpha), (s\alpha)\} \subseteq \left[\frac{j-1}{Q}, \frac{j}{Q}\right).$$

Let $q = s - r$ and $p = [s\alpha] - [r\alpha]$. Then $p, q \in \mathbf{Z}$, $1 \leq q \leq Q$, and

$$|q\alpha - p| = |(s\alpha - [s\alpha]) - (r\alpha - [r\alpha])| < \frac{1}{Q}.$$

It follows that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ} \leq \frac{1}{q^2}.$$

This completes the proof.

Exercises

1. a. There is a drawer contain socks of 5 different colors. What is the least number of socks you must choose to be certain that you have a pair of socks of the same color?
   b. There is a drawer contain socks of 5 different colors. What is the least number of socks you must choose to be certain that you have a three socks of the same color?
2. a. There is a drawer contain socks of k different colors. What is the least number of socks you must choose to be certain that you have a pair of socks of the same color?
   b. There is a drawer contain socks of k different colors. What is the least number of socks you must choose to be certain that you have a three socks of the same color?
3. Find a rational number p/q such that $|\sqrt{2} - p/q| < 1/25$ and $1 \leq q \leq 5$.
4. Prove that if $2n+1$ pigeons are put into n pigeonholes, then at least one pigeonhole contains at least three pigeons.
5. Let k be a positive integer. Prove that if $kn+1$ pigeons are put into n pigeonholes, then at least one pigeonhole contains at least $k+1$ pigeons.

A.14 Zorn's lemma

Infinite paths in infinite trees of bounded degree.

A.15 Cardinal numbers

A.16 Permutation groups and the symmetric group S_n

A *function* from the set X to the set Y is a relation f on $X \times Y$ such that for each $x \in X$ there is a unique $y \in Y$ with $(x,y) \in f$. If f is a function, we write $f : X \to Y$. The set X is called the *domain* of the function f, and the set Y is called the *range* of f. We write $f(x) = y$ if $(x,y) \in f$. The *image* of f is the set $\{y \in Y : y = f(x) \text{ for some } x \in X\}$.

If $f : X \to Y$ and $g : Y \to Z$ are functions, then the *composite function* $gf : X \to Z$ is defined by $(gf)(x) = g(f(x))$. Composition of functions is associative, that is, if $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$, then $(hg)f$ and $h(gf)$ are functions from X to W, and $(hg)f = h(gf)$ (Exercise 2).

A function $f : X \to Y$ is *one-to-one* if for all $x_1, x_2 \in X$ we have $f(x_1) = f(x_2)$ only if $x_1 = x_2$. A function $f : X \to Y$ is *onto* if for each $y \in Y$ there exists $x \in X$ such that $f(x) = y$. If the functions $f : X \to Y$ and $g : Y \to Z$ are one-to-one, then the composite function $gf : X \to Z$ is one-to-one. If the functions $f : X \to Y$ and $g : Y \to Z$ are onto, then the composite function $gf : X \to Z$ is onto (Exercise 1). It follows that if $f : X \to Y$ and $g : Y \to Z$ are one-to-one and onto functions, then the composite function $gf : X \to Z$ is also one-to-one and onto.

A function $f : X \to Y$ is *one-to-one and onto* if it is both one-to-one and onto. For example, the identity function $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$ for all $x \in X$ is a one-to-one and onto function. If $f : X \to Y$ is one-to-one and onto, then for each $y \in Y$ there is a unique $x \in X$ such that $f(x) = y$. We define the function $g : Y \to X$ by $g(y) = x$, where x is the unique element of X such that $f(x) = y$. Then $gf = \mathrm{id}_X$ and $fg = \mathrm{id}_Y$. We call g the *inverse function* of f, and denote it by f^{-1}.

We say the sets X and Y *have the same cardinality* or *have the same number of elements* if there exists a function $f : X \to Y$ that is one-to-one and onto. We denote this by $|X| = |Y|$.

A *permutation* of a set X is a function $f : X \to X$ that is one-to-one and onto. Let $\mathrm{Sym}(X)$ denote the set of all permutations of X. If f and g are permutations of X, then fg is also a permutation of X, and so $\mathrm{Sym}(X)$ is closed under the binary operation of composition of functions. Moreover, $\mathrm{id}_X \in \mathrm{Sym}(X)$ and every permutation has an inverse. Therefore, $\mathrm{Sym}(X)$ is a group.

If $|X| = 1$, then the only permutation of X is id_X. If $|X| = 2$ and $X = \{a,b\}$, then the function $\sigma : X \to X$ defined by $\sigma(a) = b$ and $\sigma(b) = a$ is a permutation, and $\mathrm{Sym}(X) = \{\mathrm{id}_X, \sigma\}$ is an abelian group of cardinality 2.

Suppose that $|X| \geq 3$ and that a,b,c are three pairwise distinct elements of X. Define permutations $\sigma, \tau \in \mathrm{Sym}(X)$ by

$$\begin{aligned} \sigma(a) &= b \\ \sigma(b) &= c \\ \sigma(c) &= a \\ \sigma(x) &= x \quad \text{for all } x \in X \setminus \{a,b,c\}. \end{aligned}$$

and

$$\begin{aligned} \tau(a) &= b \\ \tau(b) &= a \\ \tau(x) &= x \quad \text{for all } x \in X \setminus \{a,b\}. \end{aligned}$$

Then $\tau\sigma(a) = a$ and $\sigma\tau(a) = c$, and so $\sigma\tau \neq \tau\sigma$. Thus $\mathrm{Sym}(X)$ is a nonabelian group if $|X| \geq 3$.

For every positive integer n, the *symmetric group* S_n is the the group of permutations of the finite set $\{1,2,3,\ldots,n\}$.

Exercises

1. a. Prove that if the functions $f : X \to Y$ and $g : Y \to Z$ are one-to-one, then the composite function $gf : X \to Z$ is one-to-one.
   b. Prove that if the functions $f : X \to Y$ and $g : Y \to Z$ are onto, then the composite function $gf : X \to Z$ is onto.
2. Prove that if $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$ are functions, then $(hg)f = h(gf)$.

Appendix B
Solutions

B.1 Linear Equations and Vector Sapces

Section 4.

Let L denote the affine subspace of solutions.

Problem 3.

$$L = \left\{ z \begin{pmatrix} 1/3 \\ -5/3 \\ 1 \end{pmatrix} : z \in \mathbf{R} \right\} = \left\{ z \begin{pmatrix} 1 \\ -5 \\ 3 \end{pmatrix} : z \in \mathbf{R} \right\}$$

Problem 6.

$$L = \begin{pmatrix} 6 \\ -8 \\ 0 \end{pmatrix} + \left\{ z \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} : z \in \mathbf{R} \right\}$$

Problem 8.

$$L = \left\{ z \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} : z \in \mathbf{R} \right\}$$

Problem 11.

$$L = \begin{pmatrix} 13/7 \\ 18/7 \\ 0 \end{pmatrix} + \left\{ z \begin{pmatrix} -1/7 \\ -10/7 \\ 1 \end{pmatrix} : z \in \mathbf{R} \right\} = \begin{pmatrix} 13/7 \\ 18/7 \\ 0 \end{pmatrix} + \left\{ z \begin{pmatrix} -1 \\ -10 \\ 7 \end{pmatrix} : z \in \mathbf{R} \right\}$$

Problem 13.

$$L=\begin{pmatrix}7/5\\0\\1/5\end{pmatrix}+\left\{z\begin{pmatrix}1/5\\1\\-7/5\end{pmatrix}:z\in\mathbf{R}\right\}=\begin{pmatrix}7/5\\0\\1/5\end{pmatrix}+\left\{z\begin{pmatrix}1\\5\\-7\end{pmatrix}:z\in\mathbf{R}\right\}$$

Problem 16.

$$L=\left\{\begin{pmatrix}97\\0\\-29\end{pmatrix}+y\begin{pmatrix}-23\\1\\7\end{pmatrix}:y\in\mathbf{R}\right\}$$

Problem 18.

$$L=\begin{pmatrix}-26/7\\29/7\\0\\0\end{pmatrix}+\left\{z\begin{pmatrix}-13/7\\4/7\\1\\0\end{pmatrix}:z\in\mathbf{R}\right\}+\left\{w\begin{pmatrix}11/7\\-5/7\\0\\1\end{pmatrix}:w\in\mathbf{R}\right\}$$

Problem 19.

$$L=\left\{y\begin{pmatrix}-3\\1\\0\\0\end{pmatrix}+w\begin{pmatrix}-4\\0\\2\\1\end{pmatrix}:y,w\in\mathbf{R}\right\}$$

Section 6.

Problem 2c.
Linearly dependent:

$$3\begin{pmatrix}5\\-2\\1\end{pmatrix}-7\begin{pmatrix}1\\-2\\5\end{pmatrix}-8\begin{pmatrix}1\\1\\-4\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}.$$

Problem 5.

$$\begin{pmatrix}7\\-3\\2\end{pmatrix}=\begin{pmatrix}5\\-2\\1\end{pmatrix}+\begin{pmatrix}1\\-2\\5\end{pmatrix}+\begin{pmatrix}1\\1\\-4\end{pmatrix}=4\begin{pmatrix}5\\-2\\1\end{pmatrix}-6\begin{pmatrix}1\\-2\\5\end{pmatrix}-7\begin{pmatrix}1\\1\\-4\end{pmatrix}.$$

References

Index